МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Навчально-науковий інститут захисту інформації

На рецензію
Завідувач кафедри УІКБ
доктор економічних наук, доцент
_____ С.В.Легомінова
«___»_____2020 р.

До захисту
Завідувач кафедри УІКБ
доктор економічних наук, доцент
_____ С.В.Легомінова
«___»_____2020 р.

ДИПЛОМНА РОБОТА

на тему:

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЯК ОСНОВА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НА ПІДПРИЄМСТВІ

СТУДЕНТ: Коваленко Олександр Олегович _____
(підпис)

КЕРІВНИК: к.е.н., доц. Мордас Ірина Василівна _____
(підпис)

НОРМОКОНТРОЛЕР: к.в.н., доц. Якименко Юрій Михайлович _____
(підпис)

Київ – 2020

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Навчально-науковий інститут захисту інформації

Кафедра управління інформаційною та кібернетичною безпекою

Освітньо-кваліфікаційних рівень – бакалавр

Спеціальність «Кібербезпека»

Спеціалізація «Управління інформаційною та кібернетичною безпекою»

"ЗАТВЕРДЖУЮ"
Завідувач кафедри УІКБ
_____ С.В.Легомінова
(підпис)
“___”_____ 2020 р.

ЗАВДАННЯ

на дипломну роботу

студенту Коваленку Олександру Олеговичу

1. Тема роботи «Політика інформаційної безпеки як основа управління інформаційної безпеки на підприємстві», затверджена наказом по університету від “___” _____ 20__ р. № ____.
2. Термін здачі студентом оформленої роботи “__” _____ 20__ р.
3. Об’єкт дослідження: інформаційна безпека підприємства.
4. Предмет дослідження: політика інформаційної безпеки підприємства як основа управління інформаційною безпекою на підприємстві.
5. Мета дослідження: вивчення засад політики інформаційної безпеки підприємства як основи управління інформаційною безпекою на підприємстві.
6. Перелік питань, які мають бути розроблені:
1. Провести аналіз основ управління інформаційною безпекою підприємства.
2. Дослідити особливості політик інформаційної безпеки сучасних підприємств.
3. Визначити рекомендації щодо політики інформаційної безпеки на підприємстві.
7. Дата видачі завдання “___”_____ 20__ р.

КАЛЕНДАРНИЙ ПЛАН

Дата видачі завдання: «__» _____ 20__ р.

№ з/п	Етапи дипломної роботи	Термін виконання етапів	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	11.03.2020	
2.	Збір та аналіз літератури.	18.03.2020	
3.	Аналіз основних характеристик політики інформаційної безпеки.	01.04.2020	
4.	Дослідження особливостей управління політикою інформаційною безпекою підприємства.	15.05.2020	
5.	Визначення напрямів та методів забезпечення політики інформаційної безпеки підприємства	29.04.2020	
6.	Формулювання висновків за результатами проведеного дослідження.	06.05.2020	
7.	Оформлення роботи.	12.05.2020	
8.	Оформлення презентації.	14.05.2020	
9.	Отримання рецензії на роботу.	20.05.2020	
10.	Захист в ДЕК.	__.06.2020	

Студент О.О.Коваленко

Науковий керівник І.В.Мордас

РЕФЕРАТ

Дипломна робота присвячена дослідженню проблем політики інформаційної безпеки як основи управління інформаційною безпекою на підприємстві. Робота складається зі вступу, трьох розділів, що містять 14 рисунків, висновків та списку використаних джерел, що містить 30 найменувань. Загальний обсяг роботи становить 62 аркуші, з яких 3 аркуша займає список використаних джерел.

Об'єктом дослідження є інформаційна безпека підприємства.

Метою роботи є дослідження засад політики інформаційної безпеки як основи управління інформаційною безпекою на підприємстві.

Як результат у роботі проведено аналіз основ управління інформаційною безпекою підприємства; досліджено особливості політик інформаційної безпеки сучасних підприємств; визначено рекомендації щодо політики інформаційної безпеки на підприємстві.

Галузь застосування. Розроблені підходи можуть бути використані при плануванні та реалізації системи управління інформаційною безпекою на підприємстві.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА, ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ.

ЗМІСТ

ВСТУП

Актуальність теми. На сучасному етапі підприємства впроваджують різноманітні засоби інформаційного захисту стосовно політики інформаційної безпеки, які активно застосовуються від конкуруючих фірм та корпорацій в конкурентній боротьбі за встановлення контролю на ринку та домінування у відповідній сфері.

Тому політика забезпечення інформаційної безпеки підприємства має бути побудована з урахуванням потреби запобігати і протидіяти загрозам, вразливостям та ризикам, що виникають внаслідок застосування методів інформаційного управління, захищати потенційно важливі інформацію, інфраструктуру підприємства.

З огляду на зазначене тема дипломної роботи є актуальною, а використання її результатів сприятиме підвищенню рівня інформаційної безпеки підприємницької діяльності.

Мета і завдання дослідження. **Мета роботи** полягає у дослідженні засад політики інформаційної безпеки як основи управління інформаційною безпекою на підприємстві.

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

1. Провести аналіз основ управління інформаційною безпекою підприємства.
2. Дослідити особливості політик інформаційної безпеки сучасних підприємств.
3. Визначити рекомендації щодо політики інформаційної безпеки на підприємстві.

Об’єкт дослідження – інформаційна безпека підприємства. **Предмет дослідження** – політика інформаційної безпеки підприємства як основа управління інформаційною безпекою на підприємстві.

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

Наукова новизна одержаних результатів. Розроблені підходи можуть бути використані при плануванні та реалізації системи управління інформаційною безпекою на підприємстві.

Практичне значення одержаних результатів. Застосування напрацювань дадуть змогу здійснити обґрунтований вибір методів і засобів щодо впровадження політики інформаційної безпеки на підприємстві.

Розділ 1
ОСНОВИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА

1.1 Концепція інформаційної безпеки підприємства

Інформаційна безпека – це стан захищеності систем обробки і зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації, використання й розвиток в інтересах громадян або комплекс заходів, спрямованих на забезпечення захищеності інформації особи, суспільства і держави від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки запису чи знищення (у цьому значенні частіше використовують термін «захист інформації»).

Інформаційна безпека держави характеризується ступенем захищеності і, отже, стійкістю основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи, суспільної свідомості і т. д.) стосовно небезпечних (дестабілізаційних, деструктивних, суперечних інтересам країни тощо), інформаційним впливам, причому як до впровадження, так і до вилучення інформації.

Концепція інформаційної безпеки в організації викладає систему поглядів, основних принципів, розкриває основні напрями забезпечення безпеки інформації. Розроблення концепції здійснюється після розгляду повної структури організації і виконується на підставі аналізу наступних чинників:

- правових і (або) договірних засад;
- вимог до забезпечення безпеки інформації згідно з завданнями і функціями організації;
- загроз, яким зазнають впливу ресурси організації, що підлягають захисту.

За результатами аналізу мають бути сформульовані загальні положення безпеки, які стосуються або впливають на технологію зберігання, оброблення та передавання інформації у організації:

- мета та пріоритети, яких необхідно дотримуватись у організації під час забезпечення інформаційної безпеки;
- загальні напрями діяльності, необхідні для досягнення цієї мети;
- аспекти діяльності у галузі безпеки інформації, які повинні вирішуватися на рівні організації в цілому;
- відповідальність посадових осіб та інших суб’єктів взаємовідносин у організації, їхні права і обов’язки щодо реалізації завдань інформаційної безпеки.

1.2 Аналіз та оцінка ризиків інформаційної безпеки підприємства

Аналіз ризиків передбачає вивчення моделі загроз для інформаційної сфери організації та моделі порушників, можливих наслідків від реалізації потенційних загроз (рівня можливої заподіяної ними шкоди) і формування на його підставі моделі захисту інформації у організації. Під час проведення аналізу ризиків необхідним є виконання наступних робіт.

Визначення компонентів і ресурсів організації, які необхідно враховувати при аналізі. Повинні бути визначені критичні з точки зору безпеки компоненти і ресурси організації, які можуть бути об'єктами атаки або самі є потенційним джерелом порушення безпеки інформації (об'єкти захисту). Для цього використовуються відомості, одержані в результаті обстеження середовищ функціонування організації.

Ідентифікація загроз з об'єктами захисту. Встановлюється відповідність моделі загроз і об'єктів захисту, тобто складається матриця загрози/компоненти (ресурси) організації. Кожному елементу матриці повинен бути зіставлений

опис можливого впливу загрози на відповідний компонент або ресурс організації. У процесі упорядкування матриці може уточнюватися список загроз і об'єктів захисту, внаслідок чого коригуватись модель загроз.

Оцінка ризиків. Повинні бути отримані оцінки гранично припустимого й існуючого (реального) ризику здійснення кожної загрози впродовж певного проміжку часу, тобто ймовірності її здійснення впродовж цього інтервалу. Для оцінки ймовірності реалізації загрози рекомендується вводити декілька дискретних ступенів (градацій). Оцінку слід робити за припущення, що кожна подія має найгірший, з точки зору власника інформації, що потребує захисту, закон розподілу, а також за умови відсутності заходів захисту інформації. На практиці для більшості загроз неможливо одержати достатньо об'єктивні дані про ймовірність їхньої реалізації і доводиться обмежуватися якісними оцінками. У цьому випадку значення ймовірності реалізації загрози визначається в кожному конкретному випадку експертним методом або емпіричним шляхом, на підставі досвіду експлуатації подібних систем, шляхом реєстрації певних подій і визначення частоти їхнього повторення тощо

Оцінка може мати числове або смислове значення (наприклад, ймовірність реалізації загрози – незначна, низька, висока, неприпустимо висока).

У будь-якому випадку існуючий ризик не повинен перевищувати гранично допустимий для кожної загрози. Перевищення свідчить про необхідність впровадження додаткових заходів захисту. Мають бути розроблені рекомендації щодо зниження ймовірності виникнення або реалізації загроз та величини ризиків.

Оцінювання величини можливих збитків, пов'язаних з реалізацією загроз. Виконується кількісна або якісна оцінка збитків, що можуть бути нанесені організації (організації) внаслідок реалізації загроз. Доцільно, щоб ця оцінка складалась з величин очікуваних збитків від втрати інформацією кожної з властивостей (конфіденційності, цілісності або доступності) або від втрати керованості організації внаслідок реалізації загрози. Для одержання оцінки

можуть бути використані такі ж методи, як і при аналізі ризиків. Величина можливих збитків визначається розміром фінансових втрат або, у разі неможливості визначення цього, за якісною шкалою (наприклад, величина збитків – відсутня, низька, середня, висока, неприпустимо висока).

1.3 Визначення політики інформаційної безпеки підприємства

Об'єктивно категорія «інформаційна безпека» виникла з появою засобів інформаційних комунікацій між людьми, а також з усвідомленням людиною наявності у людей і їхніх співтовариств інтересів, яким може бути завдано збитку шляхом дії на засоби інформаційних комунікацій, наявність і розвиток яких забезпечує і задає інформаційний обмін між всіма елементами соціуму.

Необхідність у політиці безпеки на сьогоднішній день є очевидним фактом для будь-якого навіть достатньо невеликого підприємства. Політика безпеки в цілому – це сукупність програмних, апаратних, організаційних, адміністративних, юридичних, фізичних заходів, методів, засобів, правил і інструкцій, які чітко регламентують усі аспекти діяльності підприємства, включаючи інформаційну систему, та забезпечують їх безпеку.

Крім свого прямого призначення, політика безпеки має ще один корисний ефект: у результаті аналізу інформаційних потоків, інвентаризації інформаційних ресурсів та ранжирування інформації, яка оброблюється, передається або зберігається, за мірою її цінності керівництво підприємства одержує цілісну картину одного з найбільш складних об'єктів – інформаційної системи, що позитивно впливає на якість керування бізнесом у цілому, і, як наслідок, покращує його прибутковість і ефективність

Політику інформаційної безпеки організації можна визначити як сукупність вимог та правил з інформаційної безпеки організації для об'єкта інформаційної безпеки організації, вироблених з метою протидії заданій множині загроз інформаційній безпеці організації із урахуванням цінності

інформаційної сфери, що підлягає захисту та вартості системи забезпечення інформаційної безпеки.

Під час розробки політики безпеки повинні бути враховані технологія зберігання, оброблення та передавання інформації, моделі порушників і загроз, особливості апаратно-програмних засобів, фізичного середовища та інші чинники. У організації може бути реалізовано декілька різних політик безпеки, які істотно відрізняються.

Як складові частини загальної політики безпеки у організації мають існувати політики забезпечення конфіденційності, цілісності, доступності оброблюваної інформації. Політика безпеки повинна стосуватись: інформації (рівня критичності ресурсів організації), взаємодії об'єктів (правил, відповідальності за захист інформації, гарантій захисту), області застосування (яких складових компонентів організації політика безпеки стосується, а яких – ні).

Політика безпеки має бути розроблена таким чином, що б вона не потребувала частої модифікації (потреба частої зміни вказує на надмірну конкретизацію, наприклад, не завжди доцільно вказувати конкретну назву чи версію програмного продукту).

Політика безпеки повинна передбачати використання всіх можливих заходів захисту інформації, як-то: правові та морально-етичні норми, організаційні (адміністративні), фізичні, технічні (апаратні і програмні) заходи і визначати правила та порядок застосування у організації кожного з цих видів.

Політика безпеки повинна базуватися на наступних основних принципах:

- системності;
- комплексності;
- неперервності захисту;
- достатності механізмів і заходів захисту та їхньої адекватності загрозам;
- гнучкості керування системою захисту, простоти і зручності її використання;

- відкритості алгоритмів і механізмів захисту, якщо інше не передбачено окремо.

Методологія розроблення політики безпеки організації включає в себе наступні роботи:

• розробка концепції безпеки інформації у організації;

• аналіз ризиків;

• визначення вимог до заходів, методів та засобів захисту;

• вибір основних рішень з забезпечення безпеки інформації;

• організація виконання відновлювальних робіт і забезпечення не-перервного функціонування організації;

• документальне оформлення політики безпеки.

Висновки до першого розділу

Концепція інформаційної безпеки складає систему поглядів, основних принципів, розкриває основні напрями забезпечення безпеки інформації.

Аналіз ризиків передбачає вивчення моделі загроз для інформаційної сфери організації та моделі порушників, можливих наслідків від реалізації потенційних загроз (рівня можливої заподіяної ними шкоди) і формування на його підставі моделі захисту інформації у організації.

Політику з інформаційної безпеки організації можна визначити як сукупність вимог та правил з інформаційної безпеки організації для об'єкта інформаційної безпеки організації, вироблених з метою протидії заданій множині загроз інформаційній безпеці організації із урахуванням цінності інформаційної сфери, що підлягає захисту та вартості системи забезпечення інформаційної безпеки.

Розділ 2
ОСОБЛИВОСТІ ПОЛІТИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СУЧАСНИХ ПІДПРИЄМСТВ

2.1 Політика інформаційної безпеки банківських установ

2.1.1 Сутність політики інформаційної безпеки банків

Політика інформаційної безпеки банку – сукупність правових і морально-етичних норм, правил, адміністративних, організаційних заходів і технічних, програмних і криптографічних засобів, направлених на захист інформаційної інфраструктури банку від випадкового і навмисного втручання в процес її функціонування. Політика формується на основі характеристики об'єкта застосування; аналізу поточного стану захищеності інформаційної інфраструктури банку; обліку можливих негативних факторів впливу та ймовірності їх реалізації; створення методології ухвалення управлінських рішень щодо забезпечення інформаційної безпеки з врахуванням вимог, що містяться в законах і нормативних актах держави, міжнародних, національних та промислових стандартах у галузі інформаційної безпеки, нормативних документах державного і відомчого характеру.

Розрізняють дві системи оцінки поточної ситуації у сфері інформаційної безпеки у банківських установах:

- «дослідження знизу догори» (прямий);
- «дослідження зверху вниз» (зворотній).

Метод «знизу догори» досить простий, потребує набагато менших капітальних вкладень, але й має менші можливості. Він базується на відомій схемі: «Ви – зловмисник. Ваші дії?» Тобто служба інформаційної безпеки банку, ґрунтуючись на даних про всі відомі види атак, намагається застосувати

їх на практиці з метою перевірки, чи можлива така атака з боку реального зловмисника.

Метод «зверху вниз» є, навпаки, детальним аналізом усієї наявної схеми зберігання та обробки інформації. Першим етапом цього методу є, як і завжди, визначення, які інформаційні об’єкти і потоки необхідно захищати. Далі вивчають поточний стан системи інформаційної безпеки з метою визначення того, що з класичних методик захисту інформації вже реалізоване, в якому обсязі та на якому рівні. На третьому етапі розробляється класифікація всіх інформаційних об’єктів на класи відповідно до їх конфіденційності, вимог до доступності та цілісності (незмінності). На четвертому етапі з’ясовують, наскільки серйозний збиток може завдати банку розкриття або інша атака на кожний конкретний інформаційний об’єкт. Цей етап носить назву «розрахунок ризиків». У першому наближенні ризиком є добуток «можливого збитку від атаки» на «ймовірність такої атаки». Є безліч схем обчислення ризиків.

Залежно від стану інформаційної безпеки в банку виділимо чотири основні типи політики інформаційної безпеки банку:

1. Програмна політика безпеки використовуються при оцінці стану інформаційної небезпеки в банку і розробляється з метою визначення напрямів реструктуризації основних компонентів забезпечення інформаційної безпеки і їх реалізації. Програмна політика безпеки банку визначає множину стратегічних напрямків забезпечення інформаційної безпеки, види і обсяг ресурсів, які виділяються для реалізації політики;

2. Формування проблемно-орієнтованої політики інформаційної безпеки банку здійснюють у випадку інформаційної загрози в банку. Об’єктом застосування проблемно-орієнтованої політики безпеки є окрема проблема або задача в області забезпечення безпеки інформації в фінансово-кредитній організації. Необхідність розробки проблемно-орієнтованої політики безпеки часто вимагає у відповідь як появу і використання в організації нових технологій, так і виникнення нових загроз та слабкостей. Частіше за все

проблемно-орієнтована політика безпеки уточнює, конкретизує положення програмної політики безпеки чи об’єктової політики безпеки;

3. Системно-орієнтована політика інформаційної безпеки банку використовується при стані інформаційного ризику, визначає напрямок, методи та процедури забезпечення інформаційної безпеки. Даний тип політики обмежений областю взаємодії самої системи і середовища її експлуатації. Для розробки пов’язаного та повного набору правил безпеки розробник повинен використовувати спеціальні прийоми, за допомогою яких на основі аналізу задач захисту формулюються правила безпеки;

4. Системна політика містить загальні вимоги до безпеки інформації та рішення щодо забезпечення режиму інформаційної безпеки. Повинна містити правила безпеки відносно фізичної безпеки, аутентифікація, ідентифікації та управління доступом, правила застосування криптографічних засобів, правила забезпечення антивірусного захисту та інші питання моніторингу актуальності сформульованих та уточнених задач захисту в процесі експлуатації системи (стан інформаційної безпеки банку).

Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України, затверджене постановою правління Національного банку України від 28 вересня 2017 року № 95 зобов’язує банки:

•розробити та впровадити політику інформаційної безпеки, яка має містити:

1) цілі інформаційної безпеки;

2) сферу застосування політики інформаційної безпеки;

3) принципи, правила та вимоги інформаційної безпеки в банку;

4) визначення функцій (ролей) і відповідальності за забезпечення інформаційної безпеки;

•забезпечити підтримку політики інформаційної безпеки в актуальному стані та її перегляд не рідше ніж один раз на рік;

•затвердити політику інформаційної безпеки і довести її зміст до відома всього персоналу банку та, за необхідності, представникам третіх сторін;

•розробити та затвердити стратегію розвитку інформаційної безпеки. Банк має право затвердити стратегію розвитку інформаційної безпеки банку в документі, яким затверджено загальну стратегію розвитку банку, у вигляді окремого розділу. Зміст стратегії має узгоджуватися з політикою інформаційної безпеки банку, основними стратегічними цілями банку, що пов'язані із впровадженням нових бізнес-процесів/банківських продуктів з використанням технологій, які потребують захисту інформації, а також враховувати планування розвитку інфраструктури банку та заходів інформаційної безпеки для мінімізації ризиків інформаційної безпеки.

Розглянемо ієрархічний підхід до впровадження інформаційної політики банківської установи (рис. 1.1).

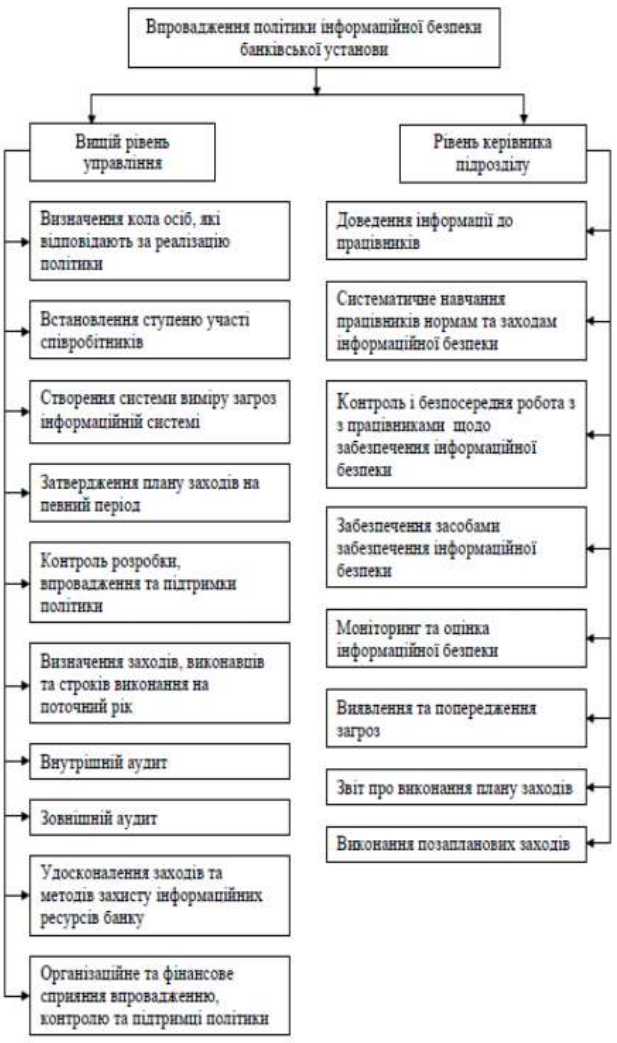

Рис. 1.1. Ієрархічний підхід до впровадження інформаційної політики банківської установи

Політика інформаційної безпеки банківських установ повинна розроблятися відповідно до вимог чинних законодавства, нормативно-правових актів, міжнародних стандартів у сфері інформаційної безпеки та внутрішніх нормативних документів банку.

Керівництво банку повинно розуміти, що інформаційна безпека є основою для нормального функціонування банку, та всебічно сприяти виконанню політики інформаційної безпеки.

Для забезпечення інформаційної безпеки банківської установи необхідно застосовувати комплекс заходів, яких повинен дотримуватися кожен працівник банку, виходячи з покладених на нього обов'язків та визначеними правилами згідно політики інформаційної безпеки банку.

Політика інформаційної безпеки банку повинна мати процедури для взаємодії з зовнішніми організаціями, до яких входять правоохоронні органи, інші організації, команди швидкого реагування, засоби масової інформації. У процедурах повинно бути визначено, хто має право на такі контакти, і як саме вони відбуваються.

Крім положень політики безпеки, описаних вище, необхідно продумати і описати процедури, що виконуються у випадку виявлення порушень правил безпеки. Для всіх видів порушень мають бути заготовлені відповідні процедури.

Інформаційну систему банку можна вважати захищеною, якщо всі операції виконуються згідно із суворо визначеними правилами безпеки (рис. 1.2), що забезпечують безпосередній захист об'єктів, ресурсів і операцій.

Рис. 1.2. Основні правила забезпечення політики безпеки в інформаційній системі

Основу для формування вимог до захисту складає список загроз. Коли такі вимоги відомі, можуть бути визначені відповідні правила забезпечення захисту, що визначають необхідні функції і засоби захисту. Чим суворішими є вимоги до захисту і більше відповідних правил, тим ефективніші її механізми і тим більше захищеною виявляється інформаційна система.

Очевидно, що будь-яка офіційна політика безпеки час від часу порушується. Порушення може бути наслідком недбалості користувачів, випадкової помилки, відсутності надійної та належної інформації про поточну політику чи її нерозуміння. Можливо, також, що деяка особа – група осіб свідомо роблять дії, що прямо суперечать затвердженій політиці безпеки.

Необхідно заздалегідь визначити характер дій, що починаються у випадку виявлення порушень політики інформаційної безпеки, щоб ці дії були швидкими й правильними. Варто організувати розслідування, щоб зрозуміти, як і чому порушення стало можливим. Після цього потрібно внести коригування в систему захисту. Тип і серйозність цих коригувань залежить від типу порушення, яке сталося.

Дотримання політики інформаційної безпеки повинно бути обов’язковим для усіх співробітників. Документи щодо системи управління інформаційною безпекою повинні бути доступними працівникам банку лише у межах їх

обов’язків і повноважень. Кожний працівник банківської установи несе відповідальність за порушення правил згідно з чинним законодавством та внутрішніми нормативними документами.

2.1.2 Перегляд політики інформаційної безпеки банків

Звичайно, неможливо побудувати ідеальну політику інформаційної безпеки банківської установи, оскільки банк це відкрита установа з тисячами клієнтів. З часом усе змінюється: устрій життя, нормативно-законодавча база, модернізується обладнання, змінюється програмне забезпечення, розвиваються технології, а водночас і шкідливе програмне забезпечення, змінюється обслуговуючий персонал.

Отже, політика інформаційної безпеки банку має доповнюватися і змінюватися згідно з критеріями змін і цінності інформації, що підлягає захисту, у зв’язку із впровадженням нових інформаційних технологій та змін у нормативно-правових актах України, також у внутрішніх нормативних документах та іншими чинниками.

Політика інформаційної безпеки повинна переглядатись у заплановані терміни або за появи істотних змін з метою забезпечення її постійної придатності, адекватності та ефективності.

Політика інформаційної безпеки повинна мати власника, який несе затверджену керівництвом відповідальність за розвиток, перегляд і оцінювання політики безпеки. Перегляд повинен охоплювати оцінку можливостей вдосконалення політики інформаційної безпеки організації і підхід до управління інформаційною безпекою в разі змін інфраструктури організації, бізнес-обставин, правових умов або технічної інфраструктури.

Перегляд політики інформаційної безпеки повинен враховувати результати переглядів з боку керівництва. Повинні бути визначені процедури перегляду з боку керівництва, включаючи графік або періодичність перегляду.

2.1.3 Реалізація політики інформаційної безпеки банків

Реалізація політики інформаційної безпеки банків починається з проведення розрахунку фінансових втрат і вибору відповідних засобів для виконання завдань із захисту інформаційної системи банку. При цьому необхідно врахувати такі фактори як безконфліктність роботи обраних засобів, репутація постачальників засобів захисту, можливість одержання повної інформації про механізми захисту і надані гарантії. Також варто враховувати основні положення з безпеки інформації:

- економічна ефективність – вартість засобів захисту має бути меншою, ніж розміри можливого збитку;
- кожен користувач повинний мати мінімальний набір привілеїв, необхідний під час роботи;
- простота системи захисту інформаційної системи – захист буде тим ефективнішим, чим легше користувачу з ним працювати;
- відключення захисту при нормальному функціонуванні – захист не повинен відключатися, за винятком особливих випадків, коли співробітник із спеціальними повноваженнями може мати можливість відключити систему захисту;
- відкритість проектування і функціонування механізму захисту (для можливості адекватного реагування обслуговуючого персоналу на виникнення збоїв у системі);
- незалежність системи захисту від суб’єктів захисту – розроблювачами не повинні бути ті, кого вона буде контролювати;
- загальний контроль без будь-яких виключень з безлічі контрольованих суб’єктів;
- звітність і підконтрольність системи захисту;
- відповідальність осіб, що займаються інформаційною безпекою;

- об’єкти захисту доцільно розділити на групи так, щоб порушення захисту в одній групі не впливало на безпеку інших груп;
- відмова від замовчування – при збої засобів захисту доступ до обчислювальних ресурсів повинен бути заборонений;
- система захисту об’єкту має бути цілком специфікованою, протестованою та погодженою;
- система повинна допускати зміну своїх параметрів адміністратором;
- важливі критичні рішення повинні прийматися людиною, а не комп’ютером;
- система захисту об’єкта повинна проектуватися в розрахунку на вороже оточення і припускати, що користувачі мають найгірші наміри, будуть робити помилки і шукати шляхи обходу механізмів захисту;
- інформація про існування механізмів захисту повинна бути, по можливості, схована від користувачів, робота яких контролюється.

При підтримці політики інформаційної безпеки банку потрібно постійне спостереження за вторгненнями зловмисників у мережу, виявлення вад і дір у системі захисту інформаційної системи, обліку випадків несанкціонованого доступу до конфіденційних даних. При цьому основна відповідальність за підтримку політики інформаційної безпеки банку лежить на відповідальній особі, призначеній керівництвом банку. Цей фахівець повинен оперативно реагувати на всі випадки зламу конкретної системи захисту, аналізувати їх і використовувати необхідні апаратні та програмні засоби захисту з урахуванням максимальної економії фінансових засобів.

2.2 Політика інформаційної безпеки промислового підприємства

Мета політики ІБ полягає в тому, щоби гарантувати використання за призначенням комп'ютерної техніки і телекомунікаційних ресурсів підприємства її співробітниками, незалежними підрядниками та іншими

користувачами. Всі користувачі корпоративної мережі мають використовувати комп'ютерні ресурси кваліфіковано, ефективно, дотримуючись норм етики і чинного законодавства.

Політика ІБ, її правила і умови стосуються всіх користувачів комп'ютерних і телекомунікаційних ресурсів і служб підприємства, де б ці користувачі не знаходилися. Порушення цієї політики тягне за собою дисциплінарні стягнення, аж до звільнення співробітника і/або притягнення його до кримінальної відповідальності. Політика ІБ може періодично змінюватись і переглядатися в міру потреби.

Отже, політика ІБ промислового підприємства має містити такі рішення та заходи щодо її забезпечення:

● проведення аудиту ІБ та оцінювання захищеності інформаційних ресурсів підприємства, підготовка її інформаційних систем для досягнення відповідності чинних вимог щодо забезпечення ІБ;

● організація комплексної системи захисту інформації, яка знаходиться в інформаційно-управлінській системі виробничо-господарської діяльності підприємства, в яку внесено:

1) комплексний захист від несанкціонованих доступів: управління доступом; реєстрація та облік подій ІБ; забезпечення контролю за цілісності та доступності інформаційних ресурсів; надійний криптографічний захист інформації;

2) забезпечення ІБ між мережевої взаємодії: проведення між мережевого екранування та сегментації доступу до мереж; створення віртуальних приватних мереж; пошук і запобігання вторгнень та ін.;

3) безпечний віддалений доступ до наявних корпоративних інформаційних ресурсів, в т.ч. конкретні мережі та мережі загального доступу;

4) професійний контроль над використанням інформаційних ресурсів;

● захист інформаційно-управлінських систем спільно з:

1) управлінням доступом на прикладному рівні, комплексним розробленням і реалізацією концепції повноважень користувачів;

2) налаштуванням аудиту подій ІБ із під'єднанням до централізованих систем контролю над інцидентами;

3) професійним захистом (безпечним налаштуванням) загальносистемного і спеціалізованого програмного забезпечення;

4) захистом від несанкціонованого доступу, розмежуванням доступу;

● повне налаштування систем захисту інформації в ІС, які призначені для надійного оброблення персональних даних;

● налаштування систем контролю та захисту інформації в АСУ ТП;

● налаштування системи управління ідентифікаційними даними, централізованого управління доступом і забезпечення аутентифікації;

● оперативна доставка і супровід засобів комп'ютерної техніки.

Отже, відповідальність за дотримання політики ІБ підприємства несе кожен її співробітник, при цьому першочерговим завданням є забезпечення безпеки всіх активів підприємства. Це означає, що інформація повинна бути захищена не менш надійно, ніж будь-який інший основний актив компанії. Головні цілі підприємства не можуть бути досягнуті без своєчасного і повного забезпечення співробітників інформацією, необхідною їм для виконання своїх службових обов'язків.

2.3 Політика інформаційної безпеки іноземних підприємств

2.3.1 Огляд політики інформаційної безпеки іноземних підприємств

Сьогодні іноземні підприємства покладаються на дані для здійснення щоденних операцій, проведення аналізу ефективності, оцінки тенденцій на ринку та отримання розуміння для отримання конкурентної переваги. Оскільки дані продовжують відігравати все більш важливу роль у впорядкуванні бізнесу та в зростанні економічності підприємств, вони розглядаються як незамінний актив. Як і всі дорогоцінні активи, інформаційні активи також повинні бути

належним чином використані та забезпечені. Отже, успішні підприємства повинні мати правила та проводити політику, яка захищає інформаційні активи.

У цьому документі висвітлюються основи того, що потрібно для створення ефективної політики безпеки даних для підприємств. У ньому обговорюються властивості даних, що мають відношення до безпеки, основні принципи, які слід враховувати, та формулюються політики відповідно до вашої організації.

Усі розробники політики повинні розуміти дані своєї організації, місію організації, принципи управління даними та формулювати відповідні та практичні політики та стандарти.

2.3.2 Характеристики даних політики інформаційної безпеки для іноземних підприємств

Дані – це актив, який виробляється та споживається майже в усіх бізнес-процесах підприємства. Він не є рівномірним у його придбанні, створенні чи використанні. Існує декілька атрибутів та особливостей таких даних, як якість, цілісність, своєчасність тощо. Однак для визначення правильної політики безпеки даних нижче обговорюються найбільш відповідні характеристики даних.

Нижче наведено деякі основні характеристики, на які слід звернути особливу увагу при формуванні політики безпеки даних:

A. Класифікація даних

Дані повинні бути класифіковані належним чином, щоб заходи захисту даних були ефективними. Це має важливе значення для ефективного вироблення політики та подальшого виконання політики. Не всі дані однакові за важливістю та чутливістю для організації. Метою встановлення заздалегідь визначеної класифікації безпеки даних є забезпечення відповідних механізмів захисту для контролю інформації від витоку, маніпулювання або недоступності.

Зазвичай іноземні організації мають такі класифікації даних, які розрізняють чутливість даних:

1. Загальнодоступне: Інформація, яка може публікуватися і ділитися вільно всередині організації або поза нею. Його можна розміщувати на корпоративних веб-сайтах тощо.

2. Внутрішня компанія: Інформацією можна вільно ділитися всередині організації, але не за її межами.

3. Конфіденційно: Інформація обмежена, і її використання повинно бути дозволено власником даних або її захисником, а його використання обмежується лише даним дозволом.

4. Суворо конфіденційна: високочутлива інформація, яка може мати високі фінансові чи юридичні наслідки для організації, якщо інформація не захищена або порушена. Найбільшою обережністю слід ставитися до цієї класифікації безпеки.

Працівники повинні знати кожну класифікацію безпеки та знати, як застосувати відповідну класифікацію до кожного документа, електронної пошти чи типу даних.

B. Зберігання даних та пристрої

Носії для зберігання даних та пристрої, які збирають та отримують доступ до даних, повинні враховуватись для захисту даних. Під час роботи з комп'ютерами з основним фреймом, до яких звертаються за допомогою німих терміналів, було досить легко забезпечити, де перебувають дані та пристрої, які отримують доступ до них. У сучасному світі доступ до даних здійснюється з настільних комп'ютерів, ноутбуків, мобільних пристроїв та обмінюється між серверами.

Він може зберігатися на будь-якому з пристроїв, що мають доступ до нього, або на серверах і носіях інформації, призначених для роботи сучасних баз даних, сховищ документів та спільних мережевих локацій. Крім того, корпоративні дані можуть необов'язково знаходитись у приміщенні для підприємства, але можуть зберігатися у Хмарі постачальником даних.

Сьогоднішня архітектура даних сильно відрізняється і набагато складніша за те, що було десять-два тому. Різні носії зберігання створюють різні ризики, і політика, що приймається підприємствами, повинна вирішувати всі проблеми. Порушення безпеки даних, здебільшого, може статися з найбільш уразливого пристрою чи носія інформації. Після того, як інформація просочиться, це не матиме значення, де відбувся витік; отже, всі сховища та пристрої повинні охоплюватися всебічною політикою безпеки даних.

C. Використання даних

Дані використовуються для кількох різних цілей на підприємстві. На більшості складних підприємств різні відділи та організаційні підрозділи рідко діють поодинці. Сучасні організації мають бізнес-процеси, в яких задіяно більше одного організаційного підрозділу, і між організаціями існує потік даних для полегшення та виконання робочих процесів. Політика безпеки даних повинна гарантувати, що дані надаються правильним особам, а також, що суб'єкт, який споживає дані, бере належну обережність та обережність при роботі з даними, що належать іншій організації.

2.3.3 Основні принципи політики інформаційної безпеки для іноземних підприємств

Комплексна політика безпеки даних повинна містити такі основні принципи. Перелічені нижче принципи є загальними і не мають тенденції змінюватися з часом. Вони викладають основні істини, які повинні враховувати підприємства, які хочуть захистити свої дані:

A. Допустиме використання

Надати працівникам чіткі однозначні вказівки щодо відповідного використання ресурсів Компанії. Зазвичай працівники вимагають офіційно підписати документ, що підтверджує прийнятну політику використання, перш ніж їм надавати доступ до систем. Інститут SANS описує це як «правила, що захищають працівника та компанію. Нераціональне використання піддає

Компанії ризики, включаючи вірусні атаки, компрометацію систем та послуг та юридичні проблеми ». Політика охоплює електронні та обчислювальні пристрої та інформаційні активи, заохочуючи правильну оцінку та використання відповідно до заявлених вказівок

B. Контроль облікових записів та доступу

Особам, які бажають отримати доступ до корпоративних систем, надається рахунок, захищений паролем. Вони отримують доступ до корпоративних систем, використовуючи обліковий запис для входу в них. Обліковий запис має пільги, необхідні фізичній особі для отримання доступу до інформаційних активів, необхідних йому для ведення бізнесу. Тому вкрай важливо підтримувати контроль над обліковими записами та контролювати їх.

Облікові записи – це те, як ми визначаємо рівень доступу, наданий користувачеві, та їх використання інформаційних активів. Тому перед тим, як отримати доступ до облікового запису, особа повинна підписати документ, згідно з яким він визнає, що буде використовувати обліковий запис для бізнесу компанії та захищати обліковий запис, використовуючи пароль, який відповідає корпоративній політиці. Політика безпеки даних повинна визначати належне використання методів автентифікації, що використовуються для перевірки особи, пов’язаної з обліковим записом.

C. Електронна пошта та комунікація

Електронні листи – це значна частина робочого дня більшості працівників. Це обраний спосіб ділових комунікацій майже на всіх сучасних підприємствах. Компанії повинні чітко заявляти про прийнятну та терпиму поведінку при роботі з корпоративними електронними листами. Це включає забезпечення того, що електронні листи не використовуються для спаму, надсилання несанкціонованого маркетингового контенту чи електронних листів, або надсилання образливих чи дискримінаційних повідомлень. Компанії також можуть викласти відповідні інструкції щодо використання, такі як передача електронної адреси на конференціях або корпоративних заходах або підписка на розсилки, які сприяють професійному зростанню.

D. Віддалений доступ

Глобальні підприємства мають бізнес, щоб дозволити своїм працівникам віддалено отримувати доступ до своїх систем. Відкривати внутрішні системи для доступу з віддалених місць є ризикованим, тому підприємства повинні визначити належні методи доступу до систем, коли вони знаходяться поза приміщеннями Компанії.

Політика спрямована на визначення правил, що мінімізують ризик під час підключення до корпоративної мережі з будь-якого хоста віддаленого доступу. Збитки несанкціонованих осіб, які отримують доступ, можуть бути втратою інтелектуальної власності та конфіденційною інформацією, яка може зашкодити іміджу громадськості або призвести до штрафів та зобов'язань.

E. Реагування на інциденти

Реагування щодо інцидентів стосується чітко визначених кроків та процедур, які будуть діяти у разі порушення безпеки даних. Ніхто не хоче порушення, але вони повинні бути готові у випадку, якщо таке трапиться. Без заздалегідь визначеного плану ваша відповідь буде затримана. Це добре визначити команду, яка буде ефективно реагувати.

«Ключовим фактором для зменшення ризику інциденту безпеки даних є наявність плану реагування на інциденти. План повинен існувати не лише, але і його місце розташування має бути відомим, і план має бути доступним »

F. Безперервність бізнесу

Планування безперервності бізнесу та відновлення після аварій використовується для відновлення служб та відновлення після відключень. Системи неминуче знизяться, і більшість організацій планують забезпечити наявність критично важливих додатків. Безперервність бізнесу - це "здатність організації продовжувати поставляти продукти чи послуги на прийнятних заздалегідь визначених рівнях після руйнівного інциденту".

У політиці безпеки даних ідея полягає у тому, щоб забезпечити доступність даних при переключенні систем з основного на резервне

копіювання. Крім того, доступ користувачів до даних повинен бути ідентичним під час переходу в режим очікування.

G. Управління патчами

Постачальники регулярно випускають патчі для свого програмного забезпечення. Деякі виправлення виправляють помилки, пов’язані з функціональністю, а інші пов'язані із безпекою. Якщо це патч, пов’язаний із безпекою, повинні бути встановлені правила, які доручають його застосуванню виходячи з суворості, встановленої продавцем. Політика повинна диктувати, що критичні виправлення застосовуватимуться в набагато коротші часові рамки, ніж менші за значенням.

Необхідно запровадити політику, щоб забезпечити існування стандартів та процедур щодо застосування програмних виправлень або випусків, пов’язаних із захистом даних. Ці стандарти та процедури включають інформування персоналу служби підтримки розробки програмного забезпечення, щоб гарантувати тестування всіх критичних програм місії та будь-які зміни, вчасно вкладені в дію для закриття будь-якої лазівки, яка може призвести до порушення безпеки даних.

H. Шифрування

Шифрування – це процес кодування (або скремблювання) інформації, щоб її можна було перетворити лише в початковий вигляд (розшифрувати) тим, хто (або щось, що) має правильний ключ розшифровки ».

Шифрування, як правило, називається останньою лінією захисту при порушенні даних. Якщо хакер зможе отримати доступ до інформації, то шифрування не дозволить йому використовувати будь-яку інформацію. Дані будуть скрембліровані, а отже, стануть марними особі, яка отримала несанкціонований доступ до інформаційного ресурсу.

Як правило, шифрування повинно використовуватися для захисту суворо конфіденційної інформації, особливо при передачі даних по мережах для захисту від будь-якого ризику перехоплення. "Там, де суто конфіденційні дані зберігаються в загальнодоступних, хмарних сховищах, дані повинні бути

зашифровані перед зберіганням, щоб переконатися, що постачальник хмарних послуг не може їх розшифрувати».

I. Моніторинг та відповідність

Важливо зберігати пильність щодо безпеки даних. Моніторинг приймає дві форми, коли перша - це операційний центр, який перевіряє наявність несанкціонованого доступу до мереж чи даних, а другий - забезпечення дотримання політики, що застосовується для захисту даних.

Персонал із захисту даних повинен стежити за будь-якими порушеннями даних та вживати заходів якомога раніше. Ця відповідальність, як правило, лежить на центрах безпеки операцій, які цілодобово відстежують мережі та незвичайні дії.

Рекомендується проводити регулярний аудит третьої сторони. "Однак усі процеси дотримання політики мають одне спільне: аудит. Без якогось процесу аудиту не існує механізму оцінки відповідності. " Аудити забезпечують дотримання політики, яка проводиться.

Висновки до другого розділу

Політика інформаційної безпеки банку – сукупність правових і морально-етичних норм, правил, адміністративних, організаційних заходів і технічних, програмних і криптографічних засобів, направлених на захист інформаційної інфраструктури банку від випадкового і навмисного втручання в процес її функціонування.

У політиці інформаційної безпеки промислового підприємства достатньо точно і чітко регламентуються всі моменти використання мережевого обладнання та програмного забезпечення.

Розробники політики інформаційної безпеки іноземних підприємств повинні розуміти дані своєї організації, місію організації, принципи управління даними та формулювати відповідні та практичні політики та стандарти.

Розділ 3
РЕКОМЕНДАЦІЇ ЩОДО ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

3.1 Розробка та реалізація політики інформаційної безпеки

Організації сьогодні більше, ніж будь-коли, залежать від інформаційних технологій (IT), оскільки IT підтримують їх щодня транзакції, а також численні інші важливі ділові функції. На думку Дафті та Грико (2005), «IT повинно бути розглядатися як спосіб підвищення доступності, швидкості та всебічності інформації, яка підтримує процеси прийняття рішень в організації». Однак залежність від IT, на жаль, призвела до збільшення потенційних загроз інформаційним активам організацій.

Опитування про кіберзлочинність 2014 року у США встановлено, що більше збитків було завдано інсайдерськими атаками, ніж за допомогою сторонніх атак із залученням інсайдерського складу Найвищий відсоток збитків у таких випадках: приватні або конфіденційна інформація ненавмисно піддається (82%); конфіденційні записи підлягають компромісу або вкраденню (76%); записи клієнтів компрометовані або вкрадені (71%); записів працівників та вкраденних (63%) (CERT Insider Threat Center, 2014). За результатами цього опитування видно, що організації повинні мати контроль безпеки для забезпечення конфіденційності, цілісності та доступності їх інформації.

У цьому документі стверджується, що одним із важливих механізмів захисту інформаційних активів організацій є формулювання та здійснення ефективної політики інформаційної безпеки.

У літературі міститься багато визначень для політики інформаційної безпеки. Чен та Лі (2014) стверджують, що інформація Політика безпеки використовується керівництвом для розмежування між ними поведінка працівників, яка або дозволена, або заборонена, а також наступні санкції, якщо заборонена поведінка відбувається. З іншого боку, ISO / IEC 27002 (2013)

стверджує, що мета політики захисту інформації – забезпечує управління з направленням та підтримкою відповідно до вимоги та норми бізнесу при роботі з інформаційною безпекою. Як підкреслено в цих двох визначеннях, Зрозуміло, що політика захисту інформації значно сприяє добробуту організації при захисті її інформації. Однак процеси, що беруть участь у розробці та здійсненні ефективної політики інформаційної безпеки важкі в кращому випадку

Існуюча література зосереджується на описі структури та змісту політики безпеки, але, як правило, не в змозі детально описати процеси розробки політики. Отже, для людей, які беруть участь у цьому, мало настанов у розробці політики інформаційної безпеки стосовно процесів, які вони повинні слідувати

Зважаючи на відсутність настанов, розробники такої політики часто використовують політику, розроблену іншими організаціями, комерційно доступні джерела або шаблони, доступні від публічних джерел, такі як Інтернет. Однак документ що має результати, отримані в результаті таких методів, не дадуть належного спрямування для захисту інформації в контексті організації, яку вона повинна захищати. У таких випадках розроблені заяви щодо політики можуть не бути безпосередньо застосовними до ризиків, які вони покликані звести нанівець, і, таким чином, вони не будуть боротись з загрозами безпеки, що є конкретною організацією облицювальної. Маккенна (2010) заявляє, що "На жаль, багато людей із безпеки IT не розуміють ділових ризиків, тому вони закінчуються написання цих величезних політик безпеки, які стосуються захисту всього в цілому".

Процес розробки та впровадження ефективної політики інформаційної безпеки не є прямим кроком, але керується багатьма питаннями, такими як нормативні вимоги, складності нових технологій та зовнішні та внутрішні загрози. В існуючій літературі висвітлюються певні методи розробки та впровадження політики інформаційної безпеки (Anand, 2012; Bayuk, 2009), але ці методи не включають комплексний, інтегрований метод, який деталізує покрокові процеси. Відповідно, цей документ спрямований на пошук проблеми життєвого циклу розвитку політики інформаційної безпеки.

Застосуємо змішаний підхід, поєднуючи як якісні, так і кількісні методи під час збору даних та аналізу даних. По-перше, це якісний підхід під час формального аналізу змісту існуючих теорій та методів розробки політики інформаційної безпеки. По-друге, кількісні дані були зібрані за допомогою опитування.

Змістовний аналіз розробки політики безпеки був проведений з використанням вторинних джерел в літературі з метою глибокого розуміння процесів, необхідних для формування та реалізації політики.

Ці документи є цитованими та поширеними публікаціями з цієї теми в Google Scholar. Це статті журналів, матеріали конференцій та галузеві публікації. Ці 21 вибіркові документи згодом були імпортовані в програмне забезпечення MAXQDA пакету. MAXQDA – це програмне забезпечення, розроблене для комп'ютерного якісного та змішаного методів аналізу даних, тексту та мультимедіа. Кожен документ був кодований окремо, підкреслюючи речення або абзац, в якому згадується процес розробки політики безпеки. Після завершення процесу кодування вийшло всього 42 коди та 568 накопичувальних кодів. Ці коди варіювалися від загального до конкретного. Загальні коди включають, наприклад, "побудова політики безпеки", а конкретні включають "розробляти політику", "писати політику" та "писати процедуру політики". 42 коди, що з'явилися в процесі кодування, були зменшені до десяти кодів, при цьому деякі менші коди об'єднані з аналогічними суміжними кодами. Наприклад, коди, позначені "ідентифікація вразливих місць", "ідентифікація загроз" та "ідентифікація активів, що підлягають захисту", були згруповані під одним кодом під назвою "оцінка ризику", оскільки всі вони були частиною оцінки процесів ризику безпеки.

Основний збір даних включав опитування. Було розроблено та розповсюджено дослідницький інструмент для 400 фахівців з безпеки – 200 у Великобританії та 200 у Сполучених Штатах Америки. Всього 310 фахівців з питань безпеки (182 з Великобританії та 128 із США) відповіли на опитувальник, який проводився за допомогою програмного забезпечення

SurveyMonkey. Професіонали інформаційної безпеки, на яких спрямовано опитування, включали IT-менеджерів, головних службовців інформаційної безпеки та спеціалістів з питань безпеки. Учасників було обрано тому, що вони беруть участь у питаннях інформаційної безпеки у своїй щоденній діяльності, а тому можуть вважати, що вони надають значний вплив на управління інформаційною безпекою у своїх організаціях. Респондентам було запропоновано вказати тип організації, для якої вони працювали. Виявилося, що 41,92% працювали у промисловості; 17,69% в уряді; 14,23% у банківському секторі; 13,46% у консалтинговому секторі; та 12,69% у торговому секторі. Крім того, респондентів попросили вказати кількість працівників, які працюють у їх організації. Отримані результати показали, що 35,71% працювали в організаціях, які мають менше 500 працівників; 25,65% для організацій, що мають від 500 до 1000 працівників; 23,70% для організацій, що мають від 1000 до 5000 працівників; 6,17% для організацій, що мають від 5000 до 10000 працівників, і 8,77% для організацій, які мають понад 10 000 працівників. Отримані результати також показали, що 62% респондентів були чоловіками, а 38% - жінками.

Анкета опитування ґрунтувалася насамперед на результатах контент-аналізу, проведеного за вторинними даними. Крім того, анкета містила відкриті запитання, які давали респондентам можливість відповісти власними словами. Респондентам було запропоновано запропонувати пропозиції щодо процесів розробки та впровадження політики інформаційної безпеки, які вони вважали важливими, але які не були включені до анкети. Анкета також включала закриті запитання за шкалою типу Лікерта, що обмежили респондентів вибирати відповіді з попередньо визначеного набору

При цьому, використовувався змішаний методичний підхід, який поєднував якісні та кількісні дані. За даними Johnson and Onwuegbuzie (2004), змішані методи дослідження включають змішування або поєднання кількісних і якісних методів дослідження, методів, підходів, концепцій або мови в одному дослідженні.

Боррего та ін. (2009) констатують, що «так само суворий статистичний аналіз є важливим у кількісних дослідженнях для забезпечення надійності та загальної спроможності результатів, так також багатий опис контексту та досвіду учасників має важливе значення в якісних дослідженнях для забезпечення надійності». У цьому документі надійність була забезпечена, оскільки конструкції були оцінені експертами з безпеки. Учасників було обрано цілеспрямовано (цілеспрямований зразок) для їх участі у питаннях безпеки, пов'язаних із повсякденною діяльністю, і тому вони розглядалися як насичена інформацією.

Крім того, Лінкольн та Губа (1985) пропонують чотири критерії надійності:

- Достовірність - це стосується впевненості у «правдивості» висновків. Критичні та конструктивні відгуки опитаних експертів з питань безпеки дозволили вдосконалити цей внесок у дослідження.
- Переносимість - це означає, що отримані результати можуть бути застосовані і в інших контекстах. Запропонований ISPDLC пропонує керівні принципи, якими можуть дотримуватися організації з метою вдосконалення механізмів розробки політики інформаційної безпеки.
- Надійність - це показує, що результати є послідовними. Дані, використані в цій роботі, були отримані з безлічі джерел, і результати підтверджувались літературою, існуючими теоріями та емпіричними результатами.
- Підтверджуваність - це стосується ступеня нейтральності або того, наскільки результати дослідження формуються респондентами, а не упередженістю, мотивацією чи зацікавленістю дослідника.

У таблиці 3.1. наведені результати статистики надійності всіх комбінованих конструкцій.

Як видно з таблиці 1 (рис. 3.1.), альфа Кронбаха становила 0,943 для всіх комбінованих конструкцій. Крім того, альфа Кронбаха була використана для

Table 1 – Reliability statistics (Cronbach's alpha).

Item	Combined constructs	RA	PC	PI	PCO	PM	MS	ES
Cronbach's alpha	.943	.907	.916	.894	.909	.898	.904	.900
No items	7	4	4	4	4	4	4	4

Рис. 3.1. Статистика надійності

встановлення внутрішньої узгодженості питань, що стосуються змінних кожної конструкції. Альфа Кронбаха має високу силу, таким чином, вимірюючи те, чого вони очікують від цих змінних, коливалася від 0,916 (найвищої) до 0,894 (найнижчий). Це, в свою чергу, вказує на те, що змінні, задані в анкеті стосовно всіх об'єднаних конструкцій, були одночасно надійними та послідовними. Значення альфа Кронбаха 0,7 або більше вважається прийнятним.

Проведений принциповий компонентний факторний аналіз на всіх комбінованих конструкціях. У таблиці 2 (рис. 3.2) наведені результати факторного аналізу.

Крім того, для змінних кожної конструкції було також виконано принциповий компонентний факторний аналіз. Як показано в таблиці 3 (рис. 3.1.), результати факторного аналізу для всіх об'єднаних конструкцій та їх змінних варіювали від 0,925 (найвищий) до 0,831 (найнижчий). Отже, факторний аналіз показав, що всі шкали виявилися дуже достовірними, таким чином, вимірюючи те, що вони очікують для вимірювання.

Навантаження розміром 0,5 і більше представляють предмети практичного значення.

Десять рамкових кодів ґрунтуються на інтеграції існуючих методів розробки та впровадження політики інформаційної безпеки, знайдених у сучасній літературі, а також на вкладах опитаних фахівців з питань безпеки. Отримані результати виявили різні кодекси, які повинні враховувати організації під час розробки та впровадження ефективної політики інформаційної безпеки. Рис. 3.3 містить останні десять кодів запропонованої рамки.

Table 2 – Combined constructs factor matrix (validity).

Item	RA	PC	PI	PCO	PM	MS	ES
Loading	.850	.886	.885	.875	.859	.884	.870

Table 3 – Items factor matrix.

Item	Loading
RA1	.897
RA2	.925
RA3	.892
RA4	.861
PC1	.893
PC2	.884
PC3	.901
PC4	.862
PI1	.831
PI2	.903
PI3	.893
PI4	.860
PCO1	.878
PCO2	.894
PCO3	.890
PCO4	.884
PM1	.872
PM2	.861
PM3	.892
PM4	.874
MS1	.879
MS2	.900
MS3	.890
MS4	.857
ES1	.877
ES2	.886
ES3	.882
ES4	.866

Рис. 3.2. Комбінована матриця факторів та елементи факторної матриці

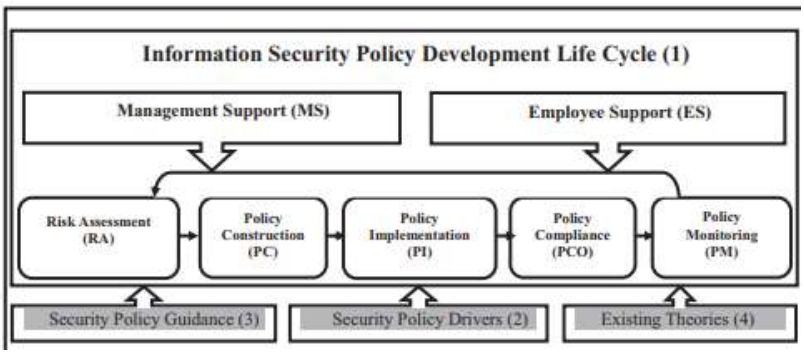

Рис. 3.3. Структура розробки політики

Розмірковуючи про різні коди, зображені на рис. 3.3, стало зрозуміло, що сім кодів – а саме оцінка ризиків, побудова політики, реалізація політики, дотримання політики, моніторинг політики, управління та підтримка працівників – охоплюють усі процеси, необхідні для розробки та впровадження

політика інформаційної безпеки. Таким чином, ці коди становили життєвий цикл розвитку політики безпеки інформації.

Другий компонент (Драйвери політики безпеки) складався з трьох кодів. Цей компонент складається із загроз, які чинять тиск на організацію, щоб застосовувати механізми захисту інформації. Абдель-Азіз (2010) зазначає, що "перш ніж обговорювати політику інформаційної безпеки та процес її оцінки, важливо знати, що в першу чергу сприяє інформаційній безпеці". Розробка політики інформаційної безпеки визначається як зовнішніми, так і внутрішніми впливами, які чинять тиск на організацію, щоб створити механізми захисту інформації організації. Внутрішні загрози включають працівників-інсайдерів, які наражають інформацію організації, а зовнішні загрози включають хакерів. Крім того, існує необхідність дотримання розповсюджених законодавчих вимог уряду.

Третій компонент (Посібник з політики безпеки) складається із стандартів безпеки, що керують організаціями при розробці політики інформаційної безпеки. Як було обговорено, міжнародні стандарти безпеки, такі як ISO / IEC 27002 (2013), використовуються як основний посібник на початковому етапі розробки політики інформаційної безпеки.

Нарешті, організаціям потрібно використовувати відповідні існуючі теорії, щоб зрозуміти поведінкові наміри працівників щодо відповідності політиці інформаційної безпеки. Аналіз контенту показав, що загальна теорія стримування (GDT) та теорія планової поведінки (TPB), серед інших, є ключовими теоріями для розуміння поведінкових намірів працівників дотримуватися політики інформаційної безпеки організації. TPB пояснює, що на намір індивіда виконати задану поведінку впливає ставлення, суб'єктивні норми та сприйнятий поведінковий контроль. З іншого боку, GDT прогнозує, що збільшення суворості покарання, призначеного тим, хто порушує правила організації, зменшує певні злочинні діяння.

Вищепроаналізовані чотири компоненти складають основні стовпи розвитку політики інформаційної безпеки та процесу впровадження. Сім конструкцій компонентів, а саме – Оцінка ризику (РА), Політика побудови (ПК), Впровадження політики (РІ), Дотримання політики (РСО), Моніторинг політики (РМ), Підтримка управління (MS) та Підтримка працівників (ES), були оцінені на основі результатів опитування. Програмне забезпечення, що використовується для проведення статистичного аналізу, SPSS.

Після введення даних в SPSS можна провести різні статистичні випробування. Описові статистичні тести були використані для генерації частот, медіани, середнього та стандартного відхилень. У таблиці 4 (рис. 3.4) представлена описова статистика конструкцій із середніми значеннями, розташованими від найвищих до найнижчих

Table 4 – Descriptive statistical results of the ISPDLC component.

	N	Mean	Median	Std. deviation
Risk assessment (RA)	308	4.1623	3.0000	1.04909
Policy construction (PC)	308	4.0032	3.0000	1.01294
Policy implementation (PI)	307	4.0130	3.0000	1.00318
Policy compliance (PCO)	307	4.0749	3.0000	.93808
Policy monitoring (PM)	307	3.9644	3.0000	1.07602
Management support (MS)	309	4.0814	3.0000	.97177
Employee support (ES)	309	4.0615	3.0000	.98335

Рис. 3.4. Описові статистичні результати компонентів

Як показано в таблиці 4 (рис. 3.4), середнє значення всіх конструкцій було вище 3 – середнє значення за п'ятибальною шкалою. Відповідно, результати описової статистики показали, що в цілому респонденти погодилися з важливістю всіх конструкцій компонентів. Загальні результати опитування показали, що Оцінка ризику є найважливішою конструкцією різних вимірюваних конструкцій.

Цей результат є очевидним, враховуючи, що головна причина розробки політики інформаційної безпеки полягає у пом'якшенні різних ризиків для безпеки, з якими стикаються організації. Другим найважливішим конструктом

була підтримка управління. Управління відіграє важливу роль у прийнятті рішень в організації, особливо щодо затвердження бюджету та затвердження політики та захисту інформації. Отримані результати також виявили, що респонденти вважають, що дотримання політики та підтримка працівників є важливими кроками для включення в процес розробки та впровадження інформаційної безпеки. Загальні результати показали, що моніторинг політики є найменш важливим з вимірюваних конструкцій. Формальний аналіз контенту виявив подібні результати, а моніторинг інформаційної безпеки показав найнижчу частоту тегів порівняно з іншими конструкціями.

У таблиці 5 (рис. 3.5) представлена описова статистика, що стосується змінних оцінок ризику, середні значення яких розташовані від найвищих до найнижчих.

Table 5 – Results of Risk Assessment variables.

	N	Mean	Median	Std. deviation
Vulnerabilities and threats	309	4.1392	3.0000	.98201
Assets identification	310	4.0774	3.0000	.96230
Legislation	308	4.0714	3.0000	.94547
Risk identification	308	4.0455	3.0000	.96412

Рис. 3.5. Результати змінних оцінок ризику

З таблиці 5 (рис. 3.5) видно, що середнє значення було вище 3, що свідчить про те, що респонденти вважали всі чотири змінні важливими. Процес ідентифікації вразливих місць та загроз мав найвищий середній показник 4,1392. Це свідчить про те, що респонденти вважали цей процес дуже важливим порівняно з іншими процесами конструкції оцінки ризиків.

У таблиці 6 (рис. 3.6) наведена описова статистика, що відноситься до змінних «Побудова політики».

Як зазначено в таблиці 6 (рис. 3.6), результати показали, що середнє значення було вище 3. Розробка детальної політики безпеки мала найвищу середню 3,9804, що свідчить про те, що респонденти вважають, що цей процес є дуже важливим порівняно з іншими процесами побудови політики побудувати

Table 6 – Results of the Policy Construction variables.

	N	Mean	Median	Std. deviation
Write detailed security policy	306	3.9804	3.0000	.93015
Write high level security policy	309	3.9612	3.0000	.97623
Consultation with stakeholders	307	3.9609	3.0000	.90664
Write lower level security policy	307	3.8567	3.0000	1.03168

Рис. 3.6. Результати змінних «Побудова політики»

У таблиці 7 (рис. 3.7) представлені описові статистичні дані, що відносяться до змінних Побудова політики, середні значення яких розташовані від найвищого до нижнього.

Table 7 – Results of Policy Implementation variables.

	N	Mean	Median	Std. deviation
Role of stakeholders	309	4.0550	3.0000	.97379
Security policy education	309	4.0356	3.0000	.99121
Security policy training	309	3.9385	3.0000	.95658
Security policy awareness	310	3.7968	3.0000	.99870

Рис. 3.7. Результати змінних щодо впровадження політики

Таблиця 7 (рис. 3.7) ілюструє, що середнє значення було вище 3, що показує, що респонденти вважали всі чотири змінні важливими. Визначення ролі зацікавлених сторін було найвищим середнім показником – 4.0550, що свідчить про те, що респонденти вважають, що цей процес є дуже важливим порівняно з іншими процесами конструкції з реалізації політики.

У таблиці 8 (рис. 3.8) представлена описова статистика, що стосується змінних дотримання політики.

У таблиці 8 (рис. 3.8) представлена описова статистика, що стосується дотримання політики. Видно, що середнє значення було вище 3 – середнє значення за п'ятибальною шкалою. Знання постали як важлива змінна з найвищим середнім рівнем 3,9934, таким чином вказуючи на те, що

респонденти вважають цей процес дуже важливим порівняно з іншими процесами конструкції дотримання політики.

Table 8 – Results of the Policy Compliance variables.

	N	Mean	Median	Std. deviation
Knowledge	305	3.9934	3.0000	.90682
Attitude	308	3.9838	3.0000	.89683
Perceived benefit	307	3.9772	3.0000	.90900
Perceived social pressure	307	3.9739	3.0000	.95279

Рис. 3.8. Результати змінних на відповідність політиці

У таблиці 9 (рис. 3.9) представлені описові статистичні дані, що відносяться до змінних моніторингу політики та оцінки, середні значення яких розташовані від найвищих до найнижчих.

Table 9 – Results of Policy Monitoring variables.

	N	Mean	Median	Std. deviation
Periodical review	308	4.0162	3.0000	.97346
Audit information	310	4.0161	3.0000	.96024
Non periodical review	307	3.9935	3.0000	.95996
Automated review	306	3.9052	3.0000	.97552

Рис. 3.9. Результати змінних моніторингу політики

У таблиці 9 (рис. 3.9) зазначено, що середнє значення було вище 3. Періодичний огляд мав найвищу середню оцінку 4,0162, що свідчить про те, що респонденти вважають цей процес найважливішим процесом моніторингу політики.

У таблиці 10 (рис. 3.10) представлена описова статистика змінних підтримки підтримки з середніми значеннями, розташованими від найвищого до нижнього

Table 10 – Results of Management Support variables.

	N	Mean	Median	Std. deviation
Management involvement	308	4.0455	3.0000	.94017
Budget	307	4.0391	3.0000	.94891
Policy enforcement	308	4.0195	3.0000	1.00792
Policy approval	305	3.9508	3.0000	.96699

Рис. 3.10. Результати змінних підтримки управління

Як було підкреслено в таблиці 10 (рис. 3.10), результати показали, що середнє значення було вище 3. Участь керівництва мала найвищий середній показник 4.0455, що свідчить про те, що респонденти вважають цей процес найважливішим процесом конструкції підтримки управління.

У таблиці 11 (рис. 3.11) представлена описова статистика змінних підтримки службовців із середніми значеннями, розташованими від найвищих до найнижчих.

Table 11 – Results of the Employee Support variables.

	N	Mean	Median	Std. deviation
Employee involvement	307	4.0326	3.0000	.92474
Binding agreement	309	3.9968	3.0000	1.00162
Job termination	307	3.9870	3.0000	.99991
Deterrence measure	307	3.8436	3.0000	.99754

Рис. 3.11. Результати змінних підтримки співробітників

З таблиці 11 (рис. 3.11) видно, що середнє значення було вище 3, що свідчить про те, що респонденти визнали всі чотири змінні важливими. Участь працівників була найвищою середньою 4.0326, що свідчить про те, що респонденти вважають, що цей процес є дуже важливим порівняно з іншими процесами конструкції підтримки працівників

Результати контент-аналізу виявили високу частоту зустрічей управління підтримки та підтримки працівників. Відповідно, було припущено, що важливо, щоб підтримка управління та підтримка працівників були залучені до всіх процесів при розробці та реалізації політики інформаційної безпеки. Тому були проведені інфекційні статистичні тести, щоб з'ясувати, чи існує взаємозв'язок між підтримкою управління та побудови циклу розвитку політики безпеки інформації.

Аналогічно, статистичні тести використовувались для того, щоб з’ясувати, чи існує взаємозв'язок між службою підтримки працівників та відповідними конструкціями.

Для того, щоб політика безпеки інформації вижила та досягнула своїх цілей, керівництву, працівникам та зацікавленим сторонам потрібно її впроваджувати. Розробка ефективної політики безпеки вимагає поєднання навичок, що випливають із досвіду різних зацікавлених сторін:

Виконавчий менеджмент.

Перший крок у формулюванні політики безпеки включає визначення способу, яким вищий менеджмент розуміє безпеку в організації. Зважаючи на те, що менеджмент відіграє значну роль в прийнятті організаційних рішень, участь виконавчого управління в розробці політики інформаційної безпеки є ключовим для його успіху. Важливо, щоб керівництво усвідомлювало важливість діяльності з розробки політики інформаційної безпеки, щоб розподіляти на них необхідні ресурси.

Кінцеві користувачі

Підтримка працівників – це підтримка кінцевих користувачів, які виконують різні види діяльності в організації. Залучення співробітників до розробки політики інформаційної безпеки призводить до їх «викупу» та підтримки, а також створює відчуття власності на політику інформаційної безпеки.

Далі рекомендують включити спільноту кінцевих споживачів як частину зусиль з розробки, щоб забезпечити включення багатопрофільного характеру організації в процес розробки політики інформаційної безпеки. Ця участь кінцевих споживачів має відбуватися на ранній стадії. що їм надається можливість виявити помилки та труднощі, які потім можуть бути усунені до впровадження політики безпеки. "Якщо документи з політикою важко зрозуміти, користувачі можуть не прочитати їх повністю або можуть не зрозуміти їх правильно, тим самим непотрібно ризикувати компромісом із безпекою".

Юрисконсульт

Юридичний відділ важливий, оскільки надає інформацію про чинні закони, а також передбачувані законодавчі вимоги.

Технічний персонал

Співробітники технічного персоналу володіють технічними знаннями, яких може бракувати група з розробки політики безпеки. Один із респондентів опитував, що фахівці з безпеки повинні брати участь у розробці політики безпеки через їхні знання, яких може не вистачати в команді, яка займається розробкою політики.

Фахівці з безпеки повинні керувати розробкою та переглядом кожного політичного документа та виступати консультантами з розробки політики. Однак, хоча фахівці з питань безпеки знайомі з питаннями безпеки, вони, можливо, не володіють всебічними знаннями та розумінням комп'ютерних систем та систем комунікаційних мереж, що є роль фахівців з ІКТ. Фахівці з ІКТ зазвичай є однією з рушійних сил у розробці політики інформаційної безпеки, оскільки вони надають технологічні знання та можуть консультувати щодо рівня безпеки, який потрібен конкретній організації.

Людські ресурси

Для того, щоб політика безпеки відповідала загальноприйнятим організаційним практикам, дуже важливо залучити відділ кадрів до життєвого циклу розвитку політики безпеки. Таким чином, буде забезпечена відповідність між політикою безпеки організації та стандартними організаційними методами. Іншими словами, політика безпеки не повинна суперечити політиці в галузі людських ресурсів.

Зовнішні представники

Існує еобхідність включення до розробки політики інформаційної безпеки зовнішніх представників, таких як замовники, постачальники та інші зовнішні організації. Це особливо важливо, якщо зовнішні суб'єкти залежать від комп'ютерних систем організації для своєї діяльності. Як обговорюється в цьому розділі, розробка ефективної політики безпеки вимагає поєднання різних навичок, що випливають із досвіду різних зацікавлених сторін. Отже, включення декількох зацікавлених сторін у розробку ефективної політики безпеки є надзвичайно важливим, оскільки воно дає організації в цілому

відчуття власності на політику безпеки, що сприяє прийняттю та прийняттю політики.

3.2 Життєвий цикл розвитку політики в галузі інформаційної безпеки

Сьогодні організаціям будь-якої форми та розміру доводиться з ентузіазмом сприймати інформаційні системи та технології, якщо вони хочуть вижити та краще процвітати у все більш конкурентному середовищі. Отже, важливо, щоб контроль безпеки був запроваджений для того, щоб інформація, вбудована в організаційні інформаційні системи, зберігала свою цілісність, конфіденційність та доступність.

Для того, щоб організація мала відповідний підхід до захисту своїх інформаційних активів, вона потребує чітко спланованої та ефективної політики інформаційної безпеки. Поліс можна визначити як "спосіб дії, керівний принцип або процедура, яка вважається доцільною" або "страховий сертифікат" Можна зробити висновок, що політика стосується, по-перше, дії, яку потрібно вжити, або процедури, якої потрібно дотримуватися, і, по-друге, заяви або заяви, які можна зробити. Таким чином, якщо дотримуватися процедури правильно, то «страховий сертифікат» повинен бути недоторканим, тому організація досягає своїх цілей та завдань

Реалізація ефективної політики безпеки стає особливо важливою в галузі управління інформаційною безпекою. Мораль полягає в тому, що якою б сильною не була наявність технічного контролю, безпека завжди залежить від людей всередині організації. У програмі захисту інформації людей часто називають найслабшою ланкою Якщо порушення інформаційної безпеки або інцидент трапляється через дії неінформованого або недбалого працівника, рада директорів та вище керівництво можуть нести персональну відповідальність за поведінку цього працівника. Тому людський фактор не слід ігнорувати. Щоб організація мала адекватні заходи безпеки, вона потребує задокументованої політики щодо управління діями своїх працівників.

Як всередині академічної, так і практичної громадськості зростає консенсус щодо того, що політика інформаційної безпеки є основою для розповсюдження та впровадження належних практик безпеки в організаційному контексті. Принаймні, серед справжніх фахівців із безпеки добре відомо, що формальна політика є необхідною умовою безпеки.

Важливість створення ефективної політики інформаційної безпеки.

Політика інформаційної безпеки встановлює, що необхідно зробити для захисту інформації організації. Добре написана політика містить достатнє визначення поняття "що" робити, щоб "як" можна було визначити, виміряти або оцінити. Проведення політики якості для вирішення проблем, що викликають занепокоєння, може забезпечити більшу глибину висвітлення стосовно покращення загальної безпеки організації, а також може виявитися корисним з юридичної точки зору, якщо політики коли-небудь ставлять під сумнів. Політика інформаційної безпеки повинна визначати повну політику організації щодо захисту інформації. Зазвичай вона складається із заяви про політику високого рівня разом з додатковими детальними документами щодо політики. Політика повинна включати всі заходи, необхідні організації для дотримання законодавчих та нормативних вимог.

Важливість документації щодо політики безпеки полягає в тому, що вона вступить у дію у випадку інциденту інформаційної безпеки. Наприклад, існує низка анекдотів, що свідчать про те, що працівників, які поводять себе неадекватно, не можна звільнити, оскільки не існувало жодної політики безпеки, в якій було б вказано, що їх поведінка є неприйнятною, навіть якщо це завдало шкоди організації. Потім стає очевидним, що політика повинна бути поінформована планами організації щодо управління її операційним ризиком та дотримуватися юридичних, статутних, регуляторних чи договірних вимог, і повинна підтримувати всі зусилля для досягнення цих цілей.

Крім того, навіть якщо компанія юридично не зобов'язана розробляти та впроваджувати політику інформаційної безпеки, така політика виявиться

корисною для компанії з наступних причин: Політика інформаційної безпеки буде прагнути знайти спосіб найкращої поведінки бізнесу, одночасно захищаючи ідентичність, достовірність, конфіденційність та цілісність інформаційних активів компанії. Закон про Інтернет все ще дуже заплутаний, але підприємства, які мають політику інформаційної безпеки, можуть захистити себе від зайвих головних болів. Він продовжує зауважувати, що компанії, які мають ефективну політику інформаційної безпеки, яка визнає та відповідає міжнародним прийнятним стандартам, матиме явну перевагу перед тими компаніями, які приймають "очікування". Компанії, які не мають політики щодо захисту інформації або такої політики, але політика не застосовується ефективно, позначаються як такі, що є жертвами атак хакерів, зломщиків та інших агентів загрози. Це в кінцевому рахунку призведе до втрати довіри клієнтів та цінності акціонерів.

Переглянувши, чому існує потреба у політиці інформаційної безпеки, повинно бути зрозуміло, що компанії (а саме рада директорів) можуть бути позначені як необачні, недбалі та безвідповідальні, якщо вони дозволяють компанії функціонувати, не маючи ефективної політики інформаційної безпеки. . Крім того, з попереднього обговорення має бути видно, що важливою причиною проведення такої політики є допомога керівникам та вищому керівництву конкретними доказами, щоб представити в суді, що вони виконали свою відповідальність за належну ретельність та ретельну перевірку. Управляючи інформацією відповідно до її цінності та захищаючи конфіденційність, цілісність, доступність та конфіденційність своїх інформаційних активів, організації можуть не лише відповідати їх юридичним та нормативним вимогам, але й усвідомлювати значні переваги для бізнесу.

Хоча реалізація всеохоплюючої політики інформаційної безпеки надає численні переваги організаціям, процеси розробки, впровадження та прийняття ефективного, що відображає бачення та місію організації, і в той же час закріплює політику в організації, щоб вона стала нормальну та прийнятну частину щоденних операцій важко, в кращому випадку.

Проблеми в реалізації ефективної політики інформаційної безпеки.

Проблеми в застосуванні ефективної інформаційної безпеки В існуючій літературі наголошено на розробці політики політики інформаційної безпеки. Опитування Ернста та Янга (1998) показало, що підприємствам, які проводять таку політику, не приділяється достатньої уваги технічному обслуговуванню та дотриманню політики. Тому можна зробити висновок, що в багатьох організаціях політика безпеки закінчується на полиці через старіння, що призводить до застарілості.

Через труднощі, що виникають при розробці політики безпеки, обрані автори часто звертаються до політик інших організацій, комерційно доступних джерел або шаблонів, доступних з публічних джерел, таких як Інтернет, для отримання відповідей на свої запитання. Часто брак навичок та розуміння сприяє необхідності дотримуватися такого підходу. Однак отриманий документ не дасть належних вказівок щодо захисту інформації в контексті організації, яку вона повинна захищати.

Формулювання ефективної політики безпеки може бути дуже вимогливим і складним видом діяльності; отже, автори боротимуться з такими питаннями, як, наприклад, що має бути включено у цей важливий документ, щоб забезпечити відповідність організаціям законодавчих та регуляторних вимог, одночасно гарантуючи, що найкращі практики управління безпекою інформації. Зокрема, формулювання політики - це лише початок процесу. Технічне обслуговування та моніторинг на відповідність є настільки ж важливими, якщо не важливішими, ніж цей початковий крок, і зазвичай представляють собою додаткові проблеми в процесі. Політика повинна також підтримувати та розширювати бізнес-цілі організації. Тому будь-яке рішення, яке пропонує вирішити проблему формування, прийняття та впровадження політики захисту інформації, повинно вирішувати проблеми.

Сучасні методи розробки політики безпеки.

Огляд літератури розкриває низку підходів або методів, які організації можуть використовувати для розробки спеціальної політики безпеки. Ці

підходи згодом порівнюються у форматі таблиці, яка намагається групувати запропоновані кожним джерелом етапи у категорії, які є частиною подібного процесу. Наприклад, етапи, класифіковані в групу 1, зазвичай стосуються процесу оцінки ризику, який передує формулюванню політики. Група 2 займається кроками, необхідними для побудови політики, наприклад, складанням політики. Група 3 зосереджується на етапі впровадження політики, тоді як група 4 зосереджується на моніторингу та підтримці політики. Група 5 виділяє ключові ролі для менеджменту, тоді як група 6 робить те саме для персоналу загалом. Зауважте, що нумерація етапів, запропонованих певним джерелом, зберігається, навіть якщо кроки не відображаються послідовно в таблиці через вимогу класифікувати етапи в певній групі. Різні автори пропонують основні кроки для розробки документа про політику безпеки.

Підхід до життєвого циклу розвитку політики інформаційної безпеки (рис. 3.12).

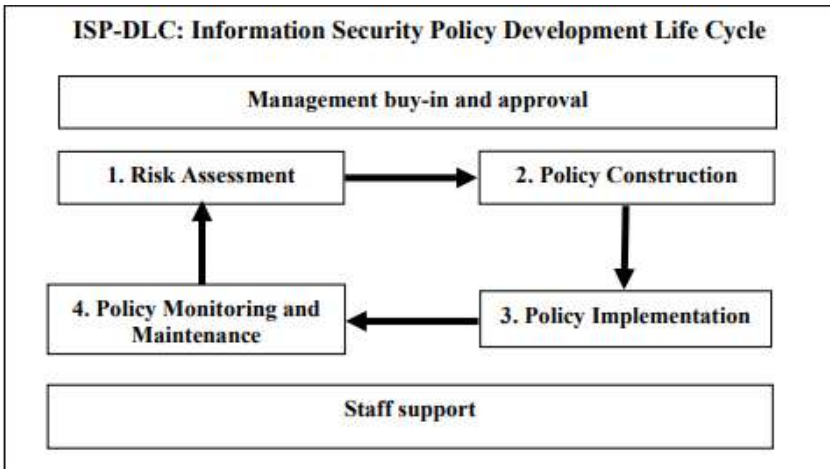

Рис. 3.12. Життєвий цикл розвитку політики інформаційної безпеки

Запропонований підхід ISP-DLC (рис. 3.12) складається з чотирьох основних фаз: Оцінка ризиків, Політика побудови, Впровадження політики, Моніторинг та підтримка політики. Кожну фазу можна розкласти на етапи, що детально описують дії, що відбуваються в межах кожної фази, як це обговорюється коротко далі. Важливо пам’ятати, що розробка політики – це ітеративний і безперервний процес. Зважаючи на зміни технології, ділового

середовища та вимог дотримання законодавства, на етапі впровадження політики завжди дотримуватиметься фаза технічного обслуговування, яка включає ці зміни, та фаза моніторингу, яка забезпечує оперативні виконання директив політики (тобто дотримання політики).

Фаза 1: Оцінка ризику

Етап оцінки ризику визначає бізнес-активи, які організація хоче захистити, та визначає потенційні загрози цим активам, задаючи наступні питання:

- Що треба захищати? (тобто активи)
- Від чого повинні бути захищені активи? (тобто загрози та вразливості)
- Скільки організація готова витратити, щоб мати належний захист?
- Яка вартість порівняно з вигодою для бізнесу?

Етап складається з чотирьох під-етапів:

- Визначення активів;
- Визначення вразливості та загроз;
- Узагальнення результатів оцінки ризиків;
- Оцінка можливих заходів та засобів контролю;

Ці під кроки повинні виконуватися послідовно, і результат буде використаний для вирішення питання, що потрібно включити до політики безпеки, щоб забезпечити зменшення виявлених ризиків.

Підтримка управління та підтримка персоналу (етап 1).

На основі результату оцінки ризику керівництво повинне оцінити витрати та переваги впровадження рекомендованих засобів контролю, щоб знизити ризик до прийнятного рівня. Якщо передбачені витрати перебувають у межах бюджету, наступний етап розробки політики може розпочатися. Якщо ні, то стратегії зменшення ризику потрібно переглянути, щоб вони були в межах бюджету, або бюджет повинен бути збільшений. На цьому етапі життєвого циклу вироблення політики участь першочергових завдань є головною

вимогою, тоді як персонал в цілому буде задіяний лише з точки зору оцінки ризиків.

Фаза 2: Побудова політики.

Політика безпеки розробляється на цій фазі на основі висновків та рекомендацій щодо зменшення ризиків, пов'язаних із загрозами та вразливими місцями, як це було узгоджено на етапі оцінки ризику. Цей етап також буде враховувати бізнес-стратегії та цілі та юридичні вимоги під час створення полісів. Етап складається з наступних кроків:

- Складання односторінкової заяви про політику та накреслення вимог безпеки на високому рівні;
- Перегляд та затвердження заяви про політику високого рівня;
- Розробка детальних документів про політику;
- Перегляд та затвердження детальних заяв про політику;
- Опублікування затверджених політик безпеки;

Процес написання політики щодо захисту інформації включає вибір відповідних цілей контролю, яких необхідно досягти. Контрольна мета визначається як "констатація бажаного результату або мети, яка повинна бути досягнута шляхом впровадження контрольних процедур у певному процесі". Мета контролю також може розглядатися як найкраща практика захисту інформації, яка реалізується за допомогою використання відповідних засобів контролю безпеки (ISO 27002, 2005). Буде розроблено заяву про політику на одній сторінці та на високому рівні вимоги безпеки для відповідності вимогам вибраних цілей контролю. Цей проект дає вихідну точку для створення ідеальної політики інформаційної безпеки, яка відображає проблеми організації найвищого рівня. Проект буде переданий виконавчому та вищому керівництву для розгляду та затвердження заяви про політику високого рівня. Якщо проект буде затверджений, проект детального документа про політику, заснований на заяві про політику високого рівня, знову передається керівництву для затвердження; і якщо буде схвалено, політика безпеки готова до публікації.

Підтримка управління та підтримка персоналу (етап 2).

За винятком цілісної ролі керівництва щодо перегляду та затвердження проектів політики та остаточних документів щодо політики безпеки, необхідна їхня чітка прихильність та підтримка цих політик з подальшими узгодженими зусиллями для забезпечення належного донесення політики до персоналу. План комунікації, який дає змогу отримувати зворотний зв'язок між аудиторією, повинен бути ініційований на етапі створення політики, щоб підготувати організацію до майбутніх змін та дати можливість людям впливати на формування нової політики. Участь має вирішальне значення для переміщення користувачів через етапи прихильності від підготовки до прийняття та, нарешті, до етапу зобов'язань.

Крім того, нова або оновлена політика безпеки неминуче змінить щось щодо того, як хтось працює, і такі зміни, якими б малими вони були, потребують уваги. Вплив змін необхідно оцінити, щоб переконатися, що воно може бути успішно здійснено. Отже, розуміння сучасного середовища є життєво важливим. Наприклад, ці питання слід задавати на етапі розробки політики, щоб оцінити здатність персоналу успішно підтримувати нову політику безпеки:

- На кого впливають?
- Чи усвідомлює культура важливість безпеки?
- Як культура вимагає введення компонентів нової політики та ключових питань впровадження?
- Що очікується, коли буде впроваджена нова політика?

Вищезазначені аспекти повинні бути вирішені на етапі впровадження політики, щоб забезпечити прийняття персоналом та підтримку нової політики.

Фаза 3: Впровадження політики.

Після завершення розробки політики настав час реалізувати новий документ про політику безпеки. Тепер необхідний детальний план реалізації, щоб перетворити дизайн в реальність. Цей етап охоплює наступні етапи:

Визначення вимог щодо безпеки та контролю за допомогою детальних процедур та вказівок,

- Виділення обов'язків щодо інформаційної безпеки;
- Випробування безпеки та контролю за безпекою;
- Виконання вимог безпеки та контролю;
- Забезпечення постійних навчань та обізнаності щодо політики безпеки;

Реєстрація та підтримка персоналу (етап 3).

Спілкування старших членів організації підвищить ймовірність прийняття політики щодо безпеки в цілому та сприятиме просуванню людей на етапах зобов'язань. Затверджена остаточна копія політики безпеки повинна бути доступною для всіх працівників. Це повинно бути повідомлено всім користувачам формально, і користувачі повинні визнати, що політика читається та розуміється, підписуючи та погоджуючись виконувати її. Наступною вимогою буде розробка програм інформованості про безпеку та навчання щодо нової політики. Ці програми є дуже важливими кроками на етапі впровадження політики, оскільки їх основною роллю буде змінити ставлення працівників шляхом заохочення їх до активної ролі в реалізації політики.

Фаза 4: Моніторинг та підтримка політики.

Ця фаза складається з двох основних видів діяльності, а саме: моніторинг та обслуговування.

Моніторинг політики.

Після впровадження політики інформаційної безпеки організації повинні включати відповідні механізми моніторингу для визначення щоденних заходів по всій організації, які забезпечують проведення політики безпеки у всій організації. Необхідно виконати наступні кроки:

- Отримати вимірювані результати, що відображають поведінку користувачів;
- Виконувати системний аудит та огляди;

- Виконувати виявлення вторгнень та тестування на проникнення;
- Проводити аналіз стежок аудиту діяльності користувачів;
- Дотримання політики аудиту;

Основна мета моніторингу політики – забезпечити дотримання персоналом нових вимог політики. Таким чином, запропонований ISP-DLC показує, що відповідність вимогам політики необхідна для забезпечення стійкості політики безпеки. Політика, яка будується лише і ніколи не застосовується та не дотримується, не приносить користі організації.

Політика обслуговування.

Ця діяльність включає наступні кроки:

- Огляд звітів про інциденти із безпекою;
- Огляд безпеки та технологічної інфраструктури;
- Перегляд бізнес-стратегій;
- Перегляд тенденцій та несподіваних подій;
- Перегляд юридичних вимог;
- Збір запиту щодо змін політики;
- Повторення життєвого циклу розробки політики;

Важливо постійно перевіряти інфраструктуру безпеки організації для виявлення нових загроз. Це може бути пов'язано зі змінами технології, що застосовується в інших місцях організації. Цілком можливо, що будуть запроваджені нові закони, які необхідно включити в політику безпеки організації. Суть полягає в тому, що зміни різного характеру можуть призвести до застарілості політики інформаційної безпеки. Ці зміни повинні бути включені до політики через етап технічного обслуговування. Фаза технічного обслуговування вимагає повторного виконання фаз 1-3 у життєвому циклі, щоб гарантувати, що зміни до політики не застосовуються ad hoc. Звичайно, існує багато невідомих, і під час цього етапу організації, ймовірно, виявлять нову загрозу, яку не враховували, нову технологію, яка потрібна, або спроможність бізнесу, яку забули і для якої слід використовувати в організаційній політиці .

Реєстрація та підтримка персоналу (етап 4).

На цьому кроці керівництво повинно забезпечити встановлення відповідних процедур та систем, щоб визначити, чи розуміє персонал реалізовану політику та процедури та чи дотримуються політики та процедури. Крім того, керівництву необхідно забезпечити наявність відповідних наслідків для недотримання вимог політики безпеки. Покарання потрібно послідовно виконувати та повідомляти всім співробітникам.

Висновки до третього розділу

Розробка політики інформаційної безпеки виходить за рамки простого написання та впровадження політики. Якщо організації не визнають різні кроки, необхідні в розробці політики безпеки, вони ризикують розробити неефективну політику.

Політика інформаційної безпеки має свій життєвий цикл. Якщо політика інформаційної безпеки не один раз проходила життєвий цикл, то вона буде більш зрілою як у розумінні підтримки принципів безпеки підприємства, так і в оперативному закріпленні на підприємстві завдяки наявності належних процедур.

ВИСНОВКИ

Концепція інформаційної безпеки складає систему поглядів, основних принципів, розкриває основні напрями забезпечення безпеки інформації.

Аналіз ризиків передбачає вивчення моделі загроз для інформаційної сфери організації та моделі порушників, можливих наслідків від реалізації потенційних загроз (рівня можливої заподіяної ними шкоди) і формування на його підставі моделі захисту інформації у організації.

Політику з інформаційної безпеки організації можна визначити як сукупність вимог та правил з інформаційної безпеки організації для об'єкта інформаційної безпеки організації, вироблених з метою протидії заданій множині загроз інформаційній безпеці організації із урахуванням цінності інформаційної сфери, що підлягає захисту та вартості системи забезпечення інформаційної безпеки.

Політика інформаційної безпеки банку – сукупність правових і морально-етичних норм, правил, адміністративних, організаційних заходів і технічних, програмних і криптографічних засобів, направлених на захист інформаційної інфраструктури банку від випадкового і навмисного втручання в процес її функціонування.

У політиці інформаційної безпеки промислового підприємства достатньо точно і чітко регламентуються всі моменти використання мережевого обладнання та програмного забезпечення.

Розробники політики інформаційної безпеки іноземних підприємств повинні розуміти дані своєї організації, місію організації, принципи управління даними та формулювати відповідні та практичні політики та стандарти.

Розробка політики інформаційної безпеки виходить за рамки простого написання та впровадження політики. Якщо організації не визнають різні кроки, необхідні в розробці політики безпеки, вони ризикують розробити неефективну політику.

Політика інформаційної безпеки має свій життєвий цикл. Якщо політика інформаційної безпеки не один раз проходила життєвий цикл, то вона буде більш зрілою як у розумінні підтримки принципів безпеки підприємства, так і в оперативному закріпленні на підприємстві завдяки наявності належних процедур.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Ахрамович В.М. Інформаційна безпека. Навчальний посібник / В.М. Ахрамович. – К.: ДП «Інформ.-аналіт. агенство», 2009.

2. Основи організації електронного документообігу: у 2 т. / С.М. Головань, І.В. Васюков, А.М. Давиденко, В.О. Хорошко, Л.М. Щербак. – К.: ДУІКТ, 2008.

3. О.Л. Голубенко, В.О. Хорошко, О.С. Петров, С.М. Головань. – Луганськ: СНУ ім. В. Даля, 2010.

4. Домарєв В.В. Ор ганізація захисту інформації на об’єктах державної та підприємницької діяльності. Навчальний посібник / В.В. Домарєв, С.О. Скворцов. – К.: Вид-во Європ. ун-ту, 2006.

5. Конахович Г.Ф. Защита информации в телекоммуникационных системах / Г.Ф. Конахович. – К.: «МК-Пресс», 2005.

6 Бондаренко М.Ф. Визначення та обґрунтування суті політики інформаційної безпеки / М.Ф. Бондаренко, О.В. Потій, Ю.І. Горбенко та ін. // Радиотехника. – 2003. – № 134

7. Бузов О.О. Защита информации от утечки по техническим каналам. Учебное пособие. – М.: Гостехкомисия Росии, 2005.

8. Хорошко В.О. Основи інформаційної безпеки / В.О. Хорошко, В.С. Чередниченко, М.Є. Шелест. – К.: ДУІКТ, 2008..

9. Богуш В.М., Юдін О.К. Інформаційна безпека держави. Навчальний посібник / В.М. Богуш, О.К. Юдін. – К.: "МК-Прес", 2005.

10. Домарєв В.В. Організаційне забезпечення захисту інформації з обмеженим доступом. Навчальний посібник / В.В. Домарєв, В.А. Швець, В.В. Шестакова. – К.: НАУ, 2006.

11. Кобозева А.А. Аналіз захищеності інформаційних систем. Підручник / А.А. Кобозева, І.О. Мачалін, В.О. Хорошко. – К. ДУІКТ, 2010.

12. Ленков С.В. Методы и средства защиты информации / С.В. Ленков, Д.А. Перегудов, В.О. Хорошко. – К: Арий, 2008.

13. Лужецький В.А. Захист персональних даних. Навчальний посібник / В.А. Лужецький, О.П. Войтович, А.В. Дудатьєв. – Вінниця: ВНТУ, 2009.

14. Лужецький В.А. Інформаційна безпека. Навчальний посібник / В.А. Лужецький, О.П. Войтович, А.В. Дудатьєв. – Вінниця: УНІВАР-СУМ-Вінниця, 2009.

15. Мамаев М. Технологии защиты информации в Интернете. Специальный справочник / М. Мамаев, С. Петренко. – СПб.: Питер, 2002.

16. Петренко С.А. Политики информационной безопасности / С.А. Петренко, В.А. Курбатов. – М.: Компания АйТи, 2006.

17 Самохвалов Ю.Я. Організаційно-технічне забезпечення захисту інформації / Ю.Я. Самохвалов, В.О. Темніков, В.О. Хорошко / За ред. проф. В.О. Хорошка – К.: Видавництво НАУ, 2002.. Конфіденційне діловодство. Практикум. Навчальний посібник /

18. Соколов А.В., Шаньгин В.Ф. Защита информации в распределенных корпоративных сетях и системах / А.В. Соколов, В.Ф. Шаньгин. – М.: ДМК Пресс, 2002.

19. Юдін О.К. Інформаційна безпека. Нормативно-правове забезпечення: підруч. / О.К. Юдін. – К. : НАУ, 2011.

20. Потій О.В. Визначення та обґрунтування суті політики інформаційної безпеки / О.В. Потій, Ю.І. Горбенко [Електронний ресурс]. – Режим доступу: http://www.security.ukrnet.net/modules/sections/index.php?op=viewarticle&artid=95

21. Chaula, JA, Yngström, L & Kowalski. Метрики безпеки та оцінка політики інформаційної безпеки [Електронний ресурс]. – Режим доступу: http://icsa.cs.up.ac.za/issa/2004/Proceedings/Research/048.pdf

22. Контрольні дані. Чому не приймаються політики безпеки [Електронний ресурс]. – Режим доступу: http://www.securityfocus.com/data/library/Why_Security_Policies_Fail.pdf

23 Doherty, NF, Fulford, H. Чи політика інформаційної безпеки зменшує частоту порушень безпеки: дослідницький аналіз // Журнал управління інформаційними ресурсами. – 2015. – № 18 (4). – С. 21-38..

24. Керівництво бізнес-менеджерів з інформаційної безпеки. Департамент торгівлі та промисловості (Великобританія) [Електронний ресурс]. – Режим доступу: http://www.dti.gov.uk/cii/datasecurity/businessmanagersguide/index.shtml

25. Міжнародне обстеження інформаційної безпеки // Ернст і Янг, 2008.

26. Etsebeth, V. Політика інформаційної безпеки - правовий ризик уніформованого персоналу. Управління інформаційною безпекою та дотримання регуляторних норм [Електронний ресурс]. – Режим доступу: http://www.icsa.cs.up.ac.za/issa/2004/Proceedings/Full/051.pdf

27. Хіггінс Х.Н. Безпека корпоративної системи: до комплексного підходу до управління. Управління інформацією та комп'ютерна безпека: Підручник для дослідників технологічної освіти // Journal of Technology Education. – 2009. – № 9 (1). – С. 47-63.

28. ISO / IEC 27002 (2005), Інформаційні технології: Методи безпеки - Кодекс практики управління інформаційною безпекою (Видання 2): SANS.

29. Карін Х. Політика інформаційної безпеки - що говорять про міжнародні стандарти безпеки / Х. Карін, Д. Елофф. – К., 2012. – 402 с..

30. Herold, R. Практичний посібник із забезпечення відповідності [Електронний ресурс]. – Режим доступу: http://www.realtimepublishers.com