Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню бакалавра

студента	***Юсипіва Михайла Сергійовича***
академічної групи	***125-20-1***
спеціальності	***125 Кібербезпека***
спеціалізації[1]	
за освітньо-професійною програмою	***Кібербезпека***
на тему	***«Аналіз політик безпеки інформації іноземних і українських***
компаній»	

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	к.т.н., доц. Герасіна О.В.			
розділів:				
спеціальний				
економічний	к.е.н., доц. Пілова Д.П.	95	відмінно	
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2024

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студе-нту	***Юсипіву Михайлу Сергійовичу***	**академічної групи**	***125-20-1***
	(прізвище ім'я по-батькові)		(шифр)

спеціальності	*125 Кібербезпека*
	(код і назва спеціальності)

на тему	***«Аналіз політик безпеки інформації іноземних і українських компаній»***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 23.05.2024р. № 469-с

Розділ	Зміст	Термін виконання
Розділ 1	Аналіз актуальності застосування та впровадження політик безпеки. Складові політик безпеки, етапи їх створення. Огляд законодавства у сфері забезпечення інформаційної безпеки. Постановка задачі.	15.03.2024
Розділ 2	Аналіз політик інформаційної безпеки іноземних компаній та українських компаній у банківській сфері. Визначення переваг та недоліків політик.	10.05.2024
Розділ 3	Аналіз економічної доцільності проведення аналізу та впровадженню нововведень до політик безпеки компаній.	11.06.2024

Завдання видано _____ Олександра ГЕРАСІНА
(підпис керівника) (ім'я, прізвище)

Дата видачі: 15.01.2024р.

Дата подання до екзаменаційної комісії: 28.06.2024р.

Прийнято до виконання _____ Михайло ЮСИПІВ
(підпис студента) (ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка: 84 с., 5 рис., 1 табл., 4 додатки, 57 джерел.

Об'єкт дослідження: політики інформаційної безпеки.

Предмет дослідження: політики інформаційної безпеки іноземних та українських організацій.

Мета роботи: аналіз та пошук інноваційних рішень у політиках інформаційної безпеки українських та іноземних організацій.

Методи дослідження: опис, аналіз, порівняння.

У першому розділі було визначено головні елементи політик безпеки, мету, завдання, сферу дії політик, а також вимоги та методи забезпечення захисту інформації в організаціях з використанням політик безпеки. Проаналізовано законодавче регулювання захисту інформації в Україні.

У другому розділі було проаналізовано політики інформаційної безпеки іноземних та українських організацій з третього сектору економіки – сфера послуг, а саме банківська сфера. Визначені головні переваги та недоліки політик інформаційної безпеки іноземних та українських організацій.

У третьому розділі було проведено розрахунок економічної доцільності проведення аналізу, розробки та впровадження складових політик інформаційної безпеки для мінімізації збитків, термін окупності, капітальні та експлуатаційні витрати.

Практична цінність роботи полягає у пошуку інноваційних рішень для покращення політик інформаційної безпеки організацій. Постійна загроза кібератак зі сторони країни-агресора вимагає постійного вдосконалення та покращення методів та засобів захисту інформації в українських організаціях, в тому числі у банківській сфері.

ПОЛІТИКА БЕЗПЕКИ, ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, ЗАХИСТ ІНФОРМАЦІЇ, ІНФОРМАЦІЙНА СИСТЕМА, КІБЕРБЕЗПЕКА, УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, ІНФОРМАЦІЙНА БЕЗПЕКА.

ABSTRACT

Explanatory note: 84 pp., 5 pics., 1 table, 4 apps, 57 sources.

Object of research: information security policies.

Subject of research: information security policies of foreign and Ukrainian organizations.

The purpose of the work: analysis and search for innovative solutions in information security policies of Ukrainian and foreign organizations.

Research methods: description, analysis, comparison.

In the first section, the main elements of security policies, the purpose, tasks, scope of policies, as well as requirements and methods of ensuring information protection in organizations using security policies. The legislative regulation of information protection in Ukraine is analyzed.

In the second section, the information security policies of foreign and Ukrainian organizations from the third sector of the economy - the service sector, namely the banking sector - were analyzed. The main advantages and disadvantages of information security policies of foreign and Ukrainian organizations are identified.

In the third section, the calculation of the economic feasibility of the analysis, development and implementation of the components of information security policies to minimize losses was carried out, payback period, capital and operating costs.

The practical value of the work lies in the search for innovative solutions to improve information security policies of organizations. The constant threat of cyberattacks from the aggressor country requires constant improvement and improvement of methods and means of information protection in Ukrainian organizations, including in the banking sector.

SECURITY POLICY, INFORMATION SECURITY POLICY, INFORMATION PROTECTION, INFORMATION SYSTEM, CYBER SECURITY, INFORMATION SECURITY MANAGEMENT, INFORMATION SECURITY

.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС	–	автоматизована система;
ЗІ	–	захист інформації;
ІБ	–	інформаційна безпека;
ІзОД	–	інформація з обмеженим доступом;
ІКС	–	інформаційно-комунікаційна система;
ІС	–	інформаційна система;
ІТ	–	інформаційні технології;
КС	–	комп'ютерна система;
ОС	–	операційна система;
ПБ	–	політика безпеки;
ПЗ	–	програмне забезпечення;
ПІБ	–	політика інформаційної безпеки;
СЗІ	–	системи захисту інформації;
СТЗІ	–	системи технічного захисту інформації.

ЗМІСТ

С.

ВСТУП

Під час активного розвитку інформаційних технологій збільшується кількість та якість протиправних дій у кіберпросторі. Кіберпростір став новим майданчиком для поширення злочинності, посягання на свободи та права людей. Організації захищаються у кіберпросторі з використанням технічних, апаратних засобів та організаційних методів. Політики інформаційної безпеки як організаційні методи повинні періодично переглядатися та актуалізуватися для підтримання надійного рівня інформаційної безпеки організації, захисту людських ресурсів, підтримання конфіденційності, цілісності та доступності інформації, спостережності інформаційної системи тощо. Для ефективного функціонування політик інформаційної безпеки та впливу їх на загальний рівень інформаційної безпеки на підприємстві повинен бути постійний аналіз, розробка та впровадження нововведень до політик, які реагуватимуть на нові виклики та мінімізуватимуть ризики від загроз для інформаційної безпеки.

Предметом розробки є політики безпеки інформації іноземних та українських організацій.

Мета роботи: аналіз політик інформаційної безпеки українських та іноземних організацій, пошук інноваційних рішень.

Завдання роботи включають:

1. Визначення основних вимог до політик безпеки, їх мету, завдання, область застосування.

2. Огляд законодавчої бази України з регулювання захисту інформації.

3. Аналіз політик інформаційної безпеки українських та іноземних організацій.

4. Визначення переваг та недоліків.

5. Розрахунок економічної доцільності аналізу та додаткового впровадження нових політик інформаційної безпеки чи покращення вже існуючих організаціям.

Практичне значення роботи полягає у пошуку інноваційних рішень для покращення політик інформаційної безпеки організацій. Постійна загроза кібератак

зі сторони країни-агресору вимагає постійного вдосконалення та покращення методів та засобів захисту інформації в українських організаціях, в тому числі у банківській сфері.

Питання аналізу та порівняння політик безпеки та їх складових є новизною у дослідженнях науковців на тему інформаційної безпеки та політик безпеки. Серед вітчизняних та іноземних науковців майже не виділяють важливість аналізу політик організацій з різних країн та знаходження нововведень, що будуть в нагоді для покращення захисту інформації у організаціях.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Політики безпеки. Мета. Завдання. Область застосування.

Політики безпеки є одним з найважливіших понять інформаційної безпеки. Політики дозволяють встановлювати відповідальність за ті чи інші дії, невиконання обов'язків, план дій на випадок порушення правил експлуатації систем чи поводження з інформацією. Політики безпеки повинні бути наявні в організаціях через важливість в бізнес процесах, а також через наявність стандартів, таких як галузеві, державні, місцеві чи міжнародні, які вимагають наявності даних документів.

Політика безпеки інформації - документ або сукупність документів системного рівня, які містять набір вимог, правил, обмежень, рекомендацій, що регламентують порядок інформаційної діяльності в ІС і спрямовані на досягнення і підтримку стану інформаційної безпеки системи та організації в цілому. [4]

Згідно з [2,3] Політика безпеки інформації являє собою набір законів, правил, обмежень, рекомендацій, інструкцій тощо, які регламентують порядок обробки інформації, поводження й взаємодію з нею. Також політика безпеки інформації спрямована на захист інформації від певних загроз. Термін «політика безпеки» можна застосовувати щодо різних за величиною об'єктів, наприклад щодо організації, автоматизованої системи (АС), обчислювальної системи (ОС), комп'ютерної системи (КС), послуги, що реалізується системою тощо. Також цим документом вводиться поняття «політики послуги» замість словосполучення «політика безпеки інформації, що реалізується послугою» Наприклад політика реєстрації акаунтів тощо.

Загалом політика безпеки є сукупністю адміністративних, програмних й апаратних рішень, щодо інформації, що циркулює в системі, персоналу, що працює з цією інформацією, а також системи, де циркулює інформація і де, персонал працює з цією інформацією. Від розміру об'єкту, залежить формальність й конкретність правил, які до цього застосовуються, наприклад для організації термін «політика безпеки» може встановлювати загальні рамки й вимоги щодо взаємодії з інформацією, що заборонено робити, а що дозволено й все, а наприклад

«політика реєстрації в онлайн банківському сервісі» встановлює чіткіші правила й обов'язки для персоналу, який взаємодіє з даними, що циркулюють у цьому сервісі, для клієнтів, які використовують цей сервіс. Дрібніші об'єкти мають більш конкретизовані й формалізовані вимоги, ніж більші. [3]

Метою політик безпеки є створення й забезпечення захисту активів організації, виробничих й бізнес-процесів від різних варіантів загроз, це можуть бути як за типом дії відносно систем: зовнішні, внутрішні, або за характером дії: випадкові чи навмисні. Також забезпечення сталого розвитку організації, стабільної, безперебійної роботи, мінімізація ризиків ІБ. ПБ під час створення додає захисту організації, покращує довіру партнерів й інвестиційну привабливість. [6]

Політика безпеки інформації в АС є частиною загальної політики безпеки організації й успадковує положення державної політики у галузі захисту інформації. Для кожної АС політика безпеки інформації є індивідуальна й залежить від багатьох факторів, наприклад фізичне середовище, особливості обчислювальної системи, технології обробки інформації тощо. [3]

Загальна політика безпеки інформації в АС має містити складові частини, такі як політики забезпечення конфіденційності, цілісності і доступності оброблюваної інформації. Має бути встановлена відповідальність персоналу за виконання положень політики безпеки й бути персоніфікована. Ще однією вимогою до політики безпеки є визначення ресурсів АС, що потребують захисту, основні загрози для обчислювальної системи, інформації, персоналу, а також вимоги до захисту від цих загроз. У ПБ повинні бути цілі, сфера застосування, ролі в ІС та відповідальні посадові особи, опис ІС. [3]

Згідно з НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу» правила розмежування доступу являють собою «Частина політики безпеки, яка регламентує правила доступу користувачів і процесів до ресурсів КС, складає правила розмежування доступу» [3, с.12]

За Антонюком А.О., визначення політики безпеки під час розгляду питання безпеки інформації в АС є наявність деяких «бажаних» захищених станів

системи, ці стани описують «захищеність» системи. В свою чергу «захищеність» пов`язана з поняттям «загроза». [1]

Антонюк виділяє «три компоненти, що пов'язані з порушенням безпеки системи:

– «загроза» - джерело порушення властивості «захищеність»;
– «об'єкт атаки» - частина системи, на яку діє загроза;
– «канал дії» - середовище перенесення зловмисної дії.» [1, с.103]

Три компоненти, що пов'язані з порушенням безпеки системи об'єднуються політикою безпеки. Цей документ повинен враховувати загрози, об'єкт атаки, канал дії. [1]

Політика безпеки під час розробки досягає компромісу серед захисту інформації, що означає найбільш вдалий захист з найменшими інвестиціями й витратами, тому політика безпеки не може задовольняти усі сторони, що беруть участь у захисті інформації. ПБ є основою для створення системи захисту тобто системи підтримки виконання правил політики безпеки. Головним критерієм якості системи захисту можна вважати відповідність ПБ. «Якщо система захисту інформації (СЗІ) побудована вдало - вона надійно підтримує виконання правил ПБ, і, навпаки, СЗІ невдала, якщо вона ненадійно підтримує ПБ.»[1, с.103]

Через технічні та програмно-апаратні проблеми, що виникають при організації захисту в захищених АС, можуть існувати ситуації, коли ПБ може залишитися єдиним засобом, який забезпечує захист. Тому вдало реалізована ПБ, може підтримувати належний рівень захисту й дозволяти безперебійно функціонувати компанії. Розробка, дослідження, правильне застосування й імплементація ПБ є надзвичайно важливою й актуальною проблемою сучасних СЗІ. [1]

Основні принципи забезпечення безпеки за використанням політик безпеки є захист властивостей інформації, такі як конфіденційність, цілісність та доступність інформаційних ресурсів, впровадження відповідальності посадових осіб щодо забезпечення кіберзахисту, постійне навчання й покращення навичок персоналу організації, забезпечення безпечного й сталого функціонування й

недопущення порушень роботи об'єкту, розмежування прав доступу персоналу, політика мінімізації ролей й привілеїв, реагування на надзвичайні ситуації. [6]

Область застосування політик безпеки розповсюджується на всі аспекти діяльності організації та поширюється на всі активи організації. Політики безпеки можуть бути у всіх сферах життя, бо конфіденційні дані є всюди, особливо важливі сфери життя, де повинні бути політики безпеки інформації, це фінансова, медична сфери економіки.

Інформаційна безпека це відношення рівня інформаційного захисту до рівня інформаційних загроз. Інформаційна безпека є найважливішим аспектом ефективності будь-якого підприємства й має на меті захищати такі властивості інформації, як конфіденційність, цілісність й доступність інформації. Політика безпеки передбачає всебічний захист інформації під час бізнес-процесів на підприємстві й є головним інструментом забезпечення інформаційної безпеки на підприємстві. [5]

1.2 Складові політик безпеки. Етапи створення

1.2.1 Етапи створення політик безпеки

Під час створення політик безпеки треба відповісти на питання для кого та навіщо це. Відповіді на ці питання дозволять врахувати головні задачі, які майбутня політика буде вирішувати, які саме загрози будуть нейтралізовані чи зменшені можливі втрати, від реалізації цих загроз. Досягнення належного рівня безпеки інформації вимагає наявності чітко визначених вимог безпеки, планування систем безпеки й управління інформаційною системою, використання надійних апаратних засобів й програмного забезпечення, постійний моніторинг й покращення систем захисту. [16]

ПБ має бути розроблена, так щоб не потрібно було часто модифікувати чи видозмінювати її, не завжди доцільна надмірна конкретизація. [17]

«ПБ повинна передбачати використання всіх можливих заходів захисту інформації, зокрема: правові та морально-етичні норми, організаційні (адміністративні), фізичні, технічні (апаратні та програмні) заходи – і визначати правила та порядок застосування в організації кожного з цих видів.» [17, с.115]

ПБ повинна відповідати гарантіям, що в організації забезпечений відповідний рівень захисту інформації у залежності від рівня критичності інформації, реалізація захисту інформації є рентабельною, забезпечена персоніфікована відповідальність, звітність, реєстрація, аудит ресурсів, критичних для безпеки інформації. Також повинні бути плани забезпечення безперервної роботи у випадках нештатних ситуацій для критичних з погляду безпеки інформації процесів. [17]

Розробка політики безпеки інформації у організації може бути наступним чином:.

Аналіз ризиків. Першим кроком при побудові ПБ є аналіз й оцінка ризиків. Під час аналізу ризиків відбувається комплексний аудит організації, огляд сфери діяльності підприємства й підприємств-конкурентів, оцінка ризиків й вірогідність реалізації загроз. Під час проводження вищезгаданих подій потрібно визначити критичні загрози, які можуть створювати небезпеку для бізнес-процесів, властивостей інформації тощо. Важливо якнайкраще проаналізувати ризики, бо без цілісної картини одного з найбільш складних об'єктів – інформаційної системи, неможливо побудувати надійний та якісний захист. Після проведення аналізу інформаційних потоків, інвентаризацію інформаційних ресурсів, ранжирування інформації за показником цінності цієї інформації керівництво організації може приймати більш вдалі управлінські рішення, тим самим збільшуючи ефективність та прибутковість. [7, 16, 17]

Визначення вимог до заходів, методів, засобів захисту. Вимоги до політик безпеки також встановлюються стандартами ISO/IEC 27001, 27002, 27003. Потрібно визначити правила користування та створити систему взаємодії з інформацією, визначення прав доступу до елементів інформації, провести оцінку цінностей інформації. Також не менш важливим елементом є встановлення персоніфікованої відповідальності за порушення правил взаємодії з інформацією. Під час створення ПБ важливо не допустити помилкового або бездумного визначення правил ПБ, бо здебільшого є руйнування цінності інформації без порушення ПБ. Тобто при незадовільній ПБ навіть надійна СЗІ може бути вразливою для зловмисника. [1, 7, 16, 17]

Вибір основних рішень із забезпечення безпеки інформації. Політика безпеки та її складова - політика інформаційної безпеки є складовою великої структури із забезпечення безпеки інформації. ПБ є організаційним рішенням, яке встановлює порядок доступу до інформації, технологію зберігання, обробки та передачі інформації, цінність інформації, модель загроз, модель порушників, особливості апаратно-програмних засобів, особливості фізичного середовища, а також визначає відповідальних осіб. В свою чергу програмно-апаратні засоби є основними заходами забезпечення технічного захисту інформації. ПБ доповнює СТЗІ. [7, 17]

Організація виконання відновлювальних робіт та забезпечення безперервної роботи організації. Політика безпеки повинна містити план відновлювальних робіт, забезпечення неперервності бізнес-процесів, та заходи забезпечення сталого захисту інформації під час нештатних ситуацій. [7, 17]

Документальне оформлення політики безпеки. ПБ може бути у вигляді опису, а може бути викладена за допомогою формальної мови. Що в першому, що в другому випадку ПБ є необхідною умовою безпеки системи. Формальний вираз політики безпеки називають моделлю ПБ. Модель ПБ створюється у вигляді правил, згідно з якими мають відбуватися всі взаємодії між об'єктами й суб'єктами. [1, 17]

Головною метою створення ПБ інформаційної системи й опису її у вигляді формальної моделі - це визначення умов, за яких система знаходиться в безпеці. Цим умовам має підпорядковуватися система, повинні бути вироблені критерії безпеки й проведенні формальні доведення відповідності системи цим критеріям при додержанні встановлених правил і обмежень. Тільки уповноважені користувачі повинні мати змогу отримати доступ до інформації й здійснювати з інформацією дозволенні дії. [1]

Як зазначає Антонюк А.О., «формальні моделі потрібні, тому що тільки за їх допомогою можна довести безпеку системи, спираючись на об'єктивні й незаперечні постулати математичної теорії. Загальним підходом щодо всіх моделей є поділ множини сутностей, що становлять систему, на множини суб'єктів і

об'єктів, хоча самі визначення понять «об'єкт» і «суб'єкт» у різних моделях можуть істотно відрізнятися. Взаємодії в системі моделюються встановленням відношень певного типу між суб'єктами та об'єктами. Множина типів відношень визначається у вигляді набору операцій, які суб'єкти можуть здійснювати над об'єктами. Усі операції в системі контролюються певним спеціально призначеним для цього суб'єктом і забороняються або дозволяються відповідно до правил ПБ». [1]

Згідно з НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі» ПІБ повинна базуватися на основних принципах: системності, комплексності, неперервності захисту, достатності механізмів й заходів захисту та їх відповідності загрозам, гнучкості керування системами захисту, простоти й зручності використання, відкритості алгоритмів й механізмів захисту. [7]

1.2.2 Складові політик безпеки

Політика інформаційної безпеки повинна містити:

– мету й основні принципи забезпечення бізнес-процесів, інформаційних ресурсів тощо;

– опис цих процесів;

– вимоги до умов надання, зміни, скасування прав доступу користувачам;

– політику фізичної безпеки об’єкта;

– вимоги при взаємодії з постачальниками;

– політику облікових записів;

– політику забезпечення сталої, безперебійної роботи;

– порядок дій користувачів об’єкта у випадку збоїв чи відмов;

– вимоги до умов зміни, контролю, надання, скасування атрибутів доступу (парольна політика);

– політику використання зовнішніх носіїв;

– політику мережевого захисту;

– політику управління й оновлень компонентів об’єкта;

- політику контролю й реєстрації подій;
- політику управління інцидентами;
- політику електронних скриньок;
- політику проведень внутрішніх аудитів. [10]

Серед моделей ПБ найвідомішими є дискреційна, мандатна та рольова. [1]

Дискреційна модель політики безпеки включає дискреційне управління доступом, яке містить декілька вимог до системи: об'єкти й суб'єкти повинні бути ідентифіковані; права доступу до об'єкта системи визначаються на основі правил. Дискреційна модель реалізується за допомогою матриці доступу, яка має інформації про множину об'єктів системи, які доступні тому чи іншому суб'єкту системи. Однією з головних переваг дискреційної моделі є проста реалізація механізмів захисту, але недоліки моделі, такі як поганий захист від проникнення вірусів у систему або автоматичне визначення прав, бо кількість об'єктів завелика й постійно змінюється, через що задаються певні правила для видачі доступу, що може негативно впливати на безпеку інформації, через вірогідне отримання доступу до інформації несанкційованим особам. Також до недоліків дискреційної моделі можна віднести проблеми з контролем поширенню прав доступу наприклад власник файлу може передати вміст файлу іншому користувачеві, а той може іншому й в цьому випадку не контролюється поширення інформації, що може мати негативний вплив на безпеку АС. Тобто дискреційна модель не реалізує чітку й ясну службу захисту інформації в АС. [1]

Мандатна модель політики безпеки включає мандатне управління доступом, що являє собою: об'єкти й суб'єкти повинні бути ідентифіковані; у системі визначено лінійно упорядкований набір міток секретності; кожному об'єкту й суб'єкту надано мітку секретності, що визначає ступінь цінності інформації в ньому. Головна мета мандатної моделі це запобігання витоку інформації від об'єктів з високим рівнем доступу та/або ролі в АС до об'єктів з низьким рівнем доступу та/або ролі в АС. Нейтралізація інформаційних каналів в АС, що виникають згори вниз дозволяє запобігти витоку інформації й потраплянню до несанкціонованих об'єктів. У сучасних системах захисту мандатна модель

реалізується мандатним контролем на найнижчому рівні, апаратно-програмному. Пристрій мандатного контролю є монітор звернень, працює він просто, кожне звернення суб'єкта до об'єкта аналізується монітором звернень й після порівняння мітки секретності об'єкта з міткою рівня доступу суб'єкту видається рішення про допуск чи відхилення. Якщо порівнювати мандатну модель з дискреційною, можна побачити суттєві відмінності, по-перше, мандатна модель на відміну від дискреційної має важку практичну реалізацію й вимагає великих ресурсів, це є головним недоліком мандатної моделі. По-друге мандатна модель є більш надійною ніж дискреційна, бо мандатна модель безпеки відстежує не тільки правила доступу суб'єктів до об'єктів, а ще стан АС, також правила мандатної політики простіші для розуміння користувачам й розробникам АС, що покращує безпеку. [1]

Рольова модель політики безпеки має керування доступом, що здійснюється на основі матриці прав доступу по ролям й за допомогою правил, що встановлюють умови призначення ролей користувачам. Рольова модель має поняття користувач й роль, на заміну суб'єкта й об'єкта. Користувач – суб'єкт, що працює в системі й має службові обов'язки, а роль – набір повноважень, необхідний для виконання обов'язків користувачем. Під час використання рольової моделі визначаються права доступу ролей до об'єктів, а також набори мінімальних повноважень для користувачів. Через гнучкість рольова модель має переваги над іншими моделями. [1]

1.3 Законодавче регулювання сфери інформаційної безпеки.

У сучасному світі політика інформаційної безпеки відіграє все більшу роль й скоро стане ключовим фактором життя суспільства, Україна не виключення з правил. В Україні так само як і в усьому світі є проблеми з забезпеченням безпеки держави, особливо в інформаційному середовищі. Активний розвиток інформаційних технологій ставить під загрозу сталий розвиток цілих держав, тому політика інформаційної безпеки відіграє дедалі більшу роль, держава будує свою політику таким чином, щоб суспільство могло розвиватися соціально, політично, економічно й технологічно. Розвиток інформаційних технологій призвів до того,

що злочини у інформаційному середовищі несуть все більш руйнівний вплив на економіку й безпеку цілих країн й суспільств. З кожним роком виклики, які ставляться перед політиками, діячами в сфері інформаційної безпеки потребують все більшої уваги до наростаючих загроз, компанії повинні збільшувати штат співробітників, які забезпечують безпечне функціонування компанії й організовують безпеку бізнес-процесів.

Розвиток інформаційних засобів робить можливим злочини проти суспільства й цілих країн через причини, Стичинська А.Б. вважає, що «причини, через які це стало можливим:

– прогрес збору, обробки і передачі інформації;
– прогрес засобів комунікації;
– прогрес засобів маніпулювання людьми, спостереження за ними, застереження масових рухів. [11, с.101]

Інформаційна безпека не може бути забезпечена без розвитку інформаційно-телекомунікаційної інфраструктури й законодавчого регулювання захисту інформації. Україна пройшла величезний шлях трансформації законодавства після російської агресії проти України й анексії Криму. З 2014-го року Україна суттєво оновила нормативно-правові акти й є одним з найбільш вдалих прикладів для опису законодавчого регулювання сфери інформаційної безпеки серед країн, що розвиваються. Україна була першою країною, яка на собі зрозуміла, що таке велика, добре спланована кібератака. Найбільша кібератака в світі на телекомунікаційну мережу була скоєна на оператору мобільного зв'язку ПрАТ «Київстар» асоційованою з ГРУ ГШ РФ злочинною хакерською групою, також ідентичні за розмірами були скоєні атаки на об'єкти критичної інфраструктури, державні компанії, елементи електронного урядування тощо. Україна має доволі розгалужену систему реагування, запобігання, мінімізації наслідків, розслідування й навіть кібератак в інформаційному середовищі. В Україні діють величезна кількість нормативно-правових актів у сфері інформаційної безпеки, найголовніші, це закони, постанови, нормативні документи з технічного захисту інформації, державні стандарти України.

Закони:

– ЗУ «Про інформацію»;

– ЗУ «Про основні засади забезпечення кібербезпеки України»;

– ЗУ «Про захист інформації в інформаційно-комунікаційних системах»;

– ЗУ «Про державну таємницю»;

– ЗУ «Про захист персональних даних».

Постанови:

– Постанова Кабінету Міністрів України про «Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури»;

– Постанова Кабінету Міністрів України про «Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі»;

НД ТЗІ:

– НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу»;

– НД ТЗІ 2.5-004-99. «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу»;

– НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу»;

– НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу».

ДСТУ:

– ДСТУ 3396.0-97;

– ДСТУ 3396.1-97;

– ДСТУ 3396.2-97.

Законодавчу базу України з питань інформаційної безпеки можна поділити на дві групи. Перша група – це Доктрини, Стратегії, концепти, базові документи, які визначають шляхи розвитку й модернізації сфери кібербезпеки, а також

визначають найбільші виклики й загрози, які стоять перед Україною в кібернетичній сфері. Друга група – це Закони України, Укази Президента, рішення Ради Національної Безпеки та Оборони України, інші нормативно-правові акти центральних органів державної влади, чи органів відповідальних за забезпечення кібербезпеки, наприклад Державна служба спеціального зв'язку та захисту інформації України. [14]

Правову основу забезпечення кібербезпеки України становлять Конституція України – головний нормативно-правовий документ, Закон України «Про основи національної безпеки України», Закон України «Про засади внутрішньої й зовнішньої політики», Закон України «Про захист інформації в інформаційно-комунікаційних системах». Це основні документи, але ще є інші, менш важливі документі, які також регулюють деякі питання в царині забезпечення інформаційної безпеки держави, суспільства, бізнесу тощо.[13]

Закон України «Про інформацію» вводить поняття «документ – це матеріальний носій, що містить інформацію»; «захист інформації – це сукупність правових, адміністративних, організаційних, технічних заходів тощо, що забезпечують збереження, цілісність й належний порядок доступу до неї»; «інформація – будь-які відомості або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді»; «суб'єкт владних повноважень – орган державної влади або інший суб'єкт, що здійснює владні управлінські функції відповідно до законодавства, у тому числі на виконання делегованих повноважень». Також цим законом вводяться принципи інформаційних відносин, а саме гарантоване право на інформацію, доступність інформації, достовірність й повнота, свобода вираження поглядів й переконань, право на використання, поширення й зберігання інформації. [12]

Суб'єктами інформаційних відносин є«фізичні й юридичні особи», «суб'єкти владних повноважень» й «об'єднання громадян», а об'єктами - «інформація»».[12]

Інформація поділяється за порядком доступу на відкриту інформацію та інформацію з обмеженим доступом. Інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація.» [12]

Головним Законом України у сфері кібербезпеки та інформаційної безпеки є ЗУ «Про основні засади забезпечення кібербезпеки України», який встановлює визначення багатьох важливих термінів:

– «індикатори кіберзагроз - показники (технічні дані), що використовуються для виявлення та реагування на кіберзагрози»;

– «об'єкт критичної інформаційної інфраструктури - комунікаційна або технологічна система об'єкта критичної інфраструктури, кібератака на яку безпосередньо вплине на стале функціонування такого об'єкта критичної інфраструктури»;

– «кіберзахист – сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем»;

– «кібербезпека – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі».[13]

Виходячи з цього нормативно-правового акту об'єктами кібербезпеки є: конституційні права і свободи людини і громадянина; суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища; держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканість; національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави». А об'єктами кіберзахисту є:«комунікаційні системи, де обробляються національні інформаційні ресурси, або які використовуються в інтересах

держави»; «об'єкти критичної інформаційної інфраструктури»; «комунікаційні системи, які використовуються для задоволення суспільних потреб» [13]

Національна система кібербезпеки України складається з взаємопов'язаних суб'єктів забезпечення кібербезпеки, що реалізують певні заходи, серед яких криптографічний й технічний захист інформаційних ресурсів, а також кіберзахист об'єктів критичної інфраструктури. [13]

Головними суб'єктами національної системи кібербезпеки України є: Державна служба спеціального зв'язку та захисту інформації України; Національна поліція України; Служба безпеки України; Міністерство оборони України та Генеральний штаб Збройних сил України; розвідувальні органи; Національний банк України. [13]

Державна служба спеціального зв'язку та захисту інформації України (ДССЗ ЗІ України) є головним суб'єктом формування й реалізації державної політики щодо захисту у кіберпросторі інформації та державних інформаційних ресурсів, також активної протидії агресії у кіберпросторі, кіберзахисту об'єктів критичної інформаційної інфраструктури, здійснює державний контроль у сфері кіберзахисту; координує діяльність інших суб'єктів національної системи кібербезпеки України щодо кіберзахисту; забезпечує стале функціонування Національної телекомунікаційної мережі, впровадження й покращення організаційно-технічної моделі кіберзахисту; здійснює організаційно-технічні заходи із запобігання, виявлення та реагування на кіберінциденти та/або кібератаки також займається усуненням наслідків кіберінцидентів; інформує про кіберзагрози та відповідні методи захисту від них; забезпечує впровадження аудиту інформаційної безпеки на об'єктах критичної інфраструктури, встановлює вимоги до аудиторів інформаційної безпеки, визначає порядок їх атестації; координує, організовує та проводить аудит захищеності комунікаційних і технологічних систем об'єктів критичної інфраструктури на вразливість; забезпечує функціонування Державного центру кіберзахисту та Центру активної протидії агресії у кіберпросторі, урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA; [13]

Національна поліція України підвищує поінформованість громадян про безпеку в кіберпросторі, забезпечує захист прав, свобод й гідності людини й громадянина, інтересів суспільства й держави від кримінально протиправних посягань у кіберпросторі, а також здійснює заходи із запобігання, виявлення, припинення та розкриття кіберзлочинів; [13]

Служба безпеки України здійснює виявлення та запобігання, кримінальних правопорушень проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснює розвідувальні та контррозвідувальні заходи, що спрямовані на боротьбу з кібертероризмом та кібершпигунством, перевіряє готовність об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; протидіє кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави; розслідує та реагує на кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, чутливої інформації, критичної інформаційної інфраструктури; [13]

Міністерство оборони України, Генеральний штаб Збройних Сил України відповідно до компетенції здійснюють заходи з підготовки держави до відбиття воєнної агресії у кіберпросторі; здійснюють військову співпрацю з НАТО щодо забезпечення безпеки кіберпростору та захисту від кіберзагроз; під час надзвичайного і воєнного стану впроваджують заходи щодо забезпечення кібербезпеки критичної інформаційної інфраструктури; [13]

Розвідувальні органи України здійснюють розвідувальну діяльність щодо обставин, загроз та інших подій у кіберпросторі, що можуть нести загрозу національній безпеці України; [13]

Національний банк України визначає вимоги до заходів забезпечення кіберзахисту та інформаційної безпеки банками та іншими суб'єктами, що здійснюють діяльність на ринках фінансових послуг, здійснює нагляд та державне регулювання за діяльністю, операторів платіжних систем та/або учасниками платіжних систем, технологічними операторами платіжних послуг, здійснює контроль за виконанням суб'єктами вимог та заходів забезпечення кібербезпеки; створює центр кіберзахисту Національного банку України, забезпечує функціонування

системи кіберзахисту для банків, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг; забезпечує проведення оцінювання стану кіберзахисту та аудиту інформаційної безпеки на об'єктах критичної інфраструктури в банках, операторах платіжних систем та/або учасниках платіжних систем, технологічних операторах платіжних послуг. [13]

Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA, чиї завданнями є:

– проведення аналізу та накопичення даних про кіберінциденти;

– ведення державного реєстру кіберінцидентів;

– надання власникам об'єктів кіберзахисту практичної допомоги з питань запобігання та усунення наслідків кіберінцидентів;

– організація та проведення практичних семінарів з питань кіберзахисту для суб'єктів національної системи кібербезпеки та власників об'єктів кіберзахисту;

– підготовка рекомендацій щодо протидії сучасним видам кібератак та кіберзагроз;

– взаємодія з правоохоронним органам та інформування їх про кібератаки;

– взаємодія з іноземними та міжнародними організаціями з питань реагування на кіберінциденти, а також участь у Форумі команд реагування на інциденти безпеки FIRST із сплатою щорічних членських внесків;

– взаємодія з українськими командами реагування на комп'ютерні надзвичайні події, а також іншими організаціями, які провадять діяльність, пов'язану із забезпеченням безпеки кіберпростору;

– аналіз та оцінка отриманої від громадян інформації про кіберінциденти щодо об'єктів кіберзахисту;

– сприяння державним органам, органам місцевого самоврядування, військовим формуванням, підприємствам, установам, організаціям, а також громадянам України у вирішенні питань кіберзахисту та протидії кіберзагрозам. [13]

Забезпечення функціонування CERT-UA здійснює ДССЗ та ЗІ України. Контроль за дотриманням законодавства під час забезпечення кібербезпеки здійснюється Верховною Радою України, а контроль за діяльністю здійснює Президент України [13]

В Україні діє постанова КМУ №518 від 19.06.2019 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури», що встановлює вимоги до ПІБ об'єктів критичної інфраструктури, згідно з цією постановою, політика інформаційної безпеки - політика, що визначає підхід підприємства, установи та організації, які відповідно до законодавства віднесені до об'єктів критичної інфраструктури, до інформаційної безпеки, вимоги, правила, обмеження, рекомендації, що регламентують порядок дотримання та забезпечення інформаційної безпеки, також повинно бути затверджено політику управління ризиками інформаційної безпеки і методику їх оцінювання та оброблення за стандартом ДСТУ ISO/IEC 27005. Де цінність активів оцінюється за 4-х бальною шкалою. [6]

1.4 Висновок

Визначено загальну суть питання політика безпеки, визначено мету, область застосування, необхідність впровадження, основну структуру та обов'язкові елементи. Розробка ПБ є дуже відповідальною справою й потребує дуже якісного аналізу ризиків на першому етапі побудови ПБ, визначенню вимог до засобів, заходів захисту на другому етапі, виборі основних рішень із забезпечення безпеки інформації на третьому етапі, створенню безперервної роботи організації та захисту інформації на четвертому етапі, документальному оформленню політики безпеки на п'ятому етапі.

Проведено загальний огляд законодавства України у сфері забезпечення інформаційної безпеки, нормативно-правова база України має дуже розгалужену систему суб'єктів забезпечення кібербезпеки, що в свою чергу дозволяє суб'єктам забезпечення національної системи кібербезпеки якісно доповнювати один одного.

РОЗДІЛ 2. СПЕЦІАЛЬНИЙ РОЗДІЛ

2.1 Порівняння політик безпеки інформації в іноземних та українських компаніях. Переваги та недоліки.

З розвитком інформаційних технологій збільшується важливість інформації та її вага в сучасному світі, так з появою мережі інтернет й інтеграції в життя людей, інформація набуває ціни кольорових металів і навіть більше. З-за допомогою інформації проводяться інформаційно-психологічні операції, розпочинаються війни, терористичні акти тощо. Інформація використовується будь-де, будь-ким, у всіх процесах існування людини. Особливо цінна інформація, яка циркулює в організаціях чи підприємствах, які здійснюють свою діяльність через взаємодію з іншими людьми, наприклад медичні установи, банки, державні органи влади. Людина приходить до сімейного лікаря, з причини, що в неї погане самопочуття, лікар робить огляд й виписує електронне направлення до іншого лікаря, або в амбулаторію. Це електронне направлення містить цінну інформацію таку як , номер мобільного телефону лікаря, ПІБ пацієнта й дату народження, ПІБ лікаря, діагноз за яким видали направлення, джерело фінансування. Ця інформація відноситься Законом України «Про інформацію» згідно статті 11 закону, до «інформація про фізичну особу або персональні дані», які забороняється збирати, використовувати чи поширювати без згоди фізичної особи, також ця інформація відноситься до інформації з обмеженим доступом, згідно статті 21 цього ж закону. Тому важливість забезпечення безпеки інформації важко переоцінити. Кількість порушень прав людини й свобод в будь-якій сфері. Тим паче медичній, збільшується, через низку факторів, серед який виділяється висока ціна медичної інформації на чорних ринках, а також можливості маніпулювати людьми за допомогою цих медичних даних. [6]

В Україні до об’єктів критичної інфраструктури можуть бути віднесені підприємства, установи та організації з сфери охорони здоров’я, фармацевтики, інформаційних технологій, фінансів тощо згідно статті 6 Закону України «Про основні засади забезпечення кібербезпеки України» й статті 8 Закону України «Про критичну інфраструктуру». Згідно з Постановою Кабінету Міністрів №518 від

19.06.2019 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» на об'єктах критичної інфраструктури повинна бути розроблена та впроваджена політика безпеки інформації та політику управління ризиками інформаційної безпеки і методику їх оцінювання та оброблення за стандартом ДСТУ ISO/IEC 27005.[6, 9, 13]

Зазвичай, економіки країн розділяють на сектори. Сектор економіки це пов'язана група економічної діяльності, якій притаманні спільні галузеві, організаційно правові характеристики. Існує декілька варіантів розподілу економіки на сектори, найбільш поширений варіант розподілу на три сектори: перший – агропромисловий комплекс (АПК), другий – промисловість, третій – сфера послуг.

Агропромисловий комплекс – сектор економіки, що виробляє сільськогосподарську продукцію і складається з тракторного машинобудування, виробництв добрив, рослинництва, тваринництва, рибальства, а також харчової промисловості.

Промисловий комплекс – найдосконаліший сектор економіки, що складається з машинобудування, хімічної та нафтопереробної галузі, легкої промисловості, виробництва електроенергії тощо.

Сфера послуг – найбільший сектор економіки розвинених країн, та країн, що розвиваються, складається зі всього, що не входить до першого та другого секторів економіки, це і фінансова галузь, галузь туризму, наукові, медичні, освітні, торгово-розважальні заклади тощо.

Для аналізу вибрана галузь фінансових послуг з третього сектору економіки – сфери послуг. А саме банківські організації.

2.1.1 Огляд політик безпеки інформації в іноземних компаніях у фінансовій сфері.

Вибрано 6 банків з різних регіонів світу: 2 банки з Європи: «Jyske Bank A/S» та «British Business Bank»; 3 банки з Азії: 2 банки з Китайської республіки (Тайвань): «Taiwan Business Bank», «Chang Hwa Bank» та банк з Індії: «The Manipur State Co-operative Bank Limited»; з Африки вибраний «Stanbic Bank Uganda».

Jyske Bank A/S є третім за величиною банком Данії на ринку банківської діяльності Данії. Штаб-квартира в Сількеборг. Банк має 98 відділень у Данії та 1 в Німеччині. У банку працює 3.957 штатних працівників, близько 146.000 акціонерів станом на травень 2024р., власний капітал 43,3 млрд датських крон. Основні види діяльності: надання фінансових рішень для приватних клієнтів та компаній; інвестиційні консультаційні послуги міжнародним приватним банківським клієнтам, іпотечні кредити, лізинг, IT-хостинг. [46]

Політика безпеки банку [22] складається з 8-ми розділів:

- призначення та сфера застосування;
- рівень IT безпеки;
- організація та обов'язки;
- управління IT ризиками;
- захист даних;
- аутсорсинг;
- принципи безпеки;
- затвердження політики інформаційної безпеки.

Перший розділ містить мету та сферу застосування політики, метою є забезпечення високого рівня IT-безпеки, який впроваджений та підтримується у Банку.

Другий розділ – рівень IT безпеки. Рівень IT-безпеки повинен ґрунтуватися на прагненні Банку отримати та підтримувати надійний рівень захисту. Рівень безпеки повинен гарантувати, що ризики, пов'язані з використанням ІС не будуть перевищувати рівні ризиків, встановлені Банком для даної області. Рівень безпеки повинен ґрунтуватися на оцінках ризиків і відповідати законодавству та вимогам застосованими до сектора від регулятора. Рівень IT-безпеки повинен дозволяти Банку підтримувати ефективний захист від кіберзагроз.

Технологічні механізми, процеси та людські ресурси, ІС повинні бути захищені, задля забезпечення стабільної роботи бізнес-процесів Банку.

Вимоги, наведені у цій політиці, мають бути реалізовані вимоги, визначені в описах методів, структурах, настановах необхідно дотримуватися в будь-який час.

Політику безпеки, цілі та завдання, контроль за дотриманням політики затверджує наглядова рада групи раз на рік, або у зв'язку зі суттєвими змінами.

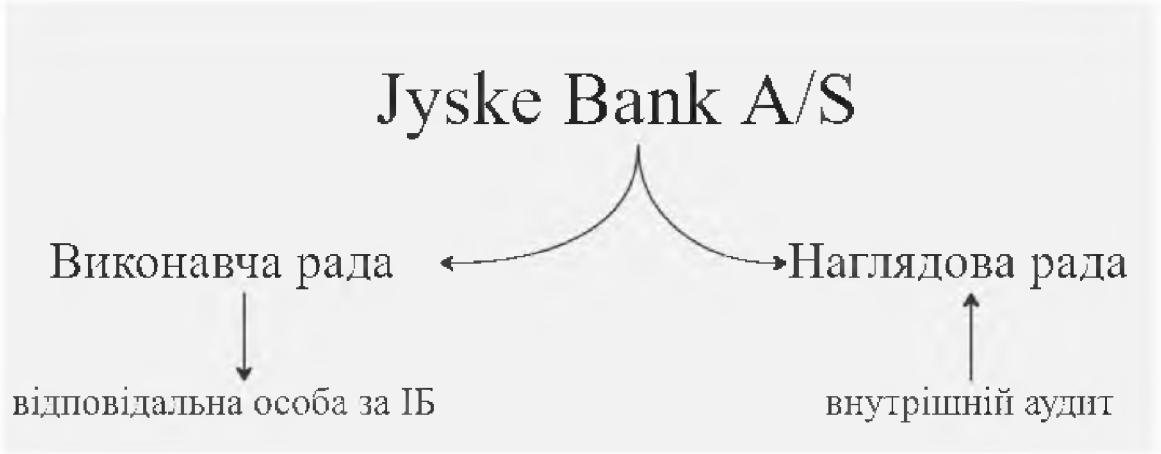

Рисунок 2.1 – Структура забезпечення ІБ у «Jyske Bank A/S».

Третій розділ – організація та обов'язки, містить інформацію про відповідальних осіб. На рисунку продемонстровано розподіл обов'язків. Виконавча рада несе загальну відповідальність за дотримання політики безпеки. Виконавча рада повинна забезпечити достатнє кадрове забезпечення служби безпеки інформації. Мінімум один член Виконавчої ради повинен володіти необхідними знаннями у галузі ІБ для забезпечення безпеки, впровадження та прийняття необхідних рішень щодо забезпечення ІБ Банку. Виконавча рада призначає відповідальну особу за ІБ.

У Банку використовується модель трьох ліній:

Перша лінія відповідає за питання, які стосуються обробки інформації та розвитку ІБ Банку, ідентифікацію, оцінку, реагування на ризики при виявленні, контролює дотримання рівня ІБ та рівні ризику. Також перша лінія готує звіти та рекомендації щодо відповідності ІБ ПІБ Банку.

Друга лінія відповідає за управління ризиками. Управління ризиками виражається у дотриманні загального рівня ризиків включно з операційними

ризиками. Управління ризиками визначає вимоги до функції безпеки щодо ефективності контролю ризиків. Функція безпеки повинна виконувати їх незалежно від організаційної приналежність до першої лінії.

Функція відповідності також здійснює контроль за дотриманням законодавства у сфері ІБ. Функція відповідності та функція управління ризиками готують звіти щодо ІБ відповідно до «Політики відповідності» та «Політики групи Jyske Bank щодо операційних ризиків».

Третя лінія складається з внутрішнього аудиту, який відповідає за проведення незалежного аудиту, загальне управління ризиками та внутрішній контроль у Групі, також звітує Наглядовій раді.

Четвертий розділ відповідає за управління ІТ ризиками. Діє «політика щодо операційних ризиків групи» згідно з цією політикою здійснюється керування ризиками.

П'ятий розділ відповідає - захисту даних. Фінансова діяльність пов'язана роботою з чутливими даними. Конфіденційні дані, які банківська група використовує під час бізнес-процесів стосується здебільшого клієнтів, а лише мала частина стосується співробітників та інших груп.

Обробка такого обсягу даних часто означатиме сильний ризик обробки персональних даних, які можуть бути неправильно оброблені, що може призвести до того, що особисті дані можуть бути розкриті неавторизованим особам. Щоб зменшити ризик, пов'язаний із обробкою персональних даних, Банк дотримується наступних принципів:

Дані надані в оренду: особисті дані не можна передавати стороннім особам, їх потрібно обробляти.

Підхід, що ґрунтується на оцінці ризику: оцінка ризику на основі того, яким ризикам піддається зареєстрована особа повинні здійснюватися для будь-яких видів обробки персональних даних, повинні бути встановлені заходи безпеки, щоб ризики, були зведені до прийнятного рівня. Якщо це неможливо, обробку необхідно припинити.

Обізнаність: усі працівники, які отримують знання про персональні дані, повинні пройти навчання та інструктаж, як обробляти персональні дані.

Мінімізація даних: лише ті дані, які необхідні для виконання мети будь-якої обробки діяльність має бути зібрана та оброблена, а також має бути зрозуміло зареєстрованій особі, для чого необхідно зібрати конкретні дані.

Конфіденційність: персональні дані мають бути доступні лише уповноваженим особам.

Цілісність: Особисті дані мають бути правильними, і їх не має бути можливою для неавторизованих осіб

Доступність: особисті дані повинні бути доступними для цілей, для яких вони були зібрані.

Шостий розділ описує вимоги, які мають бути застосовані до аутсорсингових компаній, які є постачальниками продуктів для Банку. Аутсорсингові компанії повинні бути зареєстровані та відповідати вимога цієї політики.

Сьомий розділ – принципи безпеки. Політика містить принципи безпеки, які мають додаткові інструкції:

Обізнаність – постійне навчання співробітників;

Розподіл обов'язків – ІТ операції, розвиток ІС, ведення бізнесу окремі операції, які виконує різний персонал. Критичні операції виконують декілька осіб.

Оцінка ризиків та затвердження безпеки – будь-яка система, процес тощо отримують оцінку ризиків, Особливо це стосується систем, які підтримують критичні процеси. Нові системи перед введенням в експлуатацію повинні отримати достатній рівень оцінки ризиків.

Захист ІТ-активів – активи повинні бути в задовільній мірі визначені та захищені від фізичних та логічних загроз. Сюди відносяться кіберзагрози, загрози, що виникають через несправність ІС та матимуть наслідки для клієнтів, співробітників, партнерів тощо.

Доступ до систем та даних – використовується рольова модель доступу, застосовується правило найменших ролей.

Системна розробка та обслуговування систем – повинні існувати процедури для забезпечення управління змінами. Повинні бути процедури, щоб істотні зміни та істотні ризики, пов'язані зі змінами та впровадженням визначаються, оцінюються та обробляються завчасно як невід'ємна частина на етапі розробки та тестуються перед реалізацією.

Оперативний менеджмент – у будь-який час повинні бути доступні необхідні ресурси для забезпечення безпечної роботи.

Резервне копіювання – повинні існувати резервні копії систем та даних.

Аварійне відновлення – повинен існувати план аварійного відновлення.

Тести безпеки – повинні бути проведені тести безпеки для найбільших систем. Тестування діяльності критичних системи повинні виконуватися принаймні один раз на рік, а для інших систем раз на три роки.

Управління IT-інцидентами та проблемами - необхідно визначити ефективні процедури управління інцидентами та проблемами.

Ведення журналів і моніторинг – необхідно підготувати процедури для реєстрації дій користувачів на основі оцінки ризиків, винятків, помилок, інцидентів безпеки та критичних операції.

British Business Bank (Великобританія) – державний банк економічного розвитку, створений для кредитування та консультування малих та середніх підприємств. Штаб квартира у місті Шеффілд. У Банку працює 500 осіб. Станом на 2023-й рік, активи банку досягли 2,7 мільярди фунтів стерлінгів.

ПІБ [24] складається з 7 розділів:

- мета;
- сфера застосування;
- основні вимоги;
- невідповідність;
- політика контролю;
- додаток 1: узгоджені рамки, політки, стандарти та процедури;
- додаток 2: визначення термінів

Перший розділ, описує мету, пристосування до ризику, рівень ризик-апетиту банку. Мета полягає у збереженні конфіденційності, цілісності, доступності інформації Банку. В Банку діє система управління операційним ризиком банку. Існують категорії ризиків різних рівнів, політика інформаційної безпеки належить до першого рівня ризику та узгоджується з категорією ризику другого рівня – ІБ. Ризик-апетит Банку щодо ІБ є низьким. Банк зобов'язується дотримуватися законодавства Великобританії, а саме: Закон «Про захист даних» 2018-го року, Закон «Про зловживання комп'ютером» 1990-го року, Закон «Про права людини» 1998-го року, Закон «Про регулювання слідчих повноважень» 2000-го року, Закон «Про свободу інформації» 2000-го року, Закон «Про інтелектуальну власність» 2014-го року, Загальний регламент захисту даних Великобританії (GDPR).

Згідно з другим розділом, сфера застосування політики поширюється на всю діяльність Банку, на всі філії Банку, на контрагентів Банку.

Банк обмежує доступ до своїх систем та ресурсів на основі принципу найменших привілеїв.

Також третій розділ встановлює обов'язкову поведінку для персоналу, визначаючи обов'язкові дії, щодо підтримання безпеки конфіденційності, цілісності та доступності інформації та систем, а також перелік заборонених дій.

Розділ чотири містить інформацію про дії персоналу у випадках порушення пунктів цієї політики.

П'ятий розділ містить посилання на політику контролю.

Шостий розділ розширює перелік стандартів, процедур, рамок та політик з якими вже узгоджена ця політика, або з якими процес узгодження ще триває.

В Банку функціонує Операційний центр безпеки, який є першою лінією захисту. Основними обов'язками якого є моніторинг інцидентів, а також виявлення та запобігання на інциденти в системах, ПЗ, мережах Банку. Використовує систему безпеки та керування подіями – SIEM.

Manipur State Co-operative Bank Ltd (Індія) було засновано 24 червня 1956 року. Банк розпочав банківську діяльність 24 березня 1958 року. Є головним банком штату, надає короткострокові корпоративні кредити на сезонні

сільськогосподарські операції, видає кредитні картки, середньострокові та довгострокові кредити сільськогосподарським підприємствам а також кредити готівкою чи строкові кредити, схематичне кредитування. Кількість співробітників досягає 500. Оборот Банку перевищує 225,30 крор рупій. [45]

ПІБ [23]складається з 16 розділів.

Введення – вступ до політки безпеки.

Право власності – Правління банку є власником політики та відповідає за функціонування кібербезпеки в банку.

Обсяг і застосування кібербезпеки – політика поширюється на всіх співробітників, підрядників, на всі інформаційні системи, активи, інформацію, програмне забезпечення, комп'ютерне обладнання, що пов'язане з ІС банку.

Основи політики – цілі політки: визначити надійну кібербезпекову структуру для захисту інформації; заходи та контроль за цією структурою; реагування та вирішення кіберінцидентів, відновлення після кіберінцидентів.

Керівний принцип – підхід Банку до кібербезпеки базується на принципах: відповідальності за захист конфіденційної інформації клієнтів, систем та мереж, зберігання властивостей інформації; особи несуть відповідальність за забезпеченням безпеки власних інформаційних систем; для захисту особистої та приватної інформації заохочуються суворі заходи безпеки.

Політична заява – банк буде прагнути до збереження конфіденційності цілісності та доступності інформаційних активів Банку.

Мета – захист інформаційної структури Банку.

Ролі та обов'язки – є відповідальна особа за ІБ, він же керівник відділу інформаційних технологій.

На рівні правління ІТ-підкомітет складається з головного виконавчого директору банку, три члени з правління, керівник ІТ осередку. Комітет збирається не рідше одного разу на квартал.

Керівний комітет ІТ – складається з представників ІТ HR юридичного відділу, відділу позик та авансів, бухгалтерського обліку. Комітет допомагає

виконавчому керівництву у впровадженні ІТ-стратегії, яку схвалює ІТ-підкомітет Правління.

Комітет з ІБ формується з керівників, вищих посадових осіб керівництва, основні обов'язки це розробка політик, стандартів і процедур ІБ.

Відділ інформаційних технологій забезпечує підтримку та послуги ІТ-продуктів підрозділам, надає підтримку іншим підрозділам щодо досягнення цілей та планів кібербезпеки.

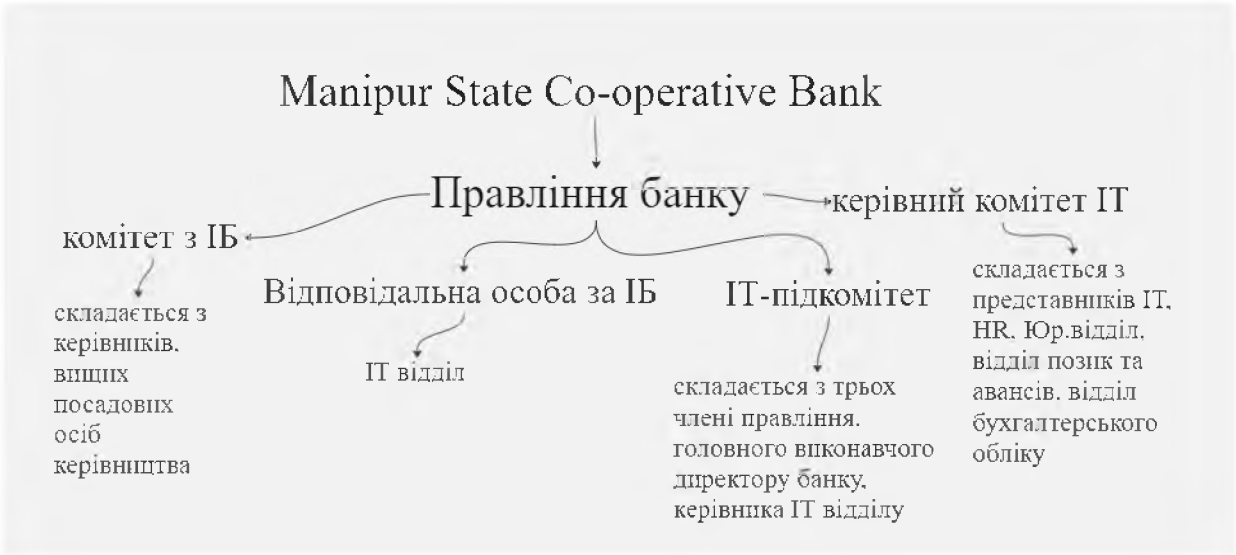

Рисунок 2.2 – Структура забезпечення ІБ у «Manipur State Co-operative Bank».

Юридичний відділ консультує з юридичних питань.

Філії та персонал повинні виконувати вимоги Банку щодо управління інформаційними ризиками.

Третя сторона повинна дотримуватися політик Банку щодо кібербезпеки.

Підхід до впровадження полягає у чотирьох пунктах:

a) план управління кіберкризою банку повинен охоплювати ефективні заходи запобігання кібератакам та своєчасне виявлення кібервторгнень;

b) відповідні посадові особи відділу ІТ повинні вжити кроків, щоб досягти прогрес в досягнені мети кібербезпеки.

c) визначити та захистити інформаційну інфраструктуру кібернетичного зв'язку банку;

d) реагування та відновлення після кіберінцидентів.

Навчання з питань кібербезпеки – банк вживає заходів для підвищення обізнаності персоналу щодо кібербезпеки.

Звітування та вимірювання ефективності – необхідність проведення регулярної оцінки для виявлення потенційних загроз, а також щоквартального звіту про інциденти кібербезпеки повинні подаватися Правлінню Банку.

Перегляд і затвердження політики – документ повинен переглядатися щорічно.

Відповідність – всі співробітники банку несуть відповідальність за дотриманням політики безпеки.

Винятки – IT комітет схвалює винятки та відхилення від політики.

Запити – будь-які запити, щодо застосування політики слід направляти керівнику IT-підрозділу.

Домени кібербезпеки – в розділ описується наміри банку, щодо керування запасами IT-активів, запобіганню доступу несанкціонованому ПЗ, екологічний контроль, мережевий менеджмент та безпека, контроль доступом користувачів, антивірусна політика, політика змінних носіїв, використання електронної пошти та системи обміну повідомленнями, управління ризиками аутсорсингу, оцінка вразливостей та тестування на проникнення, резервне копіювання та відновлення, моніторинг транзакцій на основі ризику та реагування на інциденти та управління кіберкризою.

Taiwan Business Bank (Тайвань) – провідний банк Тайваню, є міжнародною банківською фінансовою установою з штаб-квартирою в Тайбеї. Має 129 відділень на Тайвані та 7 у світі. Банк зосереджується на великих корпоративних клієнтах та фінансуванні міжнародної торгівлі основні напрямки роботи: оптові банківські послуги, комерційні позики, депозитарії, безпека та траст і капітальне фінансування. Кількість співробітників 5639. Активи банку 73 мільярди тайванських доларів. [44]

ПІБ банку [20] називається «Політика кібербезпеки» та складається з 15 стисло викладених статей.

Стаття 1 декларує Банком встановлення цієї Політки для забезпечення безпеки інформаційно-комунікаційних систем та інформаційних активів Банку, зниження операційних ризиків та для покращення загальної архітектури кібербезпеки Банку.

Стаття 2 – значення термінів, що згадуються в цій політиці.

Стаття 3 – загальна мета кібербезпеки полягає в забезпечення збереження властивостей інформації в інформаційно-комунікаційних системах та інформаційних активах.

Стаття 4 – сфера дії політики.

Стаття 5 – створюється Комітет з управління кібербезпекою для управління та наглядом за процедурами забезпечення кібербезпеки.

Стаття 6 – зобов'язання Банку дотримуватися законодавства.

Стаття 7 – Банк встановлює механізми контролю за результатами оцінки ризиків, а також здійснює належне управління запасами ІКС та інформаційних активів.

Стаття 8 – Банк розробляє план підтримки рівня кібербезпеки, механізми реагування на кіберінциденти.

Стаття 9 – Банк проводить тренінги та навчання для персоналу.

Стаття 10 – Банк має впроваджувати системи управління.

Стаття 11 – департамент ІБ раз на рік перевіряє політики.

Стаття 12 – серйозні оновлення конфігурації ІКС неможливі без звітності для Ради директорів.

Стаття 13 – Банк дотримується трьох ліній захисту. Перша лінія – відділи адміністрування та використання ІКС. Друга лінія – департамент інформації та безпеки. Третя лінія – відділ аудиту.

Стаття 14 та 15 – питання, які не охоплює ця політика безпеки вирішуються іншими нормативно-правовими актами. Політики набирають чинності після затвердженням Радою директорів.

Stanbic Bank Uganda (Уганда) – найбільший комерційний банк країни, загальні активи банку станом на 31 грудня 2023-го року оцінювалися трохи більше

2,5 мільярди доларів США. Банк має штаб-квартиру у Кампалі, кількість працівників 1907. Основні види послуг: інтернет-банкінг, мобільні гроші, кредитування малого та середнього бізнесу, кредитні та дебетові картки. Банк має 81 відділення, став першим комерційним банком країни, що отримав стандарт відповідності стандарту ISO/IEC 27001:2013. [33, 34]

Політика інформаційної безпеки Банку [21] створена на основі вимог стандарту ISO/IEC 27001:2013 та включає цілі ІБ, необхідні для конфіденційності, цілісності та доступності інформаційних активів від зовнішніх та внутрішніх загроз пов'язаних з обробкою конфіденційної банківської та клієнтської інформації. Політика декларує цілі та заходи на яких базується банк під час забезпечування ІБ:

– дотримання законодавчих вимог;
– поширення обізнаності серед персоналу;
– періодичний перегляд та оновлення операційних процедур;
– управління та контроль сеансів дистанційної роботи;
– розробка плані ведення безперервної діяльності бізнесу стосовно ІБ;
– створення та впровадження засобів контролю інформаційної безпеки;
– постійне вдосконалення системи управління інформаційною безпекою через проведення постійних перевірок вимірюваних цілей безпеки.

Дана політика є обов'язковою до виконання персоналом Банку. А керівництво Банку зобов'язується постійно вдосконалювати систему управління інформаційною безпекою.

Chang Hwa Bank (Тайвань) – тайванська фінансова установа, яка пропонує роздрібні послуги приватним і корпоративним клієнтам. Банк має 175 внутрішніх філій та 7 закордонних станом на 2008 рік. Штаб-квартира - Тайчжун. Кількість працівників 6 592. Активи: 2,74 мільярди доларів США. Банк пропонує наступні послуги:

– депозити;

– корпоративні/інституційні банківські послуги;
– роздрібні/споживі банківські послуги;
– кредитні картки;
– іноземні валюти та грошові перекази;
– електронний банкінг;
– фінансові трасти;
– інвестиції. [35]

ПІБ [19]складаються з 5 розділів:

– політика та зобов'язання;
– структура управління інформаційною безпекою;
– механізм звітування про безпеку;
– заходи безпеки та механізми управління;
– статус реалізації.

Мета ПІБ: посилення управління ІБ, забезпечення властивостей інформації, забезпечення безпеки бізнес-процесів.

Для забезпечення контролю за ІБ діє система управління з трьома лініями захисту: перша лінія – всі підрозділи Банку та ІТ відділ забезпечують ІБ; друга лінія – відділ ІБ відповідає за впровадження ПІБ та звітує перед Комітетом з управління ризиками щомісяця; третя лінія – відділ внутрішнього аудиту. Призначений директор з ІБ на рівні виконавчого віце-президента. Директор відділу ІБ є спеціальним інспектором з ІБ, щороку звітує перед Радою директорів. У Ради директорів є консультант з ІБ.

У Банку розроблений та функціонує механізм звітування про події інформаційної безпеки «Процедури звітування про події інформаційної безпеки» а також «Процедури розгляду великих непередбачуваних інцидентів Банку» згідно з цими документами відділи ІТ та ІБ повинні відслідковувати, усувати та вирішувати інциденти ІБ, пропонувати превентивні заходи для недопущення повторення даних ситуацій, а також пропонувати плани вдосконалення систем ІБ.

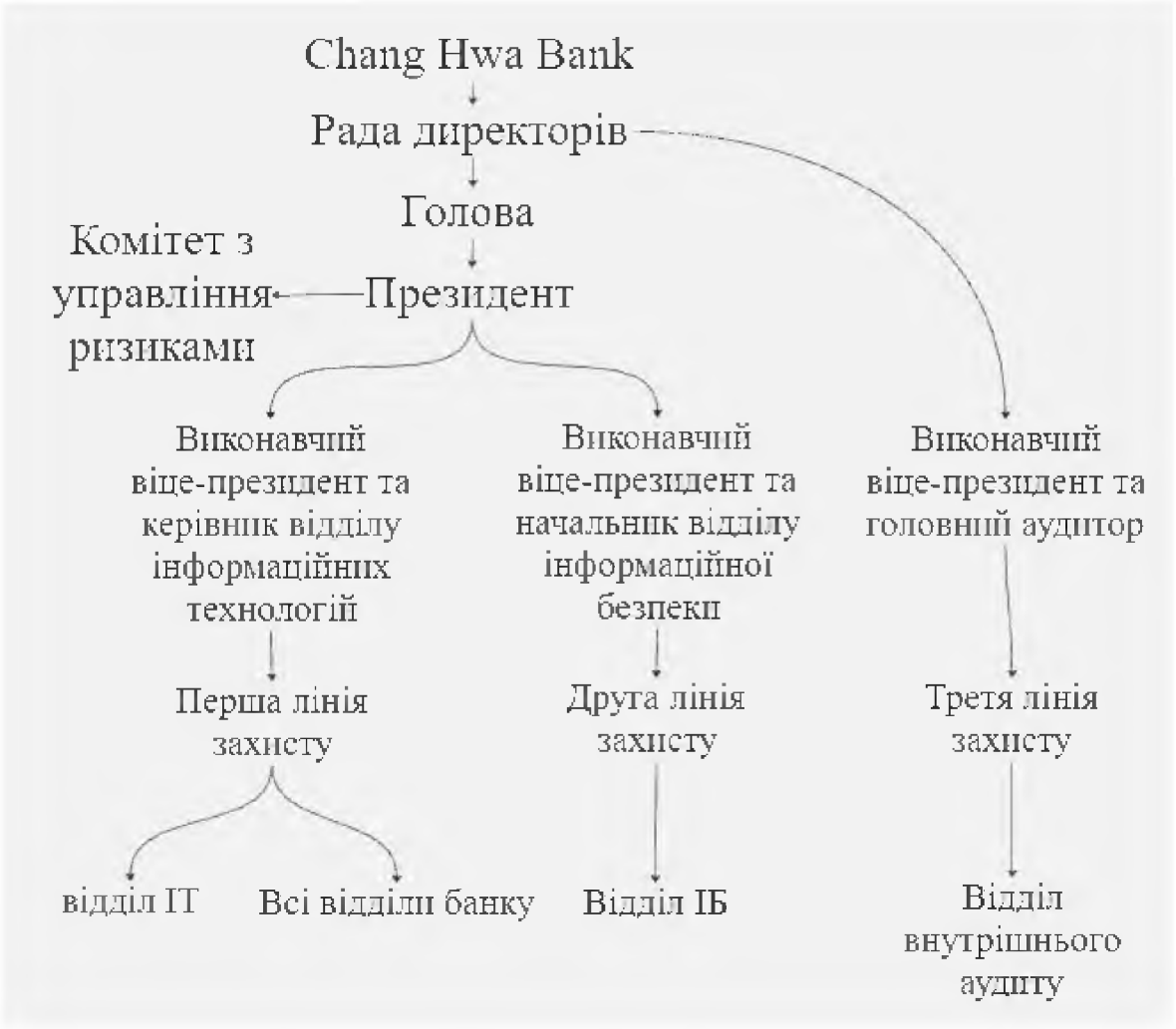

Рисунок 2.3 – Структура управління ІБ у «Chang Hwa Bank»

Банк щорічно замовляє проведення оцінки ІБ у незалежних аудиторів. Банк проводить тестування на проникнення у мобільному додатку, проходить перевірку ІБ від Промислового бюро Міністерства економіки, щороку підтверджує відповідність міжнародним стандартам «Системи управління безперервністю бізнесом ISO 22301», «Системи управління інформаційною безпекою ISO 27001», «Системи управління персональною інформацією BS 10012». Використовується багаторівневе обладнання ІБ для спільної роботи, яке створює механізми захисту мереж, баз даних та серверів. Запроваджений механізм двофакторної автентифікації, регулярне проведення сканування вразливостей та тестів на проникнення.

2.1.2 Огляд політик безпеки інформації в українських компаніях у фінансовій сфері.

Вибрано 5 компаній, що ведуть свою діяльність у фінансовій сфері, а саме банки. Згідно з офіційним інтернет ресурсом національного банку Україні вибрано 5 системно важливих банки, це АБ «Укргазбанк», АТ «Кредобанк», АТ «Таскомбанк», АТ «Ощадбанк», АТ «ПриватБанк». [18]

АТ «Ощадбанк» - український комерційний банк, другий банк України за активами. Станом на 2023-й рік має 1183 відділень, близько 249 мільярдів гривень активів. Штаб-квартира розташована у Києві. Один з 15-ти системи важливих банків за оцінкою НБУ. Кількість співробітників близько 29 тис. людей. Піддався на кібератаки зі сторони РФ 15-го лютого 2022-го року, через що кілька годин не працював офіційний сайт. Основні види діяльності:

a) кредитування підприємств;

b) обслуговування боргів державних підприємств;

c) видача кредитних та дебетових карток;

d) онлайн-банкінг. [41, 42]

Політика інформаційної безпеки в АТ «Ощадбанк» [28] складається з 12 розділів:

- загальні положення;
- терміни, скорочення та їх визначення;
- тема, завдання, принципи та межі застосування політики;
- ролі та відповідальності;
- цілі забезпечення інформаційної безпеки;
- принципи забезпечення інформаційної безпеки;
- забезпечення реалізації політики;
- контроль у межах систем внутрішнього контролю;
- порядок перегляду документу;
- прикінцеві положення;
- перелік пов’язаних документів;
- історія змін.

В першому розділі розповідається згідно з якими нормативно-правовими документами, стандартами, положеннями створена ця політика й дається визначення, що таке ПІБ АТ «Ощадбанк».

Другий розділ регулює визначення термінів та скорочень, які використовуються в цій політиці.

Третій розділ визначає мету політики, завдання забезпечення інформаційної безпеки Банку, межу дії політики, принципи на яких базується дана політика, перелік людей та персоналу, на яких діють вимоги, які встановлені в цьому документі.

Четвертий розділ – ролі та відповідальності. З цього розділу слідує, що керівництво Банку розуміє важливість забезпечення інформаційної безпеки Банку, сприяє створенню та впровадженню цілей та принципів інформаційної безпеки. Створюється Комітет СУІБ. Процес управління ризиками інформаційної безпеки у складі СУІБ є забезпечення захисту інформаційних активів Банку від можливих загроз різного типу дії.

У рамках СУІБ Банк впроваджує ризик-орієнтовний підхід. Згідно з яким:

Наглядова рада Банку:

– забезпечує функціонування та здійснює контроль за СУІБ;

– затверджує показники ризик-метрики та ліміти ризику;

– затверджує критерії прийняття та ідентифікації ризиків та їх рівнів.

– Комітет з управління ризиками:

– надає рекомендації та пропозиції наглядовій раді банку щодо управління ризиками ІБ;

– здійснює моніторинг впровадження стратегії Банку з ІБ;

– контролює стан виконання заходів з усунення недоліків, стан виконання рекомендацій та зауважень від зовнішніх й внутрішніх аудиторів, НБУ тощо.

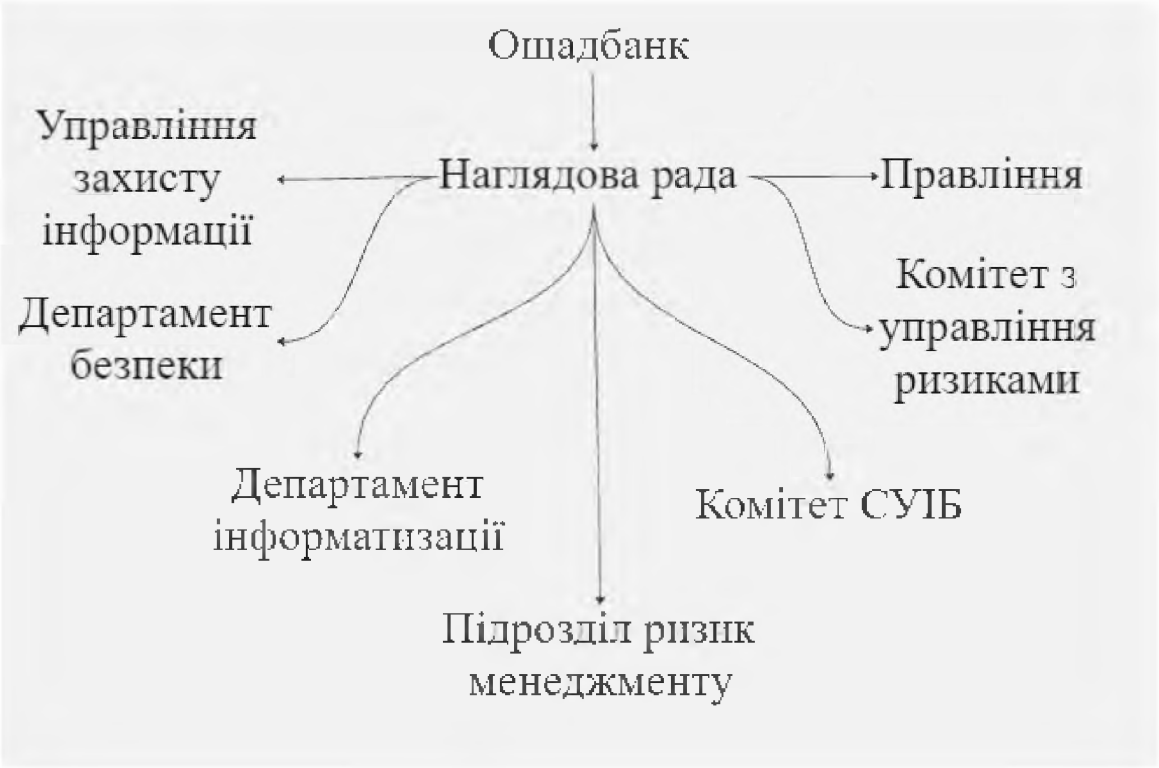

Рисунок 2.4 – Структура СУІБ в АТ «Ощадбанк»

Правління Банку й відповідальна особа за ІБ Банку:

– визначає принципи та завдання ІБ;

– визначає рівень ризику та прийняття залишкових ризиків;

– інформує наглядову раду Банку про рівень ризиків;

– забезпечує тестування та перегляд заходів ІБ;

– забезпечує ресурси для УІБ та її відповідності нормативно-правовим актам;

– забезпечує розроблення та затверджує внутрішні документи з ІБ; сприяє розслідуванню інцидентів ІБ та розробленню методології оцінки ризиків ІБ.

Комітет СУІБ:

– погоджує та переглядає ПІБ, стратегії розвитку ІБ, проекти вдосконалення СУІБ Банку;

– визначає необхідні ресурси для функціонування заходів ІБ;

– організовує практичні тренінги та інші заходи щодо навчання персоналу Банку з питань ІБ;

– забезпечує розробку та впровадження плану безперервності функціонування заходів ІБ у рамках процесу управління безперервної діяльності Банку.

Підрозділ ризик менеджменту:

– бере участь у дослідження інцидентів ІБ, та у розробці ризик апетиту щодо ризиків ІБ;

– контролює показники ризик-апетиту, лімітів ризику.

Також четвертий розділ встановлює відповідальність згідно посадових інструкцій для адміністратора інформаційного ресурсу і для адміністратора захисту інформації з забезпечення контролю за станом інформації, аналізу вразливостей інформаційних систем, експлуатації та технічного обслуговування системи, забезпечення технічної підтримки користувачам, забезпечення резервування ПЗ, а також бере участь у розслідуванні інцидентів ІБ. Для керівників структурних підрозділів, власників інформаційних активів керівників філій та територіально відокремлених відділень Банку, працівників Банку та користувачів ІС Банку, контрагентам встановлюються відповідальність та обов'язки.

Департамент безпеки, Департамент управління захисту інформації, Департамент Інформатизації забезпечують управління окремими складовими СУІБ, впровадження засобів захисту та виконання заходів безпеки Банку.

У п'ятому розділі, описуються цілі забезпечення ІБ через забезпечення властивостей інформації: конфіденційність, цілісність, доступність, спостережність.

Шостий розділ містить принципи забезпечення інформаційної безпеки:

Мінімальність повноважень – принцип найменших ролей, тільки ті, що необхідні для виконання службових обов'язків.

Явне санкціонування дій – принцип заборони всіх дій, що не дозволенні в нормативних чи внутрішніх розпорядних документах.

Законність – принцип дотримання вимог законодавства України а також міжнародних нормативно-правових документів у галузі.

Узгодженість – принцип відповідності цілей та завдань ІБ з цілями та завданнями Банку.

Єдність – принцип невід'ємності управління Банком з управлінням ІБ.

Ефективність – принцип впровадження засобів захисту відповідно до оцінки та управління ризиком та критичністю ресурсу.

Практичність – принцип дотримання балансу засобами захисту між працездатністю та захищеністю інформаційних систем.

Безперервність – принцип безперервного захисту через сферу діяльності Банку.

Відповідальність – всі користувачі, керівництво та треті сторони несуть персональну відповідальність за виконання нормативно-правових актів Банку та повинні дотримувати їх вимоги.

Принцип постійного удосконалення – принцип контролю показників ефективності кожного процесу забезпечення ІБ.

Потайність – принцип виключення можливості ознайомлення сторонніх осіб з технічними чи організаційними засобами захисту.

Принцип захисту в глибину – принцип створення послідовних рівнів захисту інформаційних ресурсів та персоналу Банку. Організаційно-правовий рівень, фізичний рівень, рівень прикладного ПЗ, рівень СУБД, рівень ОС, рівень мережі.

Комплексність та системність – принцип взаємодії всіх підрозділів Банку та забезпечення ІБ на правовому, адміністративному, організаційному, програмному, технічному рівнях.

Сьомий розділ, містить реалізацію політики.

Восьмий розділ вводить рівні контролю процесу.

Дев'ятий розділ містить порядок змін та перегляду документу.

Десятий розділ – прикінцеві положення.

Одинадцятий розділ – перелік пов'язаних документів.

Акціонерне товариство «КРЕДОБАНК» - український банк з штаб-квартирою у Львові. Активи банку становлять станом на 1 січня 2024 55,8 мільярди гривень, має 68 відділень та 1500 осіб співробітників. Основні напрями

діяльності: інвестування, кредитування, випуск кредитних та дебетових карток, онлайн банкінг. [40]

Документ [27] «Вимоги Політики інформаційної безпеки в АКЦІОНЕРНОМУ ТОВАРИСТВІ «КРЕДОБАНК»» Складається з п'ятнадцяти пунктів, які мають описовий, декларативний характер та відповідають за систему цінностей Банку, цілі інформаційної безпеки, принципи забезпечення інформаційної безпеки, вимоги до ПЗ та виклад опису дій Банку для забезпечення кібербезпеки Банку, деякі обов'язки працівників, та зобов'язання щодо нерозголошення інформації з обмеженим доступом, в тому числі персональних даних та банківської таємниці.

Четвертий та п'ятий пункти складають цілі ІБ та основні принципи забезпечення ІБ.

Цілі ІБ:

– відповідність до вимог законодавства;
– доступність інформації;
– конфіденційність інформації;
– цілісність інформації;
– спостережність;
– застосування принципів захищеної обробки інформації;
– нагляд за захистом інформації;
– адекватний захист інформації та засобів обробки згідно з рівне ризику;
– адекватна оптимізація засобів захисту відповідно до поточних потреб банку;
– забезпечення швидкої та ефективної реакції на порушення ІБ.

Принципи ІБ:

– принцип мінімальності повноважень – надаються тільки ті повноваження, які необхідні;
– принцип необхідних знань – кожен працівник володіє тільки необхідною інформацією для виконання поставлених завдань;

– принцип розподілу обов'язків – виконання задач, які є критичними з точки зору безпеки організовуються з двома чи більше особами;

– принцип санкціонування дій – можна робити тільки те, що дозволено;

– принцип законності – СУІБ Банку враховує вимогу НПА України, НБУ тощо;

– принцип узгодженості та єдності – цілі і завдання ІБ відповідають бізнес-завдання Банку;

– принцип адекватності та ефективності – засоби захисту впроваджуються на основі аналізу ризиків та критичності інформаційних ресурсів;

– принцип практичності – засоби захисту підтримують баланс між захистом на швидкодією;

– принцип безперервності – інформаційна безпека є безперервним процесом;

– принцип відповідальності – керівництво, персонал та треті особи відповідають за свої вчинки та повинні дотримуватися правил, установленими Банком;

– принцип постійного вдосконалення – СУІБ постійно вдосконалюється й містить показники для оцінки ефективності;

– принцип багаторівневого захисту – встановлені рівні захисту на всіх рівнях, а саме організаційний, фізичний, рівень прикладного ПЗ, СУБД, ОС, рівень мережі;

– принцип комплексності та системності – ІБ Банку будується комплексно, враховуючи стратегії та цілі інфомраціфйної безпеки, управлінню носіями інформації та ресурсами, безпека персоналу, процесів, безпека проектування та експлуатації систем, ведення безперервності захисту інформації.

АТ «Таскомбанк» - український банк заснований у 1989 році. Головний офіс у Києві, 1925 співробітників. Згідно з офіційним сайтом банку має 101 відділення по всій Україні, активи трохи менше 32,3 мільярдів гривень. Основні

напрями діяльності: кредитування, лізинг, інвестування, мобільний банкінг, страхування. [39]

Політика інформаційної безпеки банку набула чинності 26.01.2024, через що ця політика автоматично стає найновішою в цьому аналізі.

ПІБ [25] складається з 11 розділів серед яких:

- загальні положення;
- глосарій;
- мета, цілі та завдання політики;
- сфера застосування політики;
- засади управління інформаційною безпекою;
- принципи управління інформаційною безпекою;
- модель загроз та модель порушника;
- кіберзахист критичної інформаційної інфраструктури;
- аудит стану інформаційної безпеки;
- відповідальність за реалізацію політки;
- заключні і перехідні положення.

Перший, десятий та одинадцятий розділи не містять чогось принципово нового, але другий розділ «Глосарій» виділяється наявністю визначень «об'єкт критичної інфраструктури в банківській системі Україні (ОКІ)», «MISP-NBU Центр кіберзахисту» та «Робоча група». Ці визначення використовуються, бо в політиці наявний розділ, що відсутній у підприємств-конкурентів, чиї політики безпеки були проаналізовані, це розділ «Кіберзахист критичної інформаційної інфраструктури». Робоча група – колективний керівний орган управління СУІБ, до його складу входять Заступник Голови Правління, керівників підрозділів критичних бізнес-процесів, а також керівник підрозділу з управління ризиками.

Третій розділ визначає мету політики, цілі, на досягнення яких вона спрямована та основні завдання.

Четвертий розділ – сфера застосування політики, де визначаються об'єкти регулятивного плану, це об'єкти на які розповсюджується дія політики та регулятивний вплив. Серед них є:

– інформаційні ресурси – інформація, що обробляється, зберігається та передається;

– програмне забезпечення – прикладне, системне або сервісне ПЗ, яке використовується працівниками та системами для взаємодії;

– фізичні ресурси – виробничі приміщення та технічні засоби;

– сервісні ресурси – обчислювальні та комунікаційні сервіси;

– кадровий ресурс – персонал банку;

– треті сторони – фізичні та юридичні особи, які є стороною відносин з Банком.

Інформаційними активами є персонал, інформаційні системи, інформація в електронному вигляді та на паперових носіях, яка використовується у діяльності ІС та зберігається на всіх етапах життєвого циклу.

Також згідно з цим розділом, кожен інформаційний актив – має власника, який затверджується розпорядчим документом Банку та є начальником структурного підрозділу, який ініціював його створення.

П’ятий розділ – засади управління інформаційною безпекою. Управління інформаційною безпекою організовано у єдину систему СУІБ. Також цей розділ встановлює вимоги до функціонування Банку з залученням СУІБ та підтримкою забезпечення захисту інформації, обов’язки персоналу тощо.

У шостому розділі містяться принципи управління інформаційною безпекою, які складаються з:

– належності ресурсів;

– персональної відповідальності;

– колегіальної участі;

– виправданості витрат;

– достатньої компетенції;

– системної діяльності;

– розподілу прав доступу;

– забезпечення безперервності.

Сьомий розділ містить модель загроз та модель порушників. Модель порушника складає аналіз типу порушника, його вірогідні знання, повноваження, можливості та дії.

Восьмий розділ про кіберзахист критичної інформаційної структури містить інформацію, про процес кіберзахисту ІС, банк є учасником інформаційного обміну і згідно з ДСТУ ISO/IEC 27010:2018 під час обміну, маркує електронні повідомлення спеціальними мітками, Банк підключений до MIPS-NBU. У Банку визначаються перелік об'єктів критичної інформаційної інфраструктури, а також зазначається що зв'язок між об'єктами та мережею інтернет здійснюється з використанням захищених вузлів доступу через два чи більше каналів зв'язку, які надаються різними провайдерами.

Аудит стану інформаційної безпеки – дев'ятий розділ. Аудит відбувається регулярно відповідно до вимог законодавства. За результатом аудиту департамент інформаційної безпеки передає НБУ дані про результати аудиту, а також план дій з усунення виявлених недоліків.

АТ «ПриватБанк» - найбільший український банк та лідер банківського ринку. Станом на 2022-й рік має більше 1200 відділень. Штаб-квартира знаходиться у Дніпрі. 15-го лютого 2022-го року в результаті кібератаки офіційний сайт банку декілька годин був недоступним. Станом на 2021-й рік загальні активи більше 376 мільярдів гривень. Кількість працівників більше 22 тисяч.[37, 38]

Політика інформаційної безпеки АТ «ПриватБанк» [26] містить 9 розділів, зрозуміла структура документа, подібна до інших політик безпеки українських банків. Але є деякі нововведення, серед яких, трирівнева модель управління ризиками, де перша лінія – бізнес підрозділи, які є власниками всіх операційних ризиків, друга лінія – департамент управління операційними ризиками, який керує всією системою управління ризиками, третя лінія – внутрішній аудит, який контролює попередні лінії. Відповідно до організаційної структури підрозділ, що відповідає за ризики ІБ відноситься до першої лінії та звітує керівному органу щодо управління ризиками.

СУІБ складається з наглядової ради, комітету з питань технологій, даних та інновацій наглядової ради, правління, комітет управління операційними ризиками на інформаційної безпеки, відповідальний за інформаційну безпеку.

Наглядова рада затверджує план забезпечення безперервної діяльності Банку, внутрішні документи, які регламентують діяльність підрозділу з ІБ, розглядає звіти комітету з питань технологій, щодо ІБ.

Комітет з питань технологій, даних та інновацій надає консультації Комітету Наглядової ради з питань ризиків ІБ.

Правління забезпечує функціонування СУІБ, безпеку інформаційних систем; визначає відомості, що становлять комерційну таємницю про діяльність Банку.

Комітет з управління операційними ризиками та ІБ функціонує як колективний керівний орган для забезпечення ефективності управління ризиками та систем контролю. Також комітет переглядає ПІБ, контролює процеси щодо вдосконалення СУІБ, забезпечує моніторинг функціонування СУІБ.

Відповідальний за інформаційну безпеку забезпечує керівництво з питань ІБ Банку.

Також у цьому розділі описані напрямки роботи підрозділів Банку у питання ІБ, це напрямок інформаційної безпеки, підрозділ інформаційних технологій, дирекція з HR та корпоративного управління, служба безпеки, управління із захисту персональних даних, департамент управління операційними ризиками, напрям «compliance», напрямок правової підтримки.

Згідно з політикою управління інформаційними ризиками здійснюється за основними принципами: трирівнева модель управління ризиками; процедура управління ризиком ІБ; забезпечення високого рівня практичних навичок персоналом Банку та високого рівня обізнанності щодо ризиків ІБ.

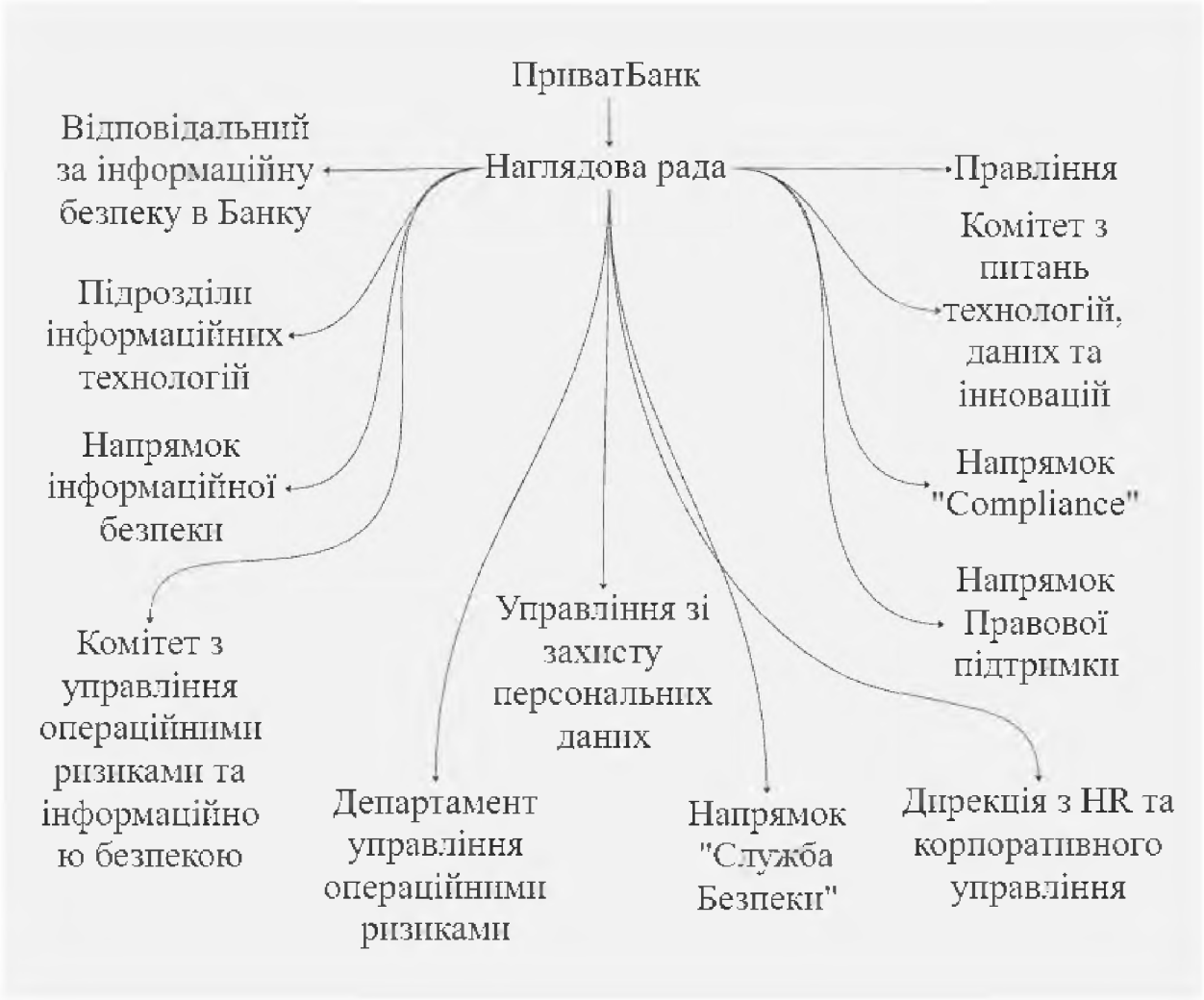

Рисунок 2.5 – Структура СУІБ у АТ «ПриватБанк»

Управління інцидентами щодо ІБ здійснюється послідовна оцінка, своєчасне інформування, впровадження оцінка та моніторингу вразливостей ІБ.

Під час управління та моніторингу ІБ створюються групи реагування на інциденти та створюється центр операційний центр безпеки.

У сьомому розділі – принципи та вимоги інформаційної безпеки, описані основні принципи: системний підхід; безперервність удосконалення ІБ; своєчасність заходів захисту; контроль за забезпеченням ІБ від керівництва; достатність ресурсів для розвитку ІБ. Також Банк розробляє внутрішні документи на теми процесу управління ключами, оновленнями, вимоги до використання корпоративної пошти, криптографічних засобів захисту, захист від зловмисного коду, вимоги до апаратних та програмних засобів.

Напрямок ІБ кожен рік надає для правління звіт з оцінки впливу ІС на діяльність Банку. Оновлення політики відбувається не рідше ніж один раз на рік.

АБ «УКРГАЗБАНК» - український банк з власністю держави в 94,94%. Штаб-квартира розташовується у Києві. Активи трохи більше 176 мільярдів гривень. Основні напрями діяльності: інтернет банкінг, кредитування, кредитні та дебетові картки. [35, 36]

Політика інформаційної безпеки АБ «УКРГАЗБАНК» [29] складається з шести розділів:

– загальні положення;
– визначення термінів;
– ціль документа та сфера застосування;
– предмет документу та опис дій;
– відповідальність;
– прикінцеві положення.

Ціллю є впровадження та ефективне функціонування СУІБ, що буде забезпечувати надійне функціонування, захист, мінімізацію ризиків та безперервну діяльність Банку. Банк використовує ризик-орієнтований підхід.

Принципи ІБ є підтримування захисту ІБ через захист властивостей інформації: цілісності; конфіденційності; доступності. Для кожного ресурсу визначаються інформаційні ризики

Об’єкти, які входять до ресурсів СУІБ:

– програмне забезпечення;
– ІТ-сервіси;
– інженерна інфраструктура;
– об’єкти;
– персонал;

Політика обов’язкова до виконання всіма працівниками. Політика базується на нормативно-правових актах, законодавства, регулятора, а також на актах внутрішнього регулювання з ІБ. Банк створив та використовує наступні підходи до забезпечення ІБ:

- перелік відомостей, що містять ІзОД;
- перелік критичних бізнес-процесів;
- правила доступу до інформаційних ресурсів, ПЗ та технічних засобів;
- парольний та антивірусний захист сервісних і програмних ресурсів;
- контроль мережі, захищений доступ до ресурсів мережі;
- інвертеризація ресурсів;
- внутрішні аудити, моніторинг та вдосконалення СУІБ;
- криптографічний захист інформації.

Банк розробив та оновлює план забезпечення безперервної діяльності Банку, план безперервного та відновлення функціонування ІС; забезпечує функціонування критичних бізнес-процесів; план забезпечення безперервної діяльності дирекцій та відділень Банку.

Розділ п'ять – відповідальність. У банку створений Комітет з питань управління інформаційною безпекою, Департамент інформаційної безпеки відповідає за політики безпеки, контроль, виконання, та підтримка їх в актуальному стані.

2.2 Переваги й недоліки.

Для початку аналізу потрібно визначити, які загрози існують для фінансових установ. З праці Заросило В.О. «Загрози фінансовій безпеці та їх класифікація» можна поділити загрози фінансовим організаціям на дві великі категорії: суб'єктивні та об'єктивні. Об'єктивні загрози – загрози, які не можуть бути передбачені та прогнозовані, ці загрози здебільшого мають великий вплив на діяльність людей і навіть на ціле суспільство. До об'єктивних загроз відносять стихійні лиха (землетруси, повені, цунамі, ураган, виверження вулканів, засухи, аномально низькі чи високі температури) а також інші природні явища, які мають великий вплив на діяльність людини та запобігання, яким вимагає великих витрат матеріальних ресурсів. Суб'єктивні загрози – загрози, які виникають через діяльність людей. Можна виокремити загрози, які виникають від діяльності людини, вони бувають зовнішні та внутрішні відносно підприємства. Зовнішні поділяють на загальноекономічну кризу, виникнення нестабільності нормативно-правової бази, брак коштів для операційної діяльності підприємств, низький

рівень інвестицій, викрадення інформації, недобросовісна конкуренція, тиск правоохоронних органів. [30]

Внутрішні можна поділити на три рівні: перший рівень – організаційні ризики, які пов'язані передусім з організацією роботи на підприємстві, наприклад розголошення комерційної та банківської таємниці, низка дисципліна праці, неефективне управління підприємством та його ресурсами; другий рівень - недоліки планування та стратегії діяльності підприємств, помилкове планування стратегії розвитку, розширення та ведення бізнесу, жахлива цінова та маркетингова політика, неефективність внутрішнього аудиту; третій рівень – технічні ризики, які пов'язані насамперед з працездатністю обладнання. [30]

Політики інформаційної безпеки спрямовані в першу чергу на вирішення чи зменшення вірогідного негативного впливу від суб'єктивних загроз тобто управління ризиком, зменшення та прийняття. ПІБ вирішують питання взаємодії персоналу, створюючи заборони та встановлюючи обов'язкові дії, які зменшують ризики пошкодження, руйнування або витоку інформації в системах підприємств.

Політики безпеки інформації українських та іноземних банків з Китайської республіки та Уганди мають дуже багато відмінностей, зокрема в структурі документів. «Taiwan Business Bank», «Chang Hwa Bank» «Uganda Stanbic Bank» мають декларативні політики інформаційної безпеки, вся політика складається з намірів, цілей та принципів, майже без реальних кроків досягнення пунктів цієї політики, що є недоліком, бо порівняно з іншими політиками ІБ, там є опис та порядок дій банку/персоналу на випадок тих чи інших ситуацій, а декларативні політик інформаційної безпеки не відображають реального плану дій, що підриває довіру інвесторів до цих банків. З позитиву можна виділити, що в політиці інформаційної безпеки тайванських банків «Taiwan Business Bank» та «Chang Hwa Bank» міститься інформація, що банки дотримуються принципу трьох ліній захисту для забезпечення виконання процедур щодо ефективності кібербезпеки банку та забезпечення управління ризиками. Перша лінія захисту – відділи адміністрування та використання інформаційно-комунікаційних систем, які

відповідають за розробку та впровадження механізмів безпеки, друга лінія захисту – Департамент інформації та безпеки, який відповідає за планування, моніторинг та виконання методів управління кібербезпекою, третя лінія захисту – відділ аудиту, який відповідає за проведення незалежного аудиту механізмів кібербезпеки. Серед оглянутих політик інформаційної безпеки, в іноземних банках, таких як: «Jyske Bank A/S» (Данія), «Chang Hwa Bank» (Тайвань) та «Taiwan Business Bank» (Тайвань), а також в українському банку АТ «ПриватБанк» функціонує та впроваджена модель трьох ліній захисту, що є суттєвою перевагою над іншими банками. В інших банках політки безпеки не містять згадки про модель трьох ліній. В Україні діє Постанова Правління Національного банку України «Про внесення деяких змін до деяких нормативно-правових актів Національного банку України» №40, яка регламентує управління ризиками в банках України, та яка вимагає впровадження моделі трьох ліній захисту. До першої лінії захисту належать структурні елементи банку, які під час своєї діяльності виконують вимоги політик та процедур щодо управління ризиками. До другої лінії згідно з постановою належить підрозділ з управління ризиками, який здійснює управління ризиками згідно з положенням НБУ, а третя лінія – підрозділ внутрішнього аудиту. В Україні банки повинні мати політику управління ризиком інформаційно-комунікаційних технологій або окремим документом, або наявні у вже існуючому документі. Тобто, оглянуті банки Україні у цій роботі, повинні мати впроваджену модель трьох ліній управління ризиками, але тільки АТ «ПриватБанк» впровадив її у документ політики інформаційної безпеки з грифом: відкритий. Для суспільства, партнерів банку, інвесторів тощо це є позитивним рішенням, що збільшує довіру до банку. АТ «ПриватБанк» впровадивши трирівневу модель управління ризиками у свою систему управління інформаційною безпекою, досягає більшого рівня захисту ресурсів, систем та інформації у банку, на відміну від інших банків, де ця модель не впроваджена. У політиках інформаційної безпеки банків АТ «Таскомбанк» та АТ «Ощадбанк» не прописані пункти про модель трьох ліній захисту, але впроваджений ризик орієнтований підхід до забезпечення захисту

інформації та є підрозділи з управління ризиками. Можна вважати, що Постанова НБУ виконана частково. [31, 32]

ПІБ банків України, індійський банк Manipur State Co-operative Bank та два банки з Європи: «Jyske Bank A/S» та «British Business Bank» подібні, вони містять конкретні вимоги до персоналу, заходи контролю за виконанням цієї ПІБ, дозволені та заборонені дії з інформаційними активами тощо. У ПІБ індійського банку наявні пункт про ролі та обов'язки: керівника відділу інформаційних технологій, ІТ-комітету на рівні правління, керівного комітету ІТ, комітету з ІБ, відділу ІТ, юридичного відділу, філій банку, співробітників, третьої сторони. Також політика містить кроки та заходи банку виражені у пунктах поточної політики, що розширює сфери діяльності банку, забезпечення безпечної діяльності персоналу банку в яких підвищує загальний рівень ІБ банку:

- забезпечення кібербезпеки інформаційних активів;
- захисту інформаційної інфраструктури кібернетичного зв'язку банку;
- реагування, вирішення та відновлення після кіберінцидентів;
- управління запасами ІТ-активів;
- запобігання доступу несанкціонованого програмного забезпечення;
- екологічному контролю;
- мережевому менеджменту та безпеці;
- безпечної конфігурації;
- антивірусному захисту та керуванню виправленнями;
- контролем та управління доступом користувачів;
- захищеної пошти та системи обміну повідомленнями, змінному носієві;
- обізнаності користувачів, працівників, керівництва;
- навчання та обізнаність клієнтів;
- резервне копіювання та відновлення;
- управління ризиками постачальників та аутсорсингу;

- оцінка вразливостей та тестування на проникнення;
- моніторинг транзакцій на основі ризиків;
- реагування на інциденти та управління кіберкризою;
- криміналістика.

Така велика політика інформаційної безпеки індійського банку є суттєвою перевагою, бо надає зацікавленим сторонам впевненість у ефективності систем захисту, які впроваджені та функціонують. Показує розуміння керівництва банку важливості забезпечення безпеки інформації. Недоліком ПІБ банку «MSCB» є відсутність впровадженої моделі трьох ліній управління ризиками. Структура забезпечення ІБ банку, що показана на рис.№2 має подібності з структурою тайванського банку «Chang Hwa Bank» та деякі подібності з українськими АТ «Ощадбанк» та АТ «ПриватБанк», АТ «Таскомбанк» але немає комітету чи відділу з управління ризиками а також відділу аудиту, що є недоліком.

Українські банки мають схожі політики інформаційної безпеки, але банки АТ «Кредобанк» та АБ «УкрГазБанк» не мають підрозділів з оцінки, керування ризиками що є суттєвим недоліком. ПІБ чотирьох українських банків за винятком АТ «Кредобанк» містять інформацію, що банки використовують ризик-орієнтований підхід, мають систему управління інформаційною безпекою (СУІБ). Перевагою банку ПІБ АТ «Таскомбанк» є наявність пункту про використання двох або більше каналів передавання даних для зв'язку технологічної платформи критичної інформаційної інфраструктури Банку з мережею через використання різних провайдерів телекомунікацій з захищеними вузлами доступу. ПІБ банків відповідають стандартам серії ДСТУ ISO/IEC 2700X, нормативно-правовим актам НБУ, КМУ, ВРУ тощо.

Політики безпеки банків Європи та України містять схожу структуру ПІБ. Загальна структура виглядає наступним чином: загальні положення, визначення термінів, мета, ціль, сфера застосування, відповідальність, основні принципи, пов'язані документи.

Таблиця 2.1 – Рейтинг банків за активами

№	Назва	Активи	Персонал
1	АТ «ПриватБанк»	376 мільярди гривень	22000
2	АТ «Ощадбанк»	249 мільярди гривень	29000
3	АБ «УКРГАЗБАНК»	176 мільярди гривень	4000
4	«Jyske Bank A/S»	43,3 млрд датських крон (173,2 мільярди гривень)	3957
5	«British Business Bank»	2,7 мільярди фунтів (137 мільярди гривень)	500
6	«Chang Hwa Bank»	2,74 мільярди доларів США (111,7 мільярди гривень)	6592
7	«Stanbic Bank Uganda»	2,5 мільярди доларів США (97,5 мільярди гривень)	1907
8	«Taiwan Business Bank»	73 мільярди тайваньских доларів (91 мільярд гривень)	5693

Продовження таблиці 2.1 – Рейтинг банків за активами

№	Назва	Активи	Персонал
9	АТ «КРЕДОБАНК»	55,8 мільярди гривень	1500
10	АТ «Таскомбанк»	32,3 мільярди гривень	1925
11	«The Manipur State Co-operative Bank Limited»	225,30 крор рупій (1,09 мільярди гривень)	500

2.3 Висновок

Розглянуті політики інформаційної безпеки мають різні структури, стилі викладення. Політики інформаційної безпеки розглянутих іноземних та українських банків мають відмінності в залежності від регіону. ПІБ європейських та українських банків подібні між собою, а ПІБ тайванських банків в свою чергу між собою. Виділяється ПІБ індійського та угандського банків. ПІБ залежать від багатьох факторів та умов. Суттєвими факторами є умови, в яких функціонує банківська система, країна тощо. В Україні діє постійна терористична та військова загроза від країни-агресора, тому на перший план виходять плани забезпечення безперебійного ведення бізнесу, захисту ІБ від посягань спеціалізованих хакерських груп, стабільності роботи та функціонування ресурсів банку, що впливає на фінансовий стан установи, на стабільність роботи пов'язаних сфер та на життя громадян. Українські банки за останні десять років зробили суттєві покращення своїх систем безпеки, в тому числі захисту інформації. Нормативно-правове забезпечення ІБ, плани безперервної діяльності, аварійного відновлення покращені та оновлені з використанням практичного досвіду, тому ПІБ українських банків

мають систему захисту більш практичну та досконалішу порівняно з іноземними банками. ПІБ найбільших банків України АТ «ПриватБанк», АТ «Ощадбанк» є більш конкретними та пропрацьованими за іноземні. Українські банки мають розлогу структуру управління інформаційною безпекою, управління ризиками, захисту персональних даних тощо. Данський банк «Jyske Bank A/S» та британський «British Business Bank» мають подібну ПІБ з українськими банками. Можна зробити припущення, що економічна близькість ЄС та України призводить до подібності ПІБ, імплементовані директиви ЄС у банківській сфері України встановлюють схожі вимоги та обов'язки банків щодо дотримання рівня захисту та забезпечення ІБ.

В свою чергу тайванські банки мають схожі між собою політику інформаційної безпеки.

Згідно з таблицею №1 можна виділити перші 5 банків, вони за кількістю активів та співробітників подібні, за винятком британського банку. Структура ПІБ схожа, кожен банк має комітет з управління ІБ на рівні правління, у кожному банку реалізована система управління інформаційною безпекою. Розміри банку, основні напрями роботи впливають на кількість та варіативність загроз.

Для покращення безпеки та безперебійної роботи українським банкам рекомендовано імплементувати у свої ПІБ питання безпечного зв'язку технічних платформ критичної інфраструктури з мережею Інтернет через захищені вузли доступу з використанням двох чи більше різних провайдерів телекомунікацій. Постійна загроза повторенню кібератак на головні провайдери телекомунікацій України зі сторони країни-агресором потребує нових підходів до планів безперервного захисту та функціонування критичних бізнес-процесів та систем.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

3.1 Обґрунтування витрат на аналіз політик інформаційної безпеки іноземних та українських організацій

Аналіз політик безпеки інформації дозволяє знаходити якісні нововведення у політиках інформаційної безпеки іноземних банків та покращувати політики інформаційної безпеки українських банків, імплементуючи найкращі світові практики.

3.2 Розрахунки витрат на аналіз політик інформаційної безпеки іноземних та українських організацій

3.2.1 Визначення трудомісткості роботи з аналізу політик безпеки

Робота з аналізу політик інформаційної безпеки українських та іноземних організацій склалася з наступних етапів:

1) пошук спеціалізованої літератури;

2) аналіз літератури та визначення вимог до методів, засобів та заходів захисту інформації в організаціях;

3) аналіз політик інформаційної безпеки іноземних та українських організацій.

$$t = t_п + t_{вв} + t_а, \quad \text{годин}, \tag{3.1}$$

де $t_п$ – тривалість пошуку літератури, години

$t_{вв}$ – тривалість визначення вимог до методів, засобів та заходів захисту, години

$t_а$ – тривалість аналізу політик інформаційної безпеки, години.

$t = 4 + 48 + 48 = 100$ годин.

3.2.2 Розрахунок витрат на аналіз політик інформаційної безпеки.

Витрати на аналіз політик інформаційної безпеки $К_{ап}$ складається з заробітної плати спеціаліста $З_{зп}$ та вартості витрат машинного часу, що необхідний для виконання аналізу $З_{мч}$.

$$К_{ап} = З_{зп} + З_{мч}, \quad \text{грн.}, \tag{3.2}$$

Заробітна плата робітника, який аналізує політки інформаційної безпеки включає основну та додаткову заробітну плату, відрахування на страхування (пенсійне, на випадок безробіття, соціальне тощо) та визначається з-за допомоги наступної формули:

$$З_{зп} = t \times З_{іб}, \text{ грн,} \quad (3.3)$$

де t – тривалість роботи, години,

$З_{іб}$ – середня погодинна заробітна плата спеціаліста з ІБ, грн.

Так, як я виконую науково-дослідну роботу тому $З_{зп} = 0$ грн.

Витрати на машинний час ПК можна прорахувати за наступною формулою:

$$З_{мч} = t \times С_{мч}, \text{ грн,} \quad (3.4)$$

де t – трудомісткість аналізу політик інформаційної безпеки, години,

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./годину.

Вартість 1 години машинного часу можна вирахувати з-за допомогою формули 3.5:

$$С_{мч} = P \times С_{Е}, \text{ грн,} \quad (3.5)$$

Де P – встановлена потужність ПК, кВт,

$С_е$ – тариф на електричну енергію, грн/кВт*годину.

Для розрахунку P – встановленої потужності ПК скористаємося онлайн сервісами для підрахунку енерговитрат ПК. ПК складається зі звичайної micro-ATX материнської плати ASUS Prime H-410 M-K, центрального процесору Intel Core i3-10100f CPU @3.60 GHz, графічного процесору AMD Radeon RX 6600 XT, з двома блоками оперативних запам'ятовуючих пристроїв 32GB (2x16GB) з накопичувачами HDD WD Blue 3.5" 1TB SATA/64MB та SSD Kingston NV2 500GB. Блок живлення: БП Zalman ZM600-LE2 600w та 4 вентилятори по 120″, вентилятор на процесорі. Спеціалізований онлайн-сервіс розрахував теплову розрахункову потужність по компонентах P = 295 Вт = 0,295 кВт. Це орієнтовний показник теплової потужності ПК, тому що за різних умов = різні показники. Тариф на електричну енергію для побутових споживачів в Україні - 3,6 грн/кВт*год, додається ПДВ - 0,72 грн/кВт*год, підсумковий тариф з ПДВ - 4,32 грн/кВт*год.[47]

Після розрахунку встановленої потужності ПК прораховуємо вартість 1 години машинного часу ПК.

$$С_{мч} = Р \times С_{Е} = 0,295 \times 4,32 = 1,27 \text{ грн.}$$

1 година машинного часу ПК орієнтовно дорівнює 1,27 грн., наступним кроком треба вирахувати орієнтовні загальні витрати на машинний час ПК та витрати на аналіз політик $К_{ап}$.

$$З_{мч} = 100 \times 1,27 = 127,00 \text{ грн.}$$

$$К_{ап} = 0 + 127 = 127,00 \text{ грн.}$$

Тобто витрати на аналіз політик інформаційної безпеки склали 127 грн.

3.3 Розрахунок економічної доцільності аналізу, розробки та впровадження додаткових складових політик для банків АТ «ПриватБанк».

Головним висновком другого розділу цієї роботи є важливість розробки та впровадження політик для вирішення питання безпечного та стабільного зв'язку об'єктів Банків з мережею Інтернет через захищені вузли доступу з використанням двох чи більше різних провайдерів телекомунікацій. Для покращення безпеки та безперебійної роботи українським банкам рекомендовано пропрацювати дане питання як це було зроблено керівництвом АТ «Таскомбанк», чия політика інформаційної безпеки оновлена та набула чинності 26.01.2024 року вже після успішної кібератаки хакерів країни-агресору на найбільшого надавача послуг з телекомунікацій України ПрАТ «Київстар» у грудні 2023-го року. Постійна загроза повторенню кібератак на головних гравців ринку телекомунікацій України зі сторони країни-агресора потребує нових підходів до планів безперервного захисту та функціонування систем. [25, 50]

На прикладі АТ «ПриватБанк» можна продемонструвати актуальність питання та важливість якнайшвидшого вирішення.

Вранці 12-го грудня 2023-го року компанія телекомунікацій ПрАТ «Київстар» зазнала атаки з частковим руйнуванням IT-інфраструктури, через що з'явилися збої в роботі банків «Ощадбанк», «ПриватБанк», «Таскомбанк», головною проблемою стало функціонування POS-терміналів, які використовували мобільний зв'язок від «Київстар», а також мали місце затримки в роботі терміналів, які

використовують інших провайдерів, через збільшення навантаження на їхні мережі. За оцінками експертів та представників «ПриватБанку» через цю атаку тимчасово стали недоступні або працювали нестабільно до 5% банкоматів, до 10% терміналів самообслуговування, до 30% POS-терміналів. [49, 50, 51]

Згідно з фінансовим звітом АТ «ПриватБанк» за 2023 мережа та інфраструктура банку налічує 6881 активних банкоматів, 10442 активних термінали самообслуговування та 288,8 тис. активних POS-терміналів. Згідно з повідомленнями керівництва ПрАТ «Київстар» з 20:00 12 грудня 2023 року «Київстар» почав відновлювати доступ абонентів до послуг фіксованого зв'язку, 14 грудня 2023 року була відновлена робота домашнього інтернету на 93%, а вже 15 грудня 2023 року «Київстар» увімкнув мобільний інтернет, включаючи стандарт 4G. [48, 49, 51]

Тобто АТ «ПриватБанк» з 12-15 грудня 2023-го року мав проблеми з 344 (6.537 продовжують функціонувати) банкоматами, 1.044 (9.398 продовжують функціонувати) термінали самообслуговування та приблизно 86.640 (202.160 продовжують функціонувати) POS-терміналів. Згідно з щорічним звітом банку за 2023-й рік банк заробив 72,8 млрд грн прибутку до оподаткування, 37,8 млрд грн чистого прибутку, заплатив 26,8 млрд грн податку на прибуток, 30,2 млрд грн річних дивідендів.

Для оцінки орієнтовного впливу відсутності недоступних банкоматів та терміналів треба вирахувати орієнтовний середній прибуток банку за 2023-й рік.

$$П_{сд1} = \frac{Пр}{365}, \text{ млн. грн.}, \quad (3.6)$$

де $П_{сд1}$ - середній добовий прибуток до оподаткування протягом 2023р., млн. грн.,

$П_р$ – річний прибуток за 2023р., млн. грн.

$$П_{сд1} = \frac{72,8}{365} = \sim 199,45$$

Потрібно вирахувати відсоток вибутих активів.

$$\Delta = \frac{А_д - А_п \times 100}{А_д}, \ \%, \quad (3.7)$$

де $А_д$ - Кількість активів до атаки, шт.

$А_п$ - Кількість активів після атаки, шт.

Кількість активів до атаки – 306.123 шт. Кількість активів після атаки – 218.095 шт.

$$\Delta = \frac{306.123-218.095 \times 100}{306.123} = 28{,}7\ \%$$

Тобто різниця працездатних активів – $\Delta =$ 28,7 %, майже 1/3 всієї мережі банку була непрацездатною або працювала з затримками, що принесло орієнтовних збитків за день $З_д$. Для розрахунку збитків в день від непрацездатності активів банку потрібно розрахований показник середньо добового прибутку до оподаткування зменшити на 28,7%, що зможе орієнтовно показати втрати від непрацездатних активів.

$$П_{сд2} = П_{сд1} - \frac{\Delta \times П_{сд1}}{100} = \text{ млн. грн.}, \quad (3.8)$$

де $П_{сд2}$ - середній добовий прибуток до оподаткування за відсутності непрацездатних активів, млн. грн.,

$$П_{сд2} = П_{сд1} - \frac{\Delta \times П_{сд1}}{100} = 199{,}45 - 57{,}24 = 142{,}21 \text{ млн. грн.},$$

Орієнтовний показник збитків в день $З_д$ простою дорівнює:

$$З_д = П_{сд1} - П_{сд2}, \text{ млн. грн.}, \quad (3.9)$$

$$З_д = 199{,}45 - 142{,}21 = 57{,}24 \text{ млн. грн.},$$

За повідомленнями керівництва ПрАТ «Київстар» 15.12.2023 всі основні послуги компанії були відновлені, включно з домашнім та мобільним інтернетом.[50]

Тобто максимальний орієнтовний збиток банку від вибуття майже 28,7% активів за три дні міг скласти $З_{дм}$.

$$З_{дм} = 3 \times З_д, \text{ млн. грн.}, \quad (3.10)$$

$$З_{дм} = 3 \times 57{,}24 = 171{,}72, \text{ млн. грн.},$$

Компанія АТ «ПриватБанк» найнявши спеціаліста з ІБ для аналізу питання зв'язку між технічними сервісами та критичною інформаційною інфраструктурою Банку може з мінімальними інвестиціями для аналізу та розробки складової політики інформаційної безпеки зменшити ризики повторення даної ситуації.

Згідно з попередніми розрахунками щодо аналізу політик інформаційної безпеки можна прорахувати орієнтовну вартість розробки та впровадження

складових політик інформаційної безпеки щодо дублювання засобів зв'язку з використанням різних провайдерів телекомунікацій.

Рахуємо тривалість роботи:

$$t = t_{п} + t_{вв} + t_{а} + t_{р}, \quad \text{годин}, \tag{3.11}$$

де $t_{п}$ – тривалість пошуку літератури, години

$t_{вв}$ – тривалість визначення вимог до методів, засобів та заходів захисту, години

$t_{а}$ – тривалість аналізу політик інформаційної безпеки, години,

$t_{р}$ – тривалість розробки складових політик інформаційної безпеки, години.

t = 4 + 48 + 48 + 48 = 148 годин.

Рахуємо витрати на аналіз та розробку складових політик інформаційної безпеки.

Витрати на аналіз та розробку політик інформаційної безпеки $К_{арп}$ складається з заробітної плати спеціаліста $З_{зп}$ та вартості витрат машинного часу, що необхідний для виконання аналізу та розробки $З_{мч}$.

$$К_{арп} = З_{зп} + З_{мч}. \tag{3.12}$$

Заробітна плата робітника, який аналізує політки інформаційної безпеки включає основну та додаткову заробітну плату, відрахування на страхування (пенсійне, на випадок безробіття, соціальне тощо) та визначається з-за допомоги наступної формули:

$$З_{зп} = t \times З_{іб}, \text{ грн}, \tag{3.3}$$

де t – тривалість роботи, години,

$З_{іб}$ – середня погодинна заробітна плата спеціаліста з ІБ, грн.

Згідно з порталом пошуку роботи «Work.ua» середня З/П спеціаліста з ІБ в Україні дорівнює 24.000 грн./міс., що дорівнює 150 грн./год. [57]

$$З_{зп} = 148 \times 150 = 22.200{,}00 \text{ грн},$$

Витрати на машинний час ПК можна прорахувати за наступною формулою:

$$З_{мч} = t \times С_{мч}, \text{ грн}, \tag{3.4}$$

де t – трудомісткість аналізу політик інформаційної безпеки, години

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./годину.

Вартість 1 години машинного часу можна вирахувати з-за допомогою формули 3.5:

$$С_{мч} = Р \times С_{Е},\ грн, \quad (3.5)$$

Де Р – встановлена потужність ПК, кВт,

$С_{е}$ – тариф на електричну енергію, грн/кВт*годину.

$С_{мч} = 0{,}295 \times 4{,}32 = 1{,}27$ грн.

1 година машинного часу ПК орієнтовно дорівнює 1,27 грн., наступним кроком треба вирахувати орієнтовні загальні витрати на машинний час ПК та витрати на аналіз та розробку політик $К_{арп}$.

$З_{мч} = 148 \times 1{,}27 = 187{,}96$ грн.

$$К_{арп} = З_{зп} + З_{мч},\ грн., \quad (3.3)$$

$К_{арп} = 22.200 + 187{,}96 = 22.387{,}96$ грн.

Рахуємо витрати на впровадження політики дублювання засобів зв'язку для технічних засобів.

Вартість впровадження $К_{вп}$ можна прорахувати наступним чином, вартість процедури доповнення терміналів самообслуговування, банкоматів та POS-терміналів + З/П працівників, що будуть виконувати зазначені роботи.

$$К_{вп} = З_{зп} + З_{обл} \quad (3.13)$$

де, $З_{зп}$ це заробітної плати спеціаліста, грн.,

$З_{обл}$ – вартість допоміжного обладнання, грн.

$З_{зп}$ розраховуємо виходячи з кількості витраченого часу на встановлення додаткових засобів зв'язку.

За даними прес секретаря ПриватБанку залежність сервісів банку від Київстар наступна: до 5% банкоматів, до 10% терміналів самообслуговування, до 30% POS-терміналів. Тобто це 344 банкомати, 1044 термінали самообслуговування, 86640 POS-терміналів. Сумарний показник 88028 технічні засоби, яким потрібно додати альтернативний засіб зв'язку або непрацездатні технічні засоби – $А_{н}$. В Україні відділення банку є у 458 населених пунктах. Рахуємо, що потрібно мінімум 458 робітників - $К_{с}$, які працюють у цих населених пунктах для виконання

завдання з встановлення додаткових SIM-карт у термінали та банкомати. [49, 51, 52]

Середня кількість технічних засобів на одну особу - $Т_{ск}$ рахуємо наступним чином:

$$Т_{ск} = \frac{А_н}{К_с} \quad шт., \tag{3.14}$$

де $А_н$ – непрацездатні технічні засоби, шт,

$К_с$ – кількість працівників, осіб.

$$Т_{ск} = \frac{88028}{458} = 192 \text{ шт.}$$

Згідно з порталом пошуку роботи «Work.ua» середня заробітна плата в Україні станом на червень 2024-го року дорівнює 20500 грн, що дорівнює 128,13 грн./год - $З_{сзп}$. Припустимо, що витрати на процес додавання додаткових засобів зв'язку до технічних засобів (SIM-карт) в середньому займають до 10 хв - $t_в$, тому можна прорахувати орієнтовну тривалість роботи - $t_з$ та вартість заробітної плати за виконану роботу - $З_{зп}$. [54]

$$t_з = \frac{t_в \times Т_{ск}}{60} \quad години, \tag{3.15}$$

$$t_з = \frac{10 \times 192}{60} = 32 \text{ години},$$

$$З_{зп} = t_з \times З_{сзп}, \quad грн, \tag{3.3}$$

де, $З_{сзп}$ – середня заробітна плата за виконані роботи на одну особу.

$$З_{зп} = 32 \times 128{,}13 = 4.100{,}16 \text{ грн.},$$

$$З_{ззп} = З_{зп} \times К_с \quad грн., \tag{3.16}$$

де, $З_{ззп}$ – загальні витрати на заробітну плату за виконані роботи.

$$З_{ззп} = 4.100{,}16 \times 458 = 1.877.873{,}28 \text{ грн.},$$

Щоб вирахувати вартість допоміжного обладнання потрібно проаналізувати доступні варіанти для використання, виходячи з інформації, яка міститься на офіційному сайті телекомунікаційної компанії «Vodafone», що займає друге місце на ринку послуг телекомунікації в Україні після компанії «Київстар». Для бізнесу є пакети послуг, які містять 250.000 МБ мобільного інтернету за тарифом 125 грн./рік.[53] Можна прорахувати вартість допоміжного обладнання, використовуючи формулу 3.17:

$$З_{обл} = А_н \times В_{обл},\ \text{грн.}, \quad (3.17)$$

де $В_{обл}$ – вартість одиниці потрібного обладнання.

$$З_{обл} = 88.028 \times 125 = 11.003.500{,}00\ \text{грн.},$$

$$К_{вп} = З_{ззп} + З_{обл} = 1.877.873{,}28 + 11.003.500{,}00 = 12.881.373{,}28\ \text{грн.},$$

Таким чином капітальні витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

$$К = К_{арп} + К_{вп},\ \text{грн.}, \quad (3.18)$$

$$К = 22.387{,}96 + 12.881.373{,}28 = 12.903.761{,}24\ \text{грн.},$$

3.3.1 Визначення та аналіз показників економічної ефективності впроваджених заходів

Коефіцієнт повернення інвестицій ROSI показує яких збитків можна запобігти, впроваджуючи додатковий захист. Коефіцієнт ROSI розраховується за формулою:

$$ROSI = \frac{Е}{К}, \quad (3.19)$$

де Е-загальний ефект від впровадження, тис. грн.,

К-капітальні інвестиції, тис. грн.

$E = (В \times R - С)$ – загальний ефект від впровадження системи інформаційної безпеки,

В – загальний збиток від атаки, тис. грн.,

R – очікувана ймовірність повторення атаки, частка одиниці,

С – щорічні витрати на експлуатацію систем захисту, тис. грн.

Згідно з заявами керівництва компанії, «Київстар» до цієї атаки відбив понад 500 атак, тому ймовірність повторення атаки використаємо – 0,2. С буде дорівнювати $З_{обл}$. Розраховуємо загальний ефект від впровадження. [50]

$$Е = В \times R - С,\ \text{тис. грн.}, \quad (3.20)$$

$$Е = 171.720 \times 0{,}2 - 11.003{,}5 = 23.340{,}5\ \text{тис. грн.},$$

$$\text{Тоді, } ROSI = \frac{Е}{К} = \frac{23.340{,}5}{12.903{,}76} = 1{,}8.$$

Проект впровадження заходів системи інформаційної безпеки або додаткового захисту визнається економічно доцільним за умови $ROSI > Е_н$.

Показник ефективності $Е_н$ можна розрахувати наступним чином. Для кредитних грошей $Е_н = (Н_{кр} + Н_{інф})/100$,

де $Н_{кр}$ – банківська кредитна ставка, %,

$Н_{інф}$ – річний рівень інфляції, %.

Для власних коштів підприємства: $Е_н = (Н_{деп} - Н_{інф})/100$

де $Н_{деп}$ – річна депозитна ставка, %,

$Н_{інф}$ – річний рівень інфляції, %.

Прогнозований рівень інфляції згідно з оцінкою НБУ $Н_{інф}$ = 8,2%, облікова ставка з 14.06.2024 на рівні 13%. [55, 56]

Якщо Банк використає кредитні кошти:

$$ROSI > (Н_{кр} + Н_{інф})/100 \quad (3.21)$$

$$ROSI > (13 + 8{,}2)/100 = 1{,}8 > 0{,}212$$

Якщо Банк використає власні кошти:

$$ROSI > (Н_{деп} - Н_{інф})/100 \quad (3.22)$$

$$ROSI > (13 - 8{,}2)/100 = 1{,}8 > 0{,}048$$

Економічно доцільним вважається варіант вкладення власних грошей. Термін окупності $Т_о$ рахується за наступною формулою:

$$Т_о = \frac{К}{Е} = \frac{1}{ROSI}, \text{ роки,} \quad (3.23)$$

$$Т_о = \frac{К}{Е} = \frac{1}{ROSI} = 0{,}55 \text{ роки,}$$

Термін окупності складає 0,55 роки або 200 днів, що є 6 місяців та 18 днів.

3.4 Висновок

В економічному розділі були прораховані показники банку АТ «ПриватБанк», які показують яких втрат можна було запобігти від масштабної атаки на ПрАТ «Київстар» взимку 2023р та аналіз, розробка та впровадження складових політик інформаційної безпеки щодо дублювання засобів зв'язку для технічних засобів банку, які залежали виключно від працездатності мережі від «Київстар». Прораховані наступні показники: капітальні витрати 12.903.761,24 грн., експлуатаційні витрати 11.003.500 грн./рік, вірогідну величину збитку банку від атаки на телекомунікаційну компанію «Київстар» 171,72 млн.грн., термін окупності 6

місяців та 18 днів. Впровадження складової політик інформаційної безпеки щодо дублювання засобів зв'язку для технічних засобів банків є економічно доцільним рішенням та важливою складовою безперебійного ведення бізнес-процесів та захисту інформації.

ВИСНОВКИ

В першому розділі кваліфікаційної роботи було визначено загальну суть питання політики безпеки, визначено її мету, область застосування, необхідність впровадження, основну структуру та обов'язкові елементи. Визначено основні етапи розробки політик безпеки та поширені складові політик безпеки інформації. Також у цьому розділі проведений стислий огляд законодавчого регулювання сфери захисту інформації в Україні.

У другому розділі роботи проведений огляд політик інформаційної безпеки українських та іноземних компаній у фінансовій галузі, третього сектору економіки – банківські установи. Розглянуті політики мають різну структуру та стилі викладення. Проведений аналіз переваг та недоліків українських та іноземних банків. Для покращення безпеки та безперебійної роботи українським банкам рекомендовано розробити та впровадити у свої ПІБ питання дублювання зв'язку технічних платформ з мережею Інтернет через захищені вузли доступу.

В економічному розділі були прораховані наступні показники: вартість проведення аналізу політик безпеки інформації українських та іноземних компаній, капітальні витрати, експлуатаційні витрати, вірогідну величину збитку банку від атаки на телекомунікаційну компанію «Київстар», термін окупності за основою банку АТ «ПриватБанк», які показують яких втрат можна було запобігти від масштабної атаки на ПрАТ «Київстар» взимку 2023р

ПЕРЕЛІК ПОСИЛАНЬ

1.Антонюк А.О. Політика безпеки інформації в захищених автоматизованих системах / А. О. Антонюк // Наукові записки НаУКМА : Комп'ютерні науки. - 2003. - Т. 21. - С. 103-107. [Електронний ресурс]. – Режим доступу https://ekmair.ukma.edu.ua/server/api/core/bitstreams/50763dd1-6bf8-4c7d-96a2-947a38487b09/content

2. НД ТЗІ 1.1—003—99.Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. Вид. офіц. Київ: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 1999.- 5-6 с. [Електронний ресурс]. – Режим доступу https://tzi.ua/assets/files/1.1_003_99.pdf

3. НД ТЗІ 1.1—002—99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Вид. офіц. Київ: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 1999.11-12 с. [Електронний ресурс]. – Режим доступу https://tzi.com.ua/downloads/1.1-002-99.pdf

4. Методичні рекомендації щодо забезпечення кіберзахисту автоматизованих систем управління технологічними процесами: ДССЗ та ЗІ України від 29 травня 2023 року N 463, 3 с. [Електронний ресурс]. – Режим доступу https://ips.ligazakon.net/document/view/fn077605?an=27&ed=2023_05_29

5. Маковський І. Ю., ЕТАПИ СТАНОВЛЕННЯ ТА ЗНАЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ ЕФЕКТИВНОГО ФУНКЦІОНУВАННЯ ПІДПРИЄМСТВ / Маковський І. Ю - Житомирська політехніка, 1.с. [Електронний ресурс]. – Режим доступу https://conf.ztu.edu.ua/wp-content/uploads/2019/12/554.pdf%20.

6. Куперштейн, Л., Дудатьєв, А., Войтович, О., & Ясінська, Я. МОДЕЛЬ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЛЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ.*MEASURING AND COMPUTING DEVICES IN*

TECHNOLOGICAL PROCESSES, 2021 30–38. [Електронний ресурс]. – Режим доступу: https://doi.org/10.31891/2219-9365-2021-68-2-4

7.НД ТЗІ 1.4—001—2000. Типове положення про службу захисту інформації в автоматизованій системі Вид. офіц. Київ: Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України, 2000.- 26-37 с. [Електронний ресурс]. – Режим доступу https://tzi.com.ua/downloads/1.4-001-2000.pdf

8. Про інформацію: Закон України від 02.10.1992 р. № 1992 -XII. Дата оновлення: 27.07.2023. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 20.06.2024).

9.Про критичну інфраструктуру : Закон України від 16.11.2021 р. № 1882 - IX. Дата оновлення: 01.01.2024. URL: https://zakon.rada.gov.ua/laws/show/1882-20 (дата звернення: 20.06.2024).

10. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 19.06.2019 р. № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text

11. Стичинська А.Б. Теоретичні основи політики інформаційної безпеки [Електронний ресурс]: стаття Стичинська А.Б. – Дніпро, видавництво «Грані» Том 24 №6 2021 [Електронний ресурс]. – Режим доступу: https://grani.org.ua/index.php/journal/article/view/1661/1637

12. Про інформацію: Закон України від 02.010.1992 р. № 2657-XII. Дата оновлення: 27.07.2023. URL: https://zakon.rada.gov.ua/laws/show/2657-12 (дата звернення: 20.06.2024).

13. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. Дата оновлення: 04.04.2024. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 20.06.2024).

14. Валюшко І.О. ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ: ТРАНСФОРМАЦІЯ ЗАКОНОДАВСТВА ПІСЛЯ РОСІЙСЬКОГО ВТОРГНЕННЯ [Електронний ресурс]: стаття Валюшко І.О. – Режим доступу: https://core.ac.uk/download/pdf/197266255.pdf

16. НД ТЗІ 3.6—004—21. Порядок впровадження системи безпеки інформації в державних органах, на підприємствах, організаціях, в інформаційно-комунікаційних системах яких обробляється інформація, вимога щодо захисту якої встановлена законом та не становить державної таємниці Вид. офіц. Київ: Адміністрація Державної служби спеціального зв'язку та захисту інформації України, 2021.19-21 с. [Електронний ресурс]. – Режим доступу https://cip.gov.ua/services/cm/api/attachment/download?id=53375

17. В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ / Навчальний посібник – Ніжин 2018, 114-117с. [Електронний ресурс]. – Режим доступу http://surl.li/kzezan

18. Офіційний перелік системно важливих банків від НБУ. URL: https://bank.gov.ua/ua/supervision/institutions?page=2&perPage=10&search=&status=1&uid=&suid=&date_from=&date_to=&isSysImportant=1&fb_date_from=&fb_date_to

19. Політика інформаційної безпеки «Chang Hwa Bank» [Електронний ресурс]. – Режим доступу: https://www.bankchb.com/csr/mashup_eng.jsp?funcId=9fff75e315

20. Політика інформаційної безпеки «Taiwan Business Bank» [Електронний ресурс]. – Режим доступу: https://www.tbb.com.tw/en-us/disclosures/statements/cyber-security

21. Політика інформаційної безпеки «Stanbic Bank Uganda» [Електронний ресурс]. – Режим доступу: https://www.stanbicbank.co.ug/static_file/Uganda/Downloadable%20files/Information%20Security%20Policy.pdf

22. Політика інформаційної безпеки «Jyske Bank A/S» [Електронний ресурс]. – Режим доступу:https://jyskebank.com/wps/wcm/connect/jbc/719f3403-5967-4990-af2f-238981b7f8da/IT+Security+Policy.pdf?MOD=AJPERES&CVID=n.kKYuU

23. Політика інформаційної безпеки «The Manipur State Co-operative Bank Limited» [Електронний ресурс]. – Режим доступу: https://mscbmanipur.in/?p=952

24. Політика інформаційної безпеки «British Business Bank» [Електронний ресурс]. – Режим доступу: https://www.british-business-bank.co.uk/about/our-values/transparency/policies-and-procedures/information-security-policy

25. Політика інформаційної безпеки АТ «ТакСомБанк» [Електронний ресурс]. – Режим доступу: https://tascombank.ua/files/Polityka_informatsiinoi_bezpeky-2024.pdf

26. Політика інформаційної безпеки АТ «ПриватБанк» [Електронний ресурс]. – Режим доступу: https://static.privatbank.ua/files/22092022_InformationSecurity.pdf

27. Політика інформаційної безпеки АТ «Кредобанк» [Електронний ресурс]. – Режим доступу: https://kredobank.com.ua/public/upload/38ec79c93e4640408d341f26b88063f4.pdf

28. Політика інформаційної безпеки АТ «Ощадбанк» [Електронний ресурс]. – Режим доступу: https://www.oschadbank.ua/uploads/0/1660-politika_ib.pdf

29. Політика інформаційної безпеки АТ «УкрГазБанк» [Електронний ресурс]. – Режим доступу: https://www.ukrgasbank.com/upload/file/20201211_info_bezpek.pdf

30. Заросило В.О., Загрози фінансовій безпеці та їх класифікація // Заросило В.О. МАУП – Київ / [Електронний ресурс]. – Режим доступу https://maup.com.ua/assets/files/expert/2/zagrozi-finansovij-bezpeci-ta-ih-klasifikaciya.pdf

31 Про внесення змін до деяких нормативно-правових актів Національного банку України. Постанова Правління Національного банку України від 30.03.2023 № 40 URL: https://bank.gov.ua/admin_uploads/law/30032023_40.pdf?v=4

32. Про затвердження Положення про організацію системи внутрішнього контролю в банках України та банківських групах Постанова Правління Національного банку України від 02.07.2019 № 88 URL: https://zakon.rada.gov.ua/laws/show/v0088500-19#Text

33. Annual Reports 2023 «Stanbic Bank Uganda» URL: https://www.stanbicbank.co.ug/static_file/Uganda%20Holdings/Downloadable%20files/Annual%20Reports/Copy%20of%202023%20SUHL%20ANNUAL%20REPORT.pdf

34. «Stanbic Bank Uganda» URL: https://en.wikipedia.org/wiki/Stanbic_Bank_Uganda_Limited#cite_note-6

35. Основні показники банку АБ «Укргазбанк» URL: https://bank.gov.ua/ua/supervision/institutions/23697280

36. Фінансові результати АБ «Украгазбанк» URL: https://minfin.com.ua/ua/company/ukrgasbank/rating/

37. Про банк АТ «ПриватБанк» URL: https://privatbank.ua/about/social

38. АТ «ПриватБанк» URL: https://uk.wikipedia.org/wiki/%D0%9F%D1%80%D0%B8%D0%B2%D0%B0%D1%82%D0%91%D0%B0%D0%BD%D0%BA

39. Про банк АТ «Таскомбанк» URL: https://tascombank.ua/our-team

40. Структура АТ «Кредобанк» URL: https://kredobank.com.ua/about/struktura/struktura-pat-kredobank

41. Про банк АТ «Ощадбанк» URL: https://www.oschadbank.ua/about

42. АТ «Ощадбанк» URL: https://uk.wikipedia.org/wiki/%D0%9E%D1%89%D0%B0%D0%B4%D0%B1%D0%B0%D0%BD%D0%BA

43. «Chang Hwa Bank» URL: https://en.wikipedia.org/wiki/Chang_Hwa_Bank

44. «Taiwan Business Bank» URL: https://www.linkedin.com/company/taiwan-business-bank/

45. «Manipur State Co-operative Bank Ltd» URL: https://www.linkedin.com/company/manipur-state-co-operative-bank-ltd/?originalSubdomain=in

46. About «Jyske Bank A/S» URL: https://jyskebank.com/about

47. Онлайн ресурс визначення енерговитрат ПК URL: https://pc-builds.com/uk/power-supply-calculator/result/3iLv

48. Річний звіт 2023 АТ «ПриватБанк» URL: http://surl.li/rtdkby

49. Збій "Київстар" може вплинути на банківську систему: Приватбанк роз'яснив, що робити. Економічна правда. URL: https://www.epravda.com.ua/news/2023/12/12/707596/

50. Кібератака на «Київстар» (2023). URL: http://surl.li/mxdsoh

51. «ПриватБанк» попередив про можливі збої в роботі через атаку на «Київстар». Mc.today URL: https://mc.today/uk/privatbank-poperediv-pro-mozhlivi-zboyi-v-roboti-cherez-ataku-na-kiyivstar/

52. Відділення «ПриватБанку» .Мінфін URL: https://minfin.com.ua/ua/company/privatbank/branches/

53. Тарифи IoT Vodafone. URL: https://business.vodafone.ua/taryfy/iot-business

54. Середня заробітна плата в Україні. Work.ua. URL: https://www.work.ua/salary-all/

55. Інфляційний звіт НБУ. URL: https://bank.gov.ua/ua/news/all/inflyatsiya-zalishatimetsya-pomirnoyu-a-ekonomika-nadali-vidnovlyuvatimetsya-u-20242026-rokah--inflyatsiyniy-zvit-nbu

56. Облікова ставка НБУ. Мінфін. URL: https://index.minfin.com.ua/ua/banks/nbu/refinance/

57. Середня заробітна плата в Україні, спеціаліст з інформаційної безпеки. Work.ua. URL: http://surl.li/tfyycf

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	1 Розділ	16	
6	А4	2 Розділ	36	
7	А4	3 Розділ	11	
8	А4	Висновки	1	
9	А4	Перелік посилань	6	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

Юсипів.М.С_125-20-1_ПЗ.docx

Юсипів.М.С_125-20-1.pptx

ДОДАТОК В. Відгуки керівника економічного розділу

Економічний розділ виконаний відповідно до вимог, які ставляться до кваліфікаційних робіт, та заслуговує на оцінку 95 б. («відмінно»).

Керівник розділу _____ Д.П. ПІЛОВА

(підпис) (ініціали, прізвище)

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

В І Д Г У К

на кваліфікаційну роботу студента групи 125-20-1 Юсипіва М.С.

на тему: «Аналіз політик безпеки інформації іноземних і українських компаній»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, розташованих на 84 сторінках.

Мета роботи є актуальною, оскільки вона спрямована на аналіз та пошук інноваційних рішень у політиках інформаційної безпеки українських та іноземних організацій.

При виконанні роботи автор продемонстрував високий рівень теоретичних знань і практичних навичок. На основі аналізу поняття політик безпеки інформації, вимог і методів забезпечення захисту інформації в організаціях з використанням політик безпеки, а також законодавчого регулювання захисту інформації в Україні в ній сформульовано задачі, вирішенню яких присвячений спеціальний розділ. У ньому проаналізовано політики інформаційної безпеки іноземних і українських організацій банківської сфери.

Практична цінність роботи полягає у тому, що отримані результати можуть бути використані для забезпечення безпеки інформації та безперебійної роботи українських банків.

До недоліків роботи слід віднести недостатню проробку окремих питань.

Рівень запозичень у кваліфікаційній роботі не перевищує вимог «Положення про систему виявлення та запобігання плагіату».

В цілому робота задовольняє усім вимогам, а її автор Юсипів Михайло Сергійович заслуговує на оцінку « » та присвоєння кваліфікації «Бакалавр з кібербезпеки» за спеціальністю 125 Кібербезпека.

Керівник роботи,
к.т.н., доцент **О.В. Герасіна**