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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню бакалавра

студента *Данильченка Олексія Ігоровича*

академічної групи *125-17-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Розробка системи управління інформаційною безпекою приватного підприємства з оцінки майна*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	к.т.н., доц. Флоров С.В.			
розділів:				
спеціальний	ст. викл. Саксонов Г.М.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2021

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту ___*Данильченку Олексію Ігоровичу*___ **академічної групи** _ *125-17-2*__
(прізвище ім'я по-батькові) (шифр)

спеціальності _____ *125 Кібербезпека*___
(код і назва спеціальності)

на тему _ ***Розробка системи управління інформаційною безпекою приватного підприємства з оцінки майна***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 07.06.2021р № 317-с

Розділ	Зміст	Термін виконання
Розділ 1	Аналіз та аудит інформаційної системи об'єкту інформаційної діяльності. Нормативна документація України в галузі захисту комерційної таємниці.	29.03.2021
Розділ 2	Розробка політики інформаційної безпеки у відповідності з вихідними даними аналізу можливих загроз інформаційної безпеки. Дослідження ефективності розробки.	24.05.2021
Розділ 3	Економічне обґрунтування запропонованих заходів захисту комерційної таємниці.	14.06.2021

Завдання видано _____ _____
(підпис керівника) (прізвище, ініціали)

Дата видачі:_____р.

Дата подання до екзаменаційної комісії: 15.06.2021р.

Прийнято до виконання _____ _____
(підпис студента) (прізвище, ініціали)

Пояснювальна записка:___с.,___рис.,___табл.,___додатка,___джерел.

Об'єкт досліджень: інформаційна система приватного підприємства з оцінки майна.

Мета роботи: розробка алгоритму для підвищення рівня інформаційної безпеки приватного підприємства з оцінки майна.

В першій частині роботи розглянуто загальні відомості про інформаційної безпеки, її мету та основні задачі. Проаналізована державна нормативно-правова база у сфері захисту комерційної таємниці, конфіденційної інформації та оціночної діяльності.

У спеціальній частині роботи розроблено технічне завдання на роботу по розробці політики інформаційної безпеки приватного підприємства з оцінки майна.

В економічному розділі розглянуто потенційний збиток від втрати інформації, розраховано збиток від атаки на приватне підприємство з оцінки майна.

Практичне значення роботи полягає у впровадженні та опробуванні розроблених рекомендацій та заходів політики безпеки для типового приватного підприємства з оцінки майна, аналізі ефективності та обґрунтованості застосування запропонованого алгоритму.

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, ПОЛІТИКА БЕЗПЕКИ, КОМЕРЦІЙНА ТАЄМНИЦЯ, ПРОФІЛЬ ЗАХИЩЕННОСТІ, МОДЕЛЬ ПОРУШНИКА, МОДЕЛЬ ЗАГРОЗ, ПАРОЛЬНИЙ ЗАХИСТ.

РЕФЕРАТ

Пояснительная записка:__ с., __рис., __табл., ___ приложения, __источников.

Объект исследований: информационная система частного предприятия по оценке имущества.

Цель работы: разработка алгоритма для повышения уровня информационной безопасности частного предприятия по оценке имущества.

В первой части работы рассмотрены общие сведения о информационной безопасности, ее цель и основные задачи. Проанализирована государственная нормативно-правовая база в сфере защиты коммерческой тайны, конфиденциальной информации и оценочной деятельности.

В специальной части работы разработано техническое задание на работу по разработке политики информационной безопасности частного предприятия по оценке имущества.

В экономическом разделе рассмотрены потенциальный ущерб от потери информации, рассчитан ущерб от атаки на частное предприятие по оценке имущества.

Практическое значение работы состоит во внедрении и опробовании разработанных рекомендаций и мероприятий политики безопасности для типового частного предприятия по оценке имущества, анализе эффективности и обоснованности применения предложенного алгоритма.

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ПОЛИТИКА БЕЗОПАСНОСТИ, КОММЕРЧЕСКАЯ ТАЙНА, ПРОФИЛЬ ЗАЩИЩЕННОСТИ, МОДЕЛЬ НАРУШИТЕЛЯ, МОДЕЛИ УГРОЗ, ПАРОЛЬНОЙ ЗАЩИТЫ.

ABSTRACT

Explanatory note:___p.,____pic.,____tabl.,____app.,____sources.

Object of research: information system of a private enterprise for property valuation.

Purpose: development of an algorithm to increase the level of information security of a private enterprise for property valuation.

The first part of the paper considers general information about information security, its purpose and main tasks. The state regulatory framework in the field of protection of trade secrets, confidential information and evaluation activities is analyzed.

In the special part of the work the technical task for work on development of information security policy of the private enterprise on property estimation is developed.

The economic section considers the potential damage from the loss of information, calculates the damage from the attack on a private enterprise for property valuation.

The practical significance of the work is to implement and test the developed recommendations and security policy measures for a typical private enterprise for property valuation, analysis of the effectiveness and validity of the proposed algorithm.

INFORMATION SECURITY MANAGEMENT, SECURITY POLICY, COMMERCIAL SECRET, SECURITY PROFILE, VIOLATION MODEL, THREAT MODEL, PASSWORD.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – авторизована станція;

ІБ – інформаційна безпека;

ІзОД – інформація з обмеженим доступом;

ІС – інформаційна система;

ІТ – інформаційні технології;

КПК – кишеньковий персональний комп'ютер;

ЛОМ – локально-обчислювальна мережа;

ОС – операційна система;

ПБ – політика безпеки;

ПЗ – програмне забезпечення;

ПК – персональний комп'ютер;

ПП – приватне підприємство;

СУБД – система управління базою даних;

СУІБ – система управління інформаційною безпекою.

ЗМІСТ

ВСТУП

В даний час благополуччя і навіть життя багатьох людей залежать від забезпечення інформаційної безпеки безлічі комп'ютерних систем обробки інформації, контролю і управління різними об'єктами. До таких систем відносяться і інформаційні системи оціночних підприємств.

Їх особливістю є, насамперед, те, що в них зберігається і обробляється інформація, всебічно визначає соціальний статус людини, а це обумовлює особливу форму відносин між тими, хто її формує, і тими, хто використовує. Значить, поряд з підвищеними вимогами до достовірності інформації повинні накладатися моральні обмеження на доступ до неї, а також юридична відповідальність надають її осіб.

Будь який працівник підприємства несе повну відповідальність (моральну, адміністративну та кримінальну) за конфіденційність інформації, до якої він отримує доступ в ході своєї професійної діяльності.

Актуальність теми забезпечення інформаційної безпеки на приватних підприємствах підтверджується тим, що в більшості установ питання інформаційної безпеки не розглядаються взагалі, а також відсутністю будь-яких заходів спрямованих на забезпечення інформаційної безпеки та збереження комерційної таємниці.

Проблема безпеки інформаційних технологій виникла на перетині двох активно розвиваючих ся і, напевно, найбільш передових в плані використання технічних досягнень напрямків – безпеки технологій та інформатизації. Сама проблема безпеки, звичайно, не є новою, адже забезпечення власної безпеки – завдання першорядної важливості для будь-якої системи незалежно від її складності і призначення будь то соціальне утворення, біологічний організм або система обробки інформації. Однак, в умовах, коли захищається об'єкт являє собою інформаційну систему, або

коли засоби нападу мають форму інформаційних впливів, необхідно розробляти і застосовувати абсолютно нові технології та методи.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Загальна характеристика оціночної діяльності

Системний підхід до управління підприємством передбачає аналіз господарської діяльності підприємства у вигляді багаторівневої структури. Окрім технічного комерційного, інституційного соціального, екологічного аналізу він повинен включати оцінку активів підприємства.

Потреба в оцінці вартості підприємства при інвестуванні, кредитуванні, страхуванні, обчисленні сплати податків стає дуже актуальною в наш час.

Окрім зовнішнього напряму використання результатів оцінки існує ще й внутрішня потреба. Оцінка вартості необхідна для вибору напрямку реструктуризації підприємства. Оцінка підприємства представляє собою процес визначення його вартості з врахуванням потенційного і реального доходу за конкретний проміжок часу в умовах конкретного ринку.

Особливістю оцінки вартості підприємства являється необхідність її відповідності ринковій ситуації. Основними факторами при цьому є час і ризик, а також ринкова кон'юнктура, рівень і модель конкуренції, економічні особливості оцінюваного об'єкта , його ринкова репутація, макрос і мікроекономічна середа існування.

Згідно ст.4 Закону України № 2658-111 від 12 липня 2001 року "Про оцінку майна, майнових прав і професійну оціночну діяльність в Україні" професійна оціночна діяльність - це діяльність оцінювачів і суб'єктів оціночної діяльності, яка полягає в організаційному, методичному і практичному забезпеченні проведення оцінки майна розгляді і підготовці висновків щодо вартості майна.

Компанія здійснює оціночну діяльність на підставі:

- Сертифіката суб'єкта оціночної діяльності виданого Фондом державного майна України.
- Ліцензії Державного комітету з питань земельних ресурсів України.

Експерти нашого підприємства мають багаторічний досвід практичної діяльності по наданню послуг з оцінки.

Послуги з оцінки проводяться відповідно до процедур, визначених чинним законодавством України на підставі договору із замовником.

За наслідками проведеної роботи оформляється звіт про оцінку, що має повну юридичну силу для учасників угоди і користувачів звіту.

Закон України « Про оцінку майна, майнових прав та професійну оціночну діяльність в Україні» визначає правові засади здійснення оцінки майна, майнових прав та професійної оціночної діяльності в Україні, її державного та громадського регулювання, забезпечення створення системи незалежної оцінки майна з метою захисту законних інтересів держави та інших суб'єктів правовідносин у питаннях оцінки майна, майнових прав та використання її результатів.

Оцінка майна, майнових прав та професійна оціночна діяльність регулюються цим Законом, іншими нормативно-правовими актами з оцінки майна, що не суперечать йому.

Оцінка майна, майнових прав (далі - оцінка майна) - це процес визначення їх вартості на дату оцінки за процедурою, встановленою нормативно-правовими актами з оцінки майна і є результатом практичної діяльності суб'єкта оціночної діяльності.

Незалежною оцінкою майна вважається оцінка майна, що проведена суб'єктом оціночної діяльності - суб’єктом господарювання.

Процедури оцінки майна встановлюються нормативно-правовими актами з оцінки майна. У випадках проведення незалежної оцінки майна складається звіт про оцінку майна. У випадках самостійного проведення оцінки майна органом державної влади або органом місцевого самоврядування складається акт оцінки майна.

Датою оцінки є дата, за станом на яку здійснюються процедури оцінки майна та визначається вартість майна. Випадки обов'язкового проведення оцінки майна встановлюються цим Законом.

Професійна оціночна діяльність (далі - оціночна діяльність) - діяльність оцінювачів та суб'єктів оціночної діяльності, такими відповідно до положень, яка полягає в організаційному, методичному та практичному забезпеченні проведення оцінки майна, розгляді та підготовці висновків щодо вартості майна.

Оціночна діяльність може здійснюватися у таких формах:

- практична діяльність з оцінки майна, яка полягає у практичному виконанні оцінки майна та всіх процедур, пов'язаних з нею, відповідно до вимог, встановлених нормативно-правовими актами з оцінки майна;

- консультаційна діяльність, яка полягає в наданні консультацій з оцінки майна суб'єктам оціночної діяльності, замовникам оцінки та (або) іншим особам в усній або письмовій формі;

- рецензування звіту про оцінку майна (акта оцінки майна), яке полягає в їх критичному розгляді та наданні висновків щодо їх повноти, правильності виконання та відповідності застосованих процедур оцінки майна вимогам нормативно-правових актів з оцінки майна, в порядку, визначеному цим Законом та нормативно-правовими актами з оцінки майна;

- методичне забезпечення оцінки майна, яке полягає в розробленні методичних документів з оцінки майна та наданні роз'яснень щодо їх застосування;

- навчальна діяльність оцінювачів, яка полягає в участі у навчальному процесі з професійної підготовки оцінювачів.

Практична діяльність з оцінки майна може здійснюватися виключно суб'єктами оціночної діяльності.

Діяльність судових експертів, пов'язана з оцінкою майна, здійснюється на умовах і в порядку, передбачених Законом України "Про судову експертизу".

Суб'єктами оціночної діяльності є:

- суб'єкти господарювання;

- органи державної влади та органи місцевого самоврядування, які отримали повноваження на здійснення оціночної діяльності.

Оцінка майна проводиться у випадках, встановлених законодавством України, міжнародними угодами, на підставі договору, а також на вимогу однієї з сторін угоди та за згодою сторін.

Проведення оцінки майна є обов'язковим у випадках:

- створення підприємств (господарських товариств) на базі державного майна або майна, що є у комунальній власності;

- реорганізації, банкрутства, ліквідації державних, комунальних підприємств та підприємств (господарських товариств) з державною часткою майна (часткою комунального майна);

- виділення або визначення частки майна у спільному майні, в якому є державна частка (частка комунального майна);

- визначення вартості внесків учасників та засновників господарського товариства, якщо до зазначеного товариства вноситься майно господарських товариств з державною часткою (часткою комунального майна), а також у разі виходу (виключення) учасника або засновника із складу такого товариства;

- приватизації та іншого відчуження у випадках, встановлених законом, оренди, обміну, страхування державного майна, майна, що є у комунальній власності, а також повернення цього майна на підставі рішення суду;

- переоцінки основних фондів для цілей бухгалтерського обліку; оподаткування майна згідно з законом;

- визначення збитків або розміру відшкодування у випадках, встановлених законом;

- в інших випадках за рішенням суду або у зв'язку з необхідністю захисту суспільних інтересів.

Проведення незалежної оцінки майна є обов'язковим у випадках застави державного та комунального майна, відчуження державного та комунального майна способами, що не передбачають конкуренцію покупців у процесі продажу, або у разі продажу одному покупцю, визначення збитків або розміру

відшкодування, під час вирішення спорів та в інших випадках, визначених законодавством або за згодою сторін.

Не допускається проведення оцінки майна суб'єктами оціночної діяльності - суб'єктами господарювання у таких випадках:

- проведення суб'єктом оціночної діяльності - суб'єктом господарювання оцінки майна, що належить йому або оцінювачам, які працюють у його складі, на праві власності або на яке зазначені особи мають майнові права;
- проведення оцінки майна фізичної особи-замовника або керівників юридичної особи, яка є замовником оцінки, оцінювачем, який має родинні зв'язки з зазначеними особами, або суб'єктом оціночної діяльності -суб'єктом господарювання, керівництво якого має зазначені зв'язки;
- проведення оцінки майна своїх засновників (учасників).

Під час оцінки майна, що здійснюється органами державної влади, утому числі Фондом державного майна України, та органами місцевого самоврядування, встановлюються такі обмеження:

- не може передбачатися виключне право її проведення органами державної влади та органами місцевого самоврядування або оцінювачами, які працюють в органах державної влади та органах місцевого самоврядування, за винятком випадків, передбачених законом;
- не можуть передбачатися будь-які форми виключного права на проведення оцінки майна суб'єктами оціночної діяльності, які створені зазначеними органами державної влади та органами місцевого самоврядування.

Результати оцінки майна, проведеної з порушеннями зазначених обмежень, визнаються недійсними та підлягають обов'язковому скасуванню.

Оцінка майна у випадках її обов'язкового проведення, зазначених у статті 7 цього Закону, виконана суб'єктами, які не є суб'єктами оціночної діяльності, визнається недійсною.

Оцінка майна проводиться на підставі договору між суб'єктом оціночної діяльності - суб'єктом господарювання та замовником оцінки або на підставі ухвали суду про призначення відповідної експертизи щодо оцінки майна.

Договір на проведення оцінки майна укладається в письмовій формі та може бути двостороннім або багатостороннім. Під час укладання багатостороннього договору крім замовника оцінки стороною договору може виступати особа-платник, якщо оплату послуг суб'єкта оціночної діяльності здійснює інша особа, а не замовник.

Звіт про оцінку майна є документом, що містить висновки про вартість майна та підтверджує виконані процедури з оцінки майна суб'єктом оціночної діяльності - суб'єктом господарювання відповідно до договору. Звіт підписується оцінювачами, які безпосередньо проводили оцінку майна, і скріплюється печаткою та підписом керівника суб'єкта оціночної діяльності.

Акт оцінки майна є документом, що містить висновки про вартість майна та підтверджує виконані процедури з оцінки майна, здійсненої суб'єктом оціночної діяльності - органом державної влади або органом місцевого самоврядування самостійно

Сертифікат суб'єкта оціночної діяльності - суб'єкта господарювання (далі - сертифікат) є документом, що

Оцінка майна, яка проведена суб'єктом оціночної діяльності - суб'єктом господарювання без чинного сертифіката, є недійсною.

Державне регулювання оціночної діяльності полягає в забезпеченні формування та розвитку інфраструктури оцінки майна в Україні, об'єктивності та законності її проведення, у тому числі відповідності оцінки майна нормативно-правовим актам з оцінки майна, впровадження в практику оціночної діяльності міжнародних норм та правил оцінки майна, забезпеченні суспільних інтересів у питаннях оцінки майна, створення конкурентного середовища серед суб'єктів оціночної діяльності - суб'єктів господарювання та навчальних закладів, що здійснюють професійну підготовку оцінювачів, проведення оцінки майна

органами державної влади та органами місцевого самоврядування відповідно до законодавства

1.1.1 Аналіз програмного забезпечення типових підприємств з оцінки майна як об'єктів інформаційної діяльності

Основні програмні продукти, які використовується на фірмі, - це ОС MS Windows 10, MS Office 2016, 1С-Бухгалтерія 8.

Весь облік фірми ведеться за допомогою програмного комплексу «1С».

Цей комплекс призначений для ведення бухгалтерського і оперативного обліку, автоматизації управління бізнес-процесами.

До складу системи входить набір взаємозв'язаних модулів, що мають гнучкі зв'язки і легко налаштовуються, такі як «бухгалтерія», «банк», «основні засоби», «планування», «податковий облік», «сертифікат», «адміністратор», «конструктор звітів».

1.1.2 Характеристика інформації яка оброблюється в комп'ютерній мережі

У комп'ютерній мережі підприємства обробляється комерційна таємниця, володіти, користуватися або розпоряджатися якою можуть окремі фізичні особи, що мають доступ до неї у відповідності з умовними правилами, встановленими директором підприємства.

У комп'ютерній мережі зберігається і циркулює відкрита інформація (архіви даних), яка не потребує захисту, а також відкрита інформація, яка відповідно до рішення її власника може потребувати захисту.

КСЗІ гарантує забезпечення цілісності, конфіденційності і доступності інформації, яка має ступінь обмеження «для службового користування», згідно з певними вимогами до відповідного функціонального профілю захищеності.

1.1.3 Інформаційні потоки типових оціночних підприємств

Аналіз інформаційних потоків підприємства:

1 Електронні звіти, запити до БД, електронні документи для друку, електронне листування, запити в Інтернет.

2 Електронні звіти, запити до БД, електронні документи для друку, електронне листування, запити в Інтернет.

3 Електронні звіти, запити до БД, електронні документи для друку, електронне листування, електронні замовлення клієнтів.

4 Електронні звіти, запити до БД, електронні документи для друку, податкова документація, електронне листування.

5 Електронні документи для друку, електронне листування, запити в Інтернет.

6 Електронні документи для друку, електронне листування, запити до БД.

7 Електронні документи для друку, електронне листування, запити в Інтернет.

8 Електронні документи для друку, електронне листування.

9 Електронні звіти, підтвердження оплати, податкова документація, запити до БД, електронні документи для друку, електронне листування, банківські виписки, платіжні доручення, запити в Інтернет.

10 Банківські виписки, платіжні доручення. 11 Електронні звіти.

12 Електронні звіти, запити до БД, електронне листування, електронні замовлення від покупців, електронні документи для друку, запити в Інтернет.

13 Запити до БД, електронне листування, запити в Інтернет.

14 Електронні звіти, запити до БД, електронні документи для друку, електронне листування, замовлення постачальникам.

15 Електронні звіти, запити до БД, електронні документи для друку, електронне листування.

Вищий гриф секретності оброблюваної інформації - конфіденційна, що містить комерційну інформацію про підприємство і клієнтів.

1.1.4 Комерційна таємниця

Комерційною таємницею можуть бути відомості технічного, організаційного, комерційного, виробничого і іншого характеру, за винятком тих,

які відповідно до закону не можуть бути віднесені до комерційної таємниці.

До комерційної таємниці відносяться дані про клієнтів, постачання комплектуючих, грошовий оборот фірми, податкові звіти, зарплатні відомості.

Комерційною таємницею являються речі (у широкому сенсі слова, тобто враховуючи нематеріальну власність) чи інформація (виражена у будь-якій формі, навіть ніяк не зафіксована), які відповідають трьом вимогам:

- речі чи інформація володіють матеріальною чи нематеріальною цінністю;
- потрапляння інформації до третіх осіб може призвести до збитків підприємцю;
- на підприємстві прийняті адекватні заходи щодо збереження інформації в тайні.

Розповсюдженні приклади комерційної таємниці - формули, рецепти, нові винаходи (до тих пір, поки не видано патент), фінансова інформація, бізнес-плани та ідеї, маркетингові стратегії, комп'ютерні алгоритми, списки клієнтів.

Права власника (підприємства) на комерційну таємницю ніяк не реєструються. Строк захисту комерційної таємниці також не лімітований, на відміну від інших видів інтелектуальної власності. Комерційна таємниця захищається так довго, поки власник може зберегти інформацію в таємниці, при умові, що вона як і раніш має цінність.

Зрозуміло, що просто назвати інформацію комерційною таємницею недостатньо, щоби вона стала такою. Власник повинен прийняти розумні міри для збереження інформації в таємниці. Питання, що вважати «розумними» мірами, неоднозначне и вирішується в індивідуальному порядку у кожному конкретному випадку.

Стандартні заходи для забезпечення конфіденційності - помітка «конфіденційно» на папках (ящиках, шафах) з документами, обмеження доступу до інформації тільки визначеному колу осіб, міри комп'ютерної безпеки, зберігання документів у сейфі і т.д.

Найбільш розповсюджений спосіб захисту комерційної таємниці - згода про нерозголошення комерційної таємниці (чи збереження конфіденційності). Такий договір рекомендується заключати з усіма, кому в тій чи іншій мірі становиться доступна комерційна таємниця.

Наявність договору про нерозголошення конфіденційної інформації дає її власнику право вимагати:

1 Завершення подальшого використовування чи розголошування комерційної таємниці;

2 Виплати встановлених договором штрафних санкцій за порушення умов договору;

3 Компенсації всіх збитків, заподіяних в результаті порушення (як додаток до штрафних санкцій).

Для захисту своїх інтересів у випадках порушення договору можливо звернення до суду.

1.2 Аналіз державної нормативно-правової бази у сфері захисту комерційної таємниці та оцінки

Визнання прав приватної власності, відмовлення держави від монополії в сфері управління економікою і проголошення свободи підприємницької діяльності спричинили за собою появу великої кількості суб'єктів підприємницької діяльності. Підприємці одержали право здійснювати у встановленому законом порядку будь-які види діяльності, вибирати торговельних партнерів і укладати угоди, наймати працівників, самостійно визначати порядок використання отриманого прибутку.

Одночасно з новими економічними відносинами з'явилися нові економічні правопорушення серед самих підприємців – несумлінна конкуренція. Одним із проявів неконкурентних дій є неправомірне використання відомостей, що складають комерційну таємницю суб'єкта підприємницької діяльності.

Термін «комерційна таємниця» був введений у правовий оборот Законом України «Про підприємства в Україні» від 27.03.1991р. Під комерційною

таємницею підприємства розуміються відомості, пов'язані з виробництвом, технологічною інформацією, управлінням, фінансами й іншою діяльністю підприємства, що не є державною таємницею, розголошення (передача, витік) які може заподіювати збиток його інтересам.

Комерційна таємниця має наступні, властиві тільки її, відмінні ознаки. А саме:

1 Предмет комерційної таємниці;

2 Суб'єкт комерційної таємниці;

3 Заборона розголошення відомостей, що складають комерційну таємницю;

4 Наявність збитку і несприятливих наслідків для особи, що причинили.

5 Збиток власникові комерційної таємниці.

Розглянемо кожний з них.

Предмет «комерційної таємниці». Предметом «комерційної таємниці» є відомості, пов'язані з комерційною і господарською діяльністю підприємства: виробнича і технологічна інформація, інформація про управління, фінанси й іншу діяльність. Це можуть бути документи про комерційні переговори підприємства і методи ціноутворенні, документи пов'язані з маркетинговими дослідженнями ринку, відомості про організацію праці і підбір працівників, інформація про умови збереження документів, тобто відомості, що мають комерційну цінність.

Термін «комерційна таємниця» часто ототожнюють з терміном «конфіденційна інформація». На думку автора термін «конфіденційна інформація» є родовим стосовно терміна «комерційна таємниця». Згідно Закону України «Про інформацію» від 02.10.1992р. конфіденційна інформація це відомості, що знаходяться у володінні, користуванні або розпорядженні окремих фізичних або юридичних осіб і поширюються за їхнім бажанням відповідно до передбаченими ними умовами. Особливістю відомостей, що складають комерційну таємницю, як вид конфіденційної інформації, є їх комерційний і господарський характер. Іншими словами, це інформація, що має економічну

цінність, здатна впливати на фінансове становище суб'єкта підприємницької діяльності, розмір одержуваного ним прибутку.

Кожен підприємець самостійно визначає склад відомостей, що відносяться до комерційної таємниці. Законодавством України встановлені два обмеження, застосовуваних до таких відомостей.

По-перше, відомостями, що складають комерційну таємницю, не можуть бути відомості, що складають державну таємницю. Правовий режим відомостей, що складають державну таємницю, регулюється Законом України «Про державну таємницю» від 21.01.1994р. Державна таємниця – це вид секретної інформації, що включає відомості в сфері оборони, економіки зовнішніх відносин, державної безпеки й охорони правопорядку, розголошення яких може заподіяти шкоду життєво важливим інтересам України і які визнані законом державною таємницею і підлягають охороні з боку держави. Державним комітетом України з питань державних секретів затверджений перелік відомостей, що складають державну таємницю.

По-друге, Кабінетом Міністрів України затверджений перелік відомостей, що не складають комерційну таємницю. Ці відомості використовуються при здійсненні перевірок контролюючими органами, аудиторами для проведення аудита, при здачі звітності в різні фонди. До них відносяться:

1) статутні документ, документи, що дозволяють займатися підприємницькою або господарською діяльністю і її окремими видами;

2) інформація з усіх установлених форм державної звітності;

3) дані, необхідні для перевірки вирахування і сплати податків і інших обов'язкових платежів;

4) зведення про чисельність і склад працюючій, їхній заробітній платі в цілому за професіями і посадами, а так само наявність вільних місць;

5) документи про сплату податків і обов'язкових платежів;

6) інформація про забруднення навколишнього природного середовища, недотриманні безпечних умов праці, реалізацію продукції, що заподіює шкоду

здоров'ю, а так само інших порушень законодавства України і розмірах заподіяних при цьому збитків;

7) документи про платоспроможність;

8) відомості про участь посадових осіб підприємства в кооперативах, малих підприємствах, союзах, об'єднаннях і інших організаціях, що займаються підприємницькою діяльністю;

9) відомості, що відповідно до діючого законодавства підлягають розголошенню.

Хоча зазначені відомості не віднесені до відомостей, що складають комерційну таємницю, але вони і не є відкритими і загальнодоступними. Надаватися вони можуть лише по підставах встановленим у нормативних актах України. Так, наприклад, відповідно до Закону України «Про міліцію» від 20.12.1990р. міліції для виконання своїх обов'язків дане право безперешкодно і безкоштовно одержувати від підприємств, установ і організацій незалежно від форм власності по письмовому запиті відомості, у тому числі відомості, що складають комерційну таємницю, необхідні по справах про злочини, що знаходяться у впровадженні міліції. Для здійснення загального нагляду підприємства, установи й організації повинні представляти прокуророві свою документацію, у тому числі, по його письмовій вимозі, відомості, що складають комерційну таємницю, і, у разі потреби, прокурор має право вимагати передачу для перевірки зазначених документів у прокуратуру.

Терміном «комерційна таємниця» не охоплюються відомості, що складають банківську таємницю, страхову таємницю, авторські права. Зазначені відомості складають самостійні групи конфіденційної інформації із своїм відмінним від «комерційної таємниці» правовим регулюванням.

Суб'єкти «комерційної таємниці» Суб'єктами «комерційної таємниці» є:

1) суб'єкт підприємницької діяльності;

2) персонал, працівники суб'єкта підприємницької діяльності;

3) службові особи державних організацій і органів, що проводять перевірку підприємства.

Суб'єктом підприємницької діяльності – власником відомостей, що складають комерційну таємницю, – є як юридичні особи, так і фізичні особи – підприємці. Для зручності викладу, надалі по тексту, будемо іменувати обидві категорії суб'єктів підприємницької діяльності підприємцями.

Організаційна форма і форма власності не мають значення для віднесення суб'єкта права до категорії підприємців. Головне, щоб діяльність здійснювана такою особою була спрямована на одержання прибутку, носила комерційний характер і це було зафіксовано в установчих документах (якщо наявність таких є обов'язковою умовою здійснення підприємницької діяльності). Склад і обсяг відомостей, що складають комерційну таємницю, порядок роботи з ними і їхнього захисту визначається підприємцем самостійно.

Працівники мають право користуватися відомостями, що складають комерційну таємницю, для виконання своїх трудових обов'язків. Ступінь доступу кожного з працівників до такої інформації визначається підприємцем самостійно, а умови користування - документами, затвердженими підприємцем, і трудовим договором (контрактом).

Службовці державних організацій і органів, що проводять перевірки підприємця, одержують доступ до комерційної таємниці на підставі відповідних актів державних органів і організації. Інформацію про «комерційну таємницю» підприємця вони одержують у рамках адміністративних правовідносин. Обсяг їхнього доступу до такої інформації обмежується напрямком перевірки, про що повинно бути зазначене в документах на перевірку. За розголошення комерційної таємниці службовці державних органів і організації несуть відповідальність, установлену законодавством України. Загальною підставою такої відповідальності є Закон України «Про підприємства», вимоги якого про нерозголошення комерційної таємниці поширюються на всіх службових осіб державних органів і організацій. Але така вимога може бути передбачено

законодавчим актом, що регулює правове положення окремо про державний орган або організацію. Зокрема, Законом України «Про державну податкову службу» передбачена відповідальність співробітників податкових органів за розголошення відомостей, що складають комерційну таємницю (про види відповідальності див. нижче).

Заборона розголошення, відомостей, що складають комерційну таємницю. Відомості, що складають комерційну таємницю, не повинні бути загальнодоступні в силу своєї популярності необмеженому колу суб'єктів, або вимог закону про обнародування, або за іншими підставами. Тільки власник може визначити коло зведень підметів розголошенню, установлювати випадки й осіб, через які може відбуватися таке розголошення і при тім воно буде вважатися правомірним з погляду права. Крім того, нормативними актами України може бути передбачені обов'язкове надання або публічне обнародування відомостей, що складають комерційну таємницю. Будь-яке інше розголошення зазначених відомостей не є правомірним.

Вимога не розголошення комерційної таємниці має подвійну спрямованість: внутрішню і зовнішню. Внутрішня спрямована на працівників суб'єкта підприємницької діяльності, зовнішня – на службових осіб організацій і органів, що проводять перевірку підприємства.

Згідно Закону України «Про захист від недобросовісної конкуренції» від 07.06.1998р. розголошення комерційної таємниці – це ознайомлення іншої особи без згоди особи, уповноваженого на це, з відомостями, що відповідно до діючого законодавства України, складають комерційну таємницю, особою, якій ці відомості були довірені у встановленому порядку або стали відомі в зв'язку з виконанням службових обов'язків, у випадку якщо це заподіяло або могло заподіяти шкоду суб'єктові, що хазяює, (підприємцеві).

Хотілося б звернути увагу на один правовий нюанс, що існує у вищевказаному визначенні розголошення комерційної таємниці. У Законі України «Про підприємства в Україні» право визначати коло відомостей, що складають

комерційну таємницю, надано підприємцеві, а згідно Закону України «Про захист від недобросовісної конкуренції» такі відомості визначаються відповідно до діючого законодавства. Підприємцеві надане право самостійне визначати коло відомостей, які є комерційною таємницею, а нормативними актами України встановлюються тільки обмеження на віднесення інформації до комерційної таємниці, відповідальність за порушення, пов'язані з використанням комерційної таємниці, порядок її охорони. Таке захоплення відсильними нормами права часто приводить до того, що виникає нерозв'язна ситуація: є реальне правовідношення, є відсильна норма права, але немає норми до якої вона відсилає.

У Законі України «Про підприємства в Україні» установлені дві форми розголошення відомостей, що складають комерційну таємницю: передача і витік відомостей, що складають комерційну таємницю. З юридичної точки зору зазначені форми являють собою самостійні склади правопорушень. Передача відомостей, що складають комерційну таємницю – це незаконне ознайомлення третіх осіб із відомостями, віднесеними суб'єктом підприємницької діяльності до комерційної таємниці, особою, якій такі відомості відомі в зв'язку з виконанням своїх трудових обов'язків або в якого мається доступ до них і зв'язку з виконанням посадових обов'язків. Під витоком відомостей, що складають комерційну таємницю, розуміються навмисні або ненавмисні дії осіб, що мають доступ до комерційної таємниці, що сприяють ознайомленню з такими відомостями третіх осіб.

Способи розголошення відомостей, що складають комерційну таємницю, можуть бути різними: передача інформації конкурентам підприємця; ознайомлення з комерційною таємницею службових осіб державних організацій і органів без належних на те прав і основ як з боку розголошувача, так і з боку державного службовця, розголошення відомостей, що складають комерційну таємницю, через засоби масової інформації; використання в особистих цілях – передача родичам, знайомим для заняття власною підприємницькою діяльністю.

Мотиви розголошення так само можуть бути різні: користь, особисті неприязні відносини, халатне відношення до трудових і службових обов'язків.

Вимога дотримання і нерозголошення комерційної таємниці є не тільки правом, але й обов'язком суб'єкта підприємницької діяльності. Без належного дотримання вимог до користування і збереження інформації, що складає комерційну таємницю, неможливо забезпечити необхідну охорону такої інформації як цивільно-правовими мірами, так і державно-примусовими.

Обов'язок зберігати в таємниці зазначені відомості так само може бути встановлена в нормативних актах України. Наприклад, у Положенні про порядок заключення контрактів при прийнятті (найманні) на роботу працівників визначено, що роботодавець зобов'язаний не розголошувати конфіденційні умови контракту з працівником.

Наявність збитку і несприятливі наслідки для осіб, що заподіяли збиток власникові комерційної таємниці. До відомостей, що складають комерційну таємницю, можуть бути віднесені тільки ті відомості, розголошення яких може завдати шкоди підприємцеві. Причому не має значення який вид збитку може бути заподіяний, збиток майновим або немайновим правам (моральний збиток).

Права суб'єкта підприємницької діяльності підлягають захистові, а заподіяна шкода відшкодуванню в обох зазначених випадку.

В даний час за порушення прав власника комерційної таємниці законодавством України встановлені наступні види відповідальності:

1) відповідальність у рамках трудових відносин;
2) цивільно-правова відповідальність;
3) адміністративна відповідальність;
4) кримінальна відповідальність.

Відповідальність у рамках трудових відносин. За недотримання режиму роботи з інформацією, що складає комерційну таємницю, до працівників суб'єкта підприємницької діяльності може бути застосована матеріальна і дисциплінарна відповідальність. Залучення до матеріальної і дисциплінарної відповідальності

здійснюється на загальних підставах, з урахуванням особливостей правового статусу «комерційної таємниці». Для законного застосування санкцій за правопорушення, пов'язаних з комерційною таємницею в рамках трудових відносин, підприємцеві необхідно мати деякі документи, а саме:

1) документ, що встановлює перелік відомостей, які складають комерційну таємницю. Це може бути затверджене підприємцем (компетентним органом управління суб'єкта підприємницької діяльності) Положення про комерційну таємницю, у якому б чітко обмовлялися які відомості є комерційною таємницею, порядок віднесення їхній до таких, умови збереження, а так само хто з працівників підприємця може передавати закриті відомості представникам державних органів і організацій;

2) посадові інструкції. Посадовими інструкціями повинно визначатися коло повноважених працівників підприємця і відомості, що містять комерційну таємницю, з якими працівник має право працювати, порядок роботи з ними;

3) трудовий договір (контракт). У трудовому договорі або контракті повинна бути зазначено зобов'язання працівника дотримувати комерційної таємниці і наслідки недотримання цього обов'язку. Умови матеріальної відповідальності працівника за розголошення комерційної таємниці можуть бути передбачені як трудовим договором, так і окремою угодою про матеріальну відповідальність.

З документами, зазначеними в пункті а) і б), працівник повинний бути ознайомлений перед початком своєї трудової діяльності в даного підприємця. Факт ознайомлення повинний фіксуватися письмово, із указівкою дати ознайомлення.

За порушення режиму комерційної таємниці до працівника можуть бути застосовані наступні дисциплінарні санкції: догана, звільнення. Якщо була укладена угода про матеріальну відповідальність за розголошення відомостей, що складають комерційну таємницю, працівник так само відповідає і матеріально, у розмірах передбачених угодою сторін.

Цивільно-правова відповідальність. Відповідно до статті 440 Цивільного кодексу України заподіяна шкода повинна бути відшкодована в повному обсязі. При цьому, у відповідності із статтею 440 зазначеного кодексу, відшкодування моральної шкоди не пов'язано з відшкодуванням матеріальної, а розмір відшкодування визначається судом.

Моральний збиток відшкодовується в грошовій або іншій матеріальній формі. У будь-якому випадку розмір відшкодування не може бути менш 5 мінімальних розмірів заробітної плати.

Законодавство України не містить вичерпного переліку обставин, з настанням яких підприємець може зв'язувати заподіяння йому моральної шкоди. У позовній заяві по справах, зв'язаним з розголошенням комерційної таємниці, необхідно вказувати яка саме шкода була заподіяна розголошенням, у чому саме складається заподіяний моральний збиток, якими протиправними діями відповідача був заподіяний збиток.

Підставою для відшкодування збитку є рішення суду (господарського СУДУ)-

Адміністративна відповідальність. Адміністративна відповідальність за порушення, пов'язані з комерційною таємницею, установлюється за одержання, використання, розголошення комерційної таємниці ч. 3 ст. 164-3 Кодексу про адміністративні правопорушення України. Установлене для порушника покарання – штраф.

Законом України «Про захист від недобросовісної конкуренції» передбачена відповідальність за неправомірний збір комерційної інформації (ст.16), розголошення комерційної таємниці (ст.17), схилення до розголошення комерційної таємниці (ст. 18), неправомірне використання комерційної таємниці (ст.19). Цим же законом регулюється порядок подачі і розгляду заяв по зазначених правопорушеннях в Антимонопольний комітет України.

Кримінальна відповідальність. Кримінальним кодексом України передбачені наступні злочини зв'язані з порушенням вимог охорони комерційної таємниці:

- стаття 148-6 незаконний збір з метою використання або використання відомостей, що складають комерційну таємницю. Установлене покарання: позбавлення волі на термін до 3 років або штрафом;
- стаття 148-7 розголошення комерційної таємниці. Установлене покарання: позбавлення волі до 2 років, або виправні роботи до 2 років, позбавлення права займати визначені посади або займатися визначеною діяльністю на термін до 3 років, або штрафом.

Відповідальність за розголошення відомостей в рамках трудового права і цивільно-правова відповідальність найбільш значимі для підприємця тому, що дозволяють оперативно реагувати на факти порушення режиму «комерційної таємниці» і одержувати відшкодування збитку, заподіяного таким розголошенням.

У завершення розгляду терміна «комерційна таємниця» підведемо деякі підсумки.

Правові норми в сфері застосування терміна «комерційна таємниця» не одержали достатнього розвитку, законодавець обмежився тільки встановленням мінімальної кількості норм, що регулюють дане правове питання. Найбільший розвиток одержали норми, пов'язані з державними гарантіями розвитку і захисту підприємницької діяльності. Це норми антимонопольного законодавства, що регулюють випадки відповідальності за неконкурентні дії, пов'язані з використанням комерційної таємниці, процедуру їхнього розслідування і санкції до порушників, а так же умовно кримінально карних діянь. Разом з тим, підприємцям дана відносна воля у встановленні відомостей, що складають комерційну таємницю, і режиму її дотримання. Але через низьку правову культуру зазначене право не завжди використовується або використовується з досить серйозними порушеннями.

Рівень економічної свободи в країнах, що мають розвиту і стабільну економіку, характеризується рівнем захисту немайнових прав його суб'єктів, а також діловими етичними нормами здійснення підприємницької діяльності. В даний час на Україні вони тільки починають складатися і необхідно їхній подальший розвиток.

1.2.1 Регулювання оціночної діяльності

Законодавство, яке регулює оціночну діяльність в Україні, складається з закону " Про оцінку майна, майнових прав та професійну оціночну діяльність в Україні" і, прийнятих відповідно до нього законів та інших нормативних правових актів України, законів та інших нормативних правових актів суб'єктів України, а також з міжнародних договорів.

У становленні та розвитку оціночної діяльності в Україні активну участь беруть саморегульовані організації оцінювачів. Законом передбачено крім державного регулювання саморегулювання діяльності оцінювачів.

Механізми регулювання оціночної діяльності.

Основними механізмами регулювання оціночної діяльності є: ліцензування оцінювачів; атестація фахівців в області оціночної діяльності; система стандартів та положень оціночної діяльності; затвердження навчальних програм з перепідготовки фахівців в області оціночної діяльності; сертифікація послуг; страхування цивільної відповідальності оцінювачів.

Оціночна діяльність може здійснюватися тільки отримала відповідну ліцензію юридичною особою або індивідуальним підприємцем. Ліцензування оціночної діяльності здійснюють Союз експертів України та органи виконавчої влади суб'єктів України, що визначаються в порядку, встановленому законодавством суб'єктів України (далі іменуються – ліцензіюючі органи).

Ліцензія на право оцінки підприємств (бізнесу) надає ліцензіату право на здійснення оціночної діяльності за всіма видами оціночної діяльності. При цьому оціночна діяльність, ліцензія на здійснення якої видана Союзом експертів України, може здійснюватися на всій території України. Оціночна діяльність,

ліцензія на здійснення якої видано ліцензіюючим органом суб'єкта України, може здійснюватися на території відповідного суб'єкта України. На території інших суб'єктів України така діяльність може здійснюватися відповідно до встановленого Урядом України порядком реєстрації ліцензій, виданих органами виконавчої влади суб'єктів України, на територіях інших суб'єктів України.

Відкликання ліцензії на здійснення оціночної діяльності здійснюється на підставах, передбачених законом "Про оцінку майна, майнових прав та професійну оціночну діяльність в Україні ". Нагляд за дотриманням ліцензіатом ліцензійних вимог і умов здійснюється державними наглядовими і контрольними органами, Союз експертів України, що ліцензує органами суб'єктів України в межах їх компетенції. Союзом експертів України у встановленому порядку здійснює взаємодію з ліцензують органами суб'єктів України з питань оціночної діяльності, а також координацію їх діяльності.

Для отримання ліцензії її здобувач повинен, зокрема, представити документи, що підтверджують проходження атестації за зазначеними у ліцензії видів оціночної діяльності співробітниками здобувача (для юридичної особи), або власних таких документів (для індивідуального підприємця).

Атестація фахівців з оцінки вартості покликана забезпечити: контроль знань фахівців в області оціночної діяльності; належну відповідальність фахівця а області оціночної діяльності за результати його роботи; контроль якості підготовки фахівців навчальними закладами.

Атестати видаються на здійснення наступних видів оціночної діяльності: оцінка нерухомості, оцінка машин, обладнання та транспортних засобів; оцінка нематеріальних активів; оцінка підприємств (бізнесу). Атестат на оцінку бізнесу дає право його власникові виконувати оцінку за всіма видами оціночної діяльності.

Для проведення атестації уповноважені органи створюють відповідні державні атестаційні комісії. Видані атестати діють на всій території України. Уповноваженими органами ведуться реєстри кваліфікаційних атестатів. Союз

експертів України організує ведення єдиного державного реєстру кваліфікаційних атестатів. Після закінчення терміну дії атестата фахівця в області оціночної діяльності необхідно пройти переатестацію. Атестат буде надавати його власнику право підпису звіту про оцінку за відповідним видом оцінної діяльності.

1.2.2 Стандарти оціночної діяльності

Оціночна діяльність повинна здійснюватися в суворій відповідності з затверджуваної Урядом України Єдиною системою стандартів оцінки.

Єдина система стандартів оцінки, будучи невід'ємною частиною нормативно-правового регулювання оціночної діяльності, повинна забезпечувати:

- нормативне закріплення єдності методичних підходів при виконанні робіт з оцінки вартості;
- чіткі вимоги до найважливіших процесу оцінки, а також її результатами;
- уніфікацію вимог до складу і формами представлення документів, що відображають результати оцінки;
- відтворюваність результатів оцінки, стабільність якісних показників надаються оціночних послуг;
- визначення обсягу техніко-економічної інформації, використовуваної при оцінці;
- створення умов для дієвого контролю за якістю оціночних послуг.

Єдина система стандартів оцінки включає наступні основні стандарти:

- організаційно-методичні положення;
- оцінка нерухомого майна;
- оцінка машин, обладнання та транспортних засобів;
- оцінка інтелектуальної власності;
- оцінка вартості підприємства (бізнесу).

Система стандартів захищає інтереси і прав споживачів при взаємодії з оцінювачами з одного боку і забезпечує захист оцінювачів від необґрунтованих претензій з іншого.

1.3 Загальні відомості по створенню інформаційної безпеки

Політика безпеки має складну двояку природу та має пасивну і активну складову. З одного боку політика безпеки – це система взаємозв'язаних та узгоджених правил безпеки, які регламентують порядок обробки інформації в ІТС і направлених на запобігання визначеної множини погроз безпеці (пасивна складова). З цих позицій політика безпеки повинна мати властивості непротирічливості цілей безпеки та головної цілі функціонування ІТС, повноти вимог безпеки, непротирічливості правил безпеки вимогам нормативних документів і стандартів, законності, узгодженості. Пасивна складова відповідає за формування правил безпеки і по суті відповідає за формування політики безпеки. Правила безпеки на замінюють інструкції та стандарти, не є директивами і засобами управління і описують безпеку в загальних термінах і не дають вказівки, яким чином здійснюються конкретні заходи безпеки.

З іншого боку політика безпеки - це систематична, стабільна, організована та цілеспрямована ДІЯЛЬНІСТЬ власника ІТС відносно рішення проблем забезпечення безпеки інформації, що здійснюється або безпосередньо самим власником, або через відповідні механізми і органи управління та впливає на функціонування ІТС у цілому (активна складова). З позиції діяльнісного підходу політика безпеки повинна бути цілеспрямованою, стабільною, неперервною, організованою, управляємою, узгодженою, мотивованою, забезпечувати максимальну результативність і ефективність при досягненні цілей безпеки і вирішення задач захисту, бути адекватною погрозам безпеки, придатною та гнучкою у реалізації, здійснюваною на різних рівнях забезпечення безпеки інформації, досить простою у адміністративному забезпеченні.

Основними складовими політика безпеки є: концепція і програма забезпечення безпеки інформації в ІТС, менеджмент безпеки, інжиніринг безпеки і аудит безпеки.

Правила безпеки важливі для забезпечення якісного управління безпекою, вибору номенклатури засобів захисту інформації, демонстрації активної

підтримки власником процесів забезпечення безпеки інформації в ІТС, знищення організаційних і економічних перешкод створенню комплексної системи захисту інформації в ІТС, забезпечення послідовного і повного захисту інформаційних ресурсів на систематичній основі.

Загальний порядок розробки пасивної складової політики безпеки включає обробку вихідних даних відносно об'єкта захисту і середовища його експлуатації, визначення цілей і задач політики безпеки, розробку структури ІТС, знищення організаційних і економічних перешкод створенню комплексної системи захисту інформації в ІТС, забезпечення послідовного і повного захисту інформаційних ресурсів на систематичній основі.

Загальний порядок розробки пасивної складової політики безпеки включає обробку вихідних даних відносно об'єкта захисту і середовища його експлуатації, визначення цілей і задач політики безпеки, розробку структури
і конкретного змісту політики безпеки, визначення шляхів впровадження у життя та реалізації положень, правил, норм та вимог політики безпеки, а також визначення ступеню відповідальності за порушення вимог ПБ та контроль за їх виконанням.

Загальними задачами, на вирішення яких направлена політика безпеки є:

- забезпечення конфіденційності, цілісності та доступності інформації в ІТС;
- безпечне функціонування ІТС із придатним рівнем ризику;
- управління інформацією та ресурсами з метою вдоволення експлуатаційних вимог до ІТС;
- проведення цілеспрямованої та структурованої діяльності по тестуванню і оцінці безпеки при реалізації розробляєм их та пропонуємих до застосування функцій та механізмів безпеки;
- проведення аудиту безпеки, сертифікації та акредитації компонентів ІТС для прийняття рішення про можливість функціонування системи у захищеному режимі з вимагаємим рівнем ризику.

1.4 Система управління інформаційною безпекою

Система управління інформаційною безпекою - це частина загальної системи управління, що базується на аналізі ризиків і призначена для проектування, реалізації, контролю, супроводження та вдосконалення заходів у галузі інформаційної безпеки. Цю систему складають організаційні структури, політика, дії з планування, обов'язки, процедури, процеси і ресурси.

Найбільш значущою метою більшості систем інформаційної безпеки є захист бізнесу та знань компанії від знищення або витоку. Також однією з основних цілей системи інформаційної безпеки є гарантія майнових прав та інтересів клієнтів. У той же час заходи з інформаційної безпеки не повинні обмежувати або ускладнювати процеси обміну знаннями в компанії, оскільки це може поставити під загрозу розвиток організації.

Система управління інформаційною безпекою повинна забезпечувати гарантію досягнення таких цілей як забезпечення конфіденційності критичної інформації, забезпечення неможливості несанкціонованого доступу до критичної інформації, цілісності інформації та пов'язаних з нею процесів (створення, введення, обробки і виведення) і ряду інших цілей.

Досягнення заданих цілей можливо у ході вирішення таких основних завдань, таких як визначення відповідальних за інформаційну безпеку, розробка спектра ризиків інформаційної безпеки та проведення їх експертних оцінок, розробка політик і правил доступу до інформаційних ресурсів, розробка системи управління ризиками інформаційної безпеки, у тому числі методи їх оцінки, контролінг інформаційної безпеки на підприємстві. Слід зазначити, що тут перераховано не повний список.

Виділяється чотири стадії реалізації системи управління інформаційною безпекою:

1 Формування політики в галузі ризиків.

2 Аналіз бізнес-процесів.

3 Аналіз ризиків.

4 Формування цільової концепції.

І дві стадії подальшого управління ризиками:

1 Звіти за ризиками.

2 Контроль ризиків.

Формування політики в галузі ризиків передбачає визначення принципів управління ризиками для всієї компанії в цілому. Ці принципи базуються на цілях компанії, її стратегії, а також на вимоги, що пред'являються законом і стандартами в галузі інформаційної безпеки. Одним і ключових чинників успішності системи управління інформаційною безпекою підприємства - це побудова її на базі міжнародних стандартів серії ISO / IEC 27001.

1.4.1 Модель системи інформаційної безпеки підприємства

Розглянемо основні компоненти моделі системи інформаційної безпеки.

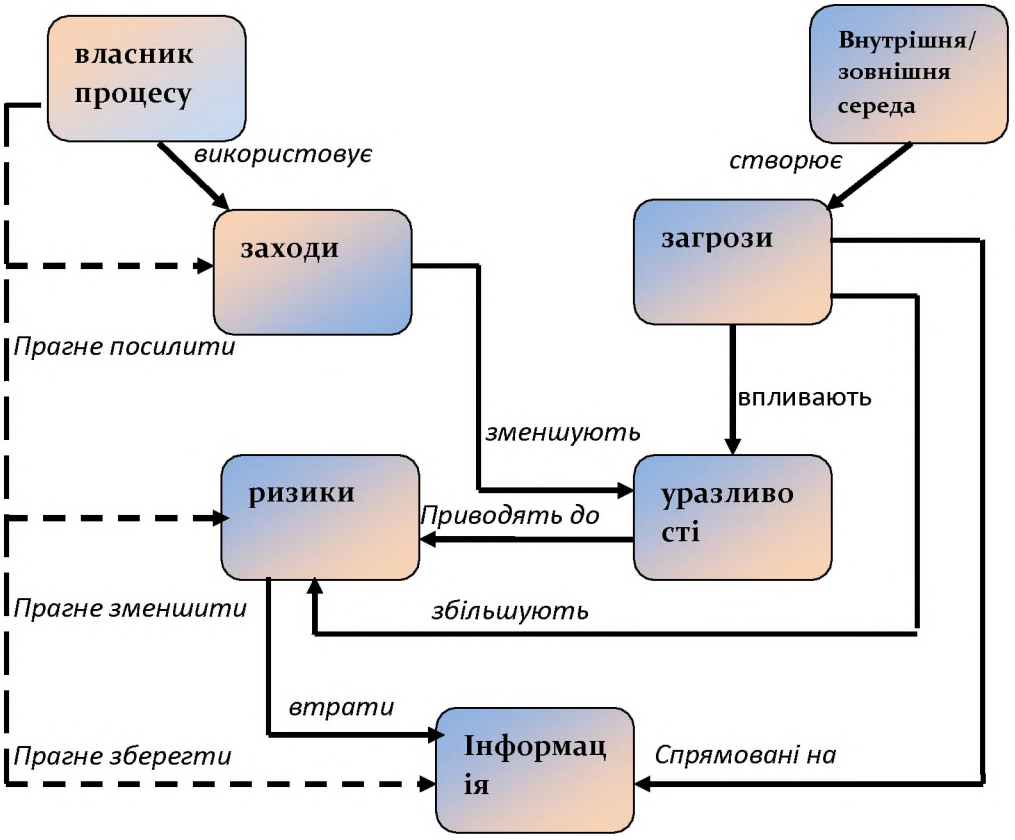

Рисунок 1.1- Модель системи інформаційної безпеки підприємства

Представлена на рис. 1.1 модель інформаційної безпеки - це сукупність зовнішніх і внутрішніх факторів та їх вплив на стан інформаційної безпеки в компанії та на забезпечення збереження ресурсів (матеріальних чи

інформаційних). Прямокутниками на малюнку представлені зовнішні і внутрішні фактори. Пунктирними стрілками вказані напрямки керуючого впливу, а суцільними - природного.

Розглядаються такі фактори як:

- загрози інформаційної безпеки. Вони характеризуються ймовірністю виникнення і реалізації;
- вразливості системи інформаційної безпеки, які впливають на ймовірність реалізації загрози;
- збитки, що відображають реальний збиток в результаті реалізації загрози інформаційної безпеки.
- ризики, що відображають передбачуваний збиток організації в результаті реалізації загрози інформаційної безпеки.
- Об'єкти захисту

Необхідно чітко розуміти, що слід захищати і від яких загроз. Інформація та матеріальні ресурси, які необхідно захищати, називаються об'єктами захисту. До них відноситься мовна інформація, інформація, що зберігається і обробляється за допомогою засобів зв'язку та інформатизації у вигляді різних носіїв інформації, документи на паперових носіях і т.д.;

1.4.2 Види загроз

Розглянемо докладніше, з якими загрозами може зіткнутися сучасне підприємство і як може порушуватися його інформаційна безпека.

Загрози класифікуються за природою виникнення (загрози випадкового або навмисного характеру) і по тому, як вони ставляться до захищається (зовнішні і внутрішні загрози).

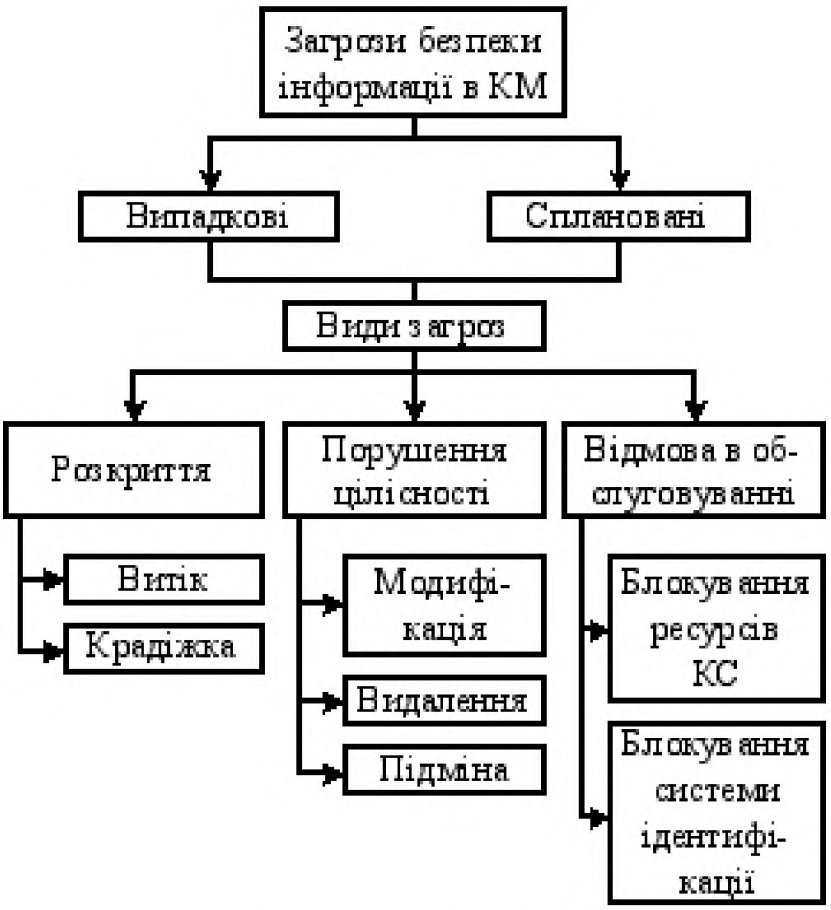

Рисунок 1.2 - Класифікація загроз

На рис. 1.2 представлена одна з найбільш популярних класифікацій загроз.

1.4.3 Види порушень

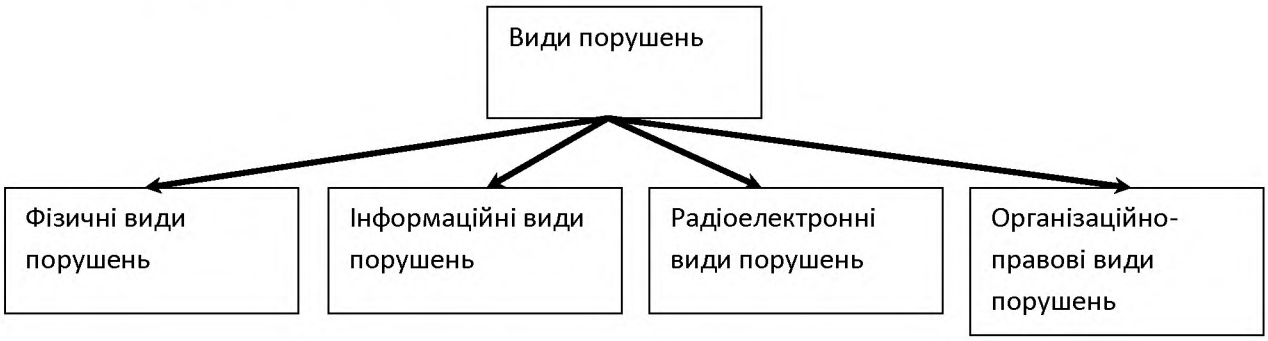

Рисунок 1.3 - Види порушень

Порушення можуть бути декількох видів (рис. 1.3).

- Організаційно-правові види порушень - це порушення, пов'язані відсутністю єдиної узгодженої політики компанії в сфері захисту інформації, невиконанням вимог нормативних документів, порушенням режиму доступу, зберіганням та знищення інформації.
- Інформаційні види порушень включають несанкціоноване отримання повноважень доступу до баз і масивів даних, несанкціонований доступ до активного мережевого обладнання, серверів доступу, некоректне застосування засобів захисту та помилки в управлінні ними, порушення в адресності розсилки інформації при веденні інформаційного обміну
- Фізичні види порушень включають фізичне пошкодження апаратних засобів автоматизованих систем, ліній зв'язку і комунікаційного устаткування, крадіжки або несанкціоноване ознайомлення з вмістом носіїв інформації, що зберігаються в неналежних місцях, розкрадання носіїв інформації, відмови апаратних засобів та ін.
- До радіоелектронним видам порушень відносяться такі порушення, як впровадження електронних пристроїв перехоплення інформації, отримання інформації шляхом перехоплення і дешифрування інформаційних потоків, дистанційна відеозапис (фотографування) моніторів, комп'ютерних роздруківок, клавіатури, нав'язування неправдивої інформації в локальних обчислювальних мережах, мережах передачі даних і лініях зв'язку .

Для протидії загрозам та припинення порушень на підприємстві доцільно організувати процес управління ризиками компанії. Даний процес є ядром системи інформаційної безпеки компанії і включає такі підпроцеси як

- збору ризиків;
- оцінки загроз;
- оцінки вразливостей;
- оцінки збитків;
- визначення порогу для управління ризиками;
- реалізації заходів інформаційної безпеки;

- оцінки ефективності отриманих результатів (процес аудиту).

1.4.4 Методологія

Побудова ефективної системи управління інформаційною безпекою - це не разовий проект, а комплексний процес, наплавлений на мінімізацію зовнішніх і внутрішніх загроз при обліку обмежень на ресурси і час.

Для побудови ефективної системи інформаційної безпеки необхідно спочатку описати процеси діяльності (рис. 4). Потім слід визначити поріг ризику - рівень загрози, при якому вона потрапляє в процес управління ризиками. Потрібно побудувати таку систему інформаційної безпеки, яка забезпечить досягнення заданого рівня ризику.

З точки зору процесного підходу систему інформаційної безпеки підприємства можна представити як процес управління ризиками (рис. 1.4). На даному малюнку прямокутниками показані узагальнені процеси верхнього рівня, а стрілками показані їх входи і виходи.

Мета будь-якого бізнес-процесу полягає у створенні виходу для отримання винагороди у вигляді іншого виходу. В даному випадку виходом є виключення настання ризикової ситуації або мінімізація її наслідків, а винагородою - збереження матеріальних і фінансових ресурсів.

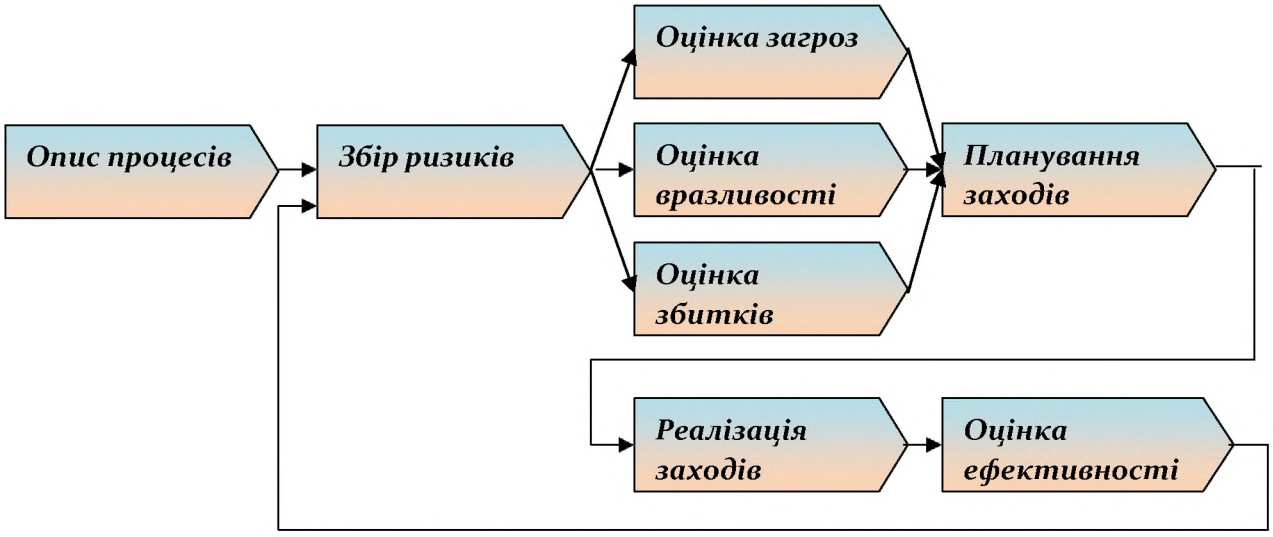

Рисунок 1.4 - Модель процесу управління ризиками для системи інформаційної безпеки підприємства

Важлива характеристика виходу - його затребуваність стороною, яка не є його виробником. Іншими словами, на даний вихід повинен бути попит. Коли існують загрози - існує і попит на захист від них, а значить, необхідно впроваджувати процес управління ризиками.

1.4.5 Управління ризиками

Одним з найбільш відомих підходів до управління ризиками є метод CRAMM (the UK Goverment Risk Analysis and Managment Method). Даний метод був розроблений Службою Безпеки Великобританії (UK Security Service) за завданням Британського уряду і прийнятий в якості державного стандарту. Він використовується, починаючи з середини 80-х років минулого століття як урядовими, так комерційними організаціями.

За минулі роки CRAMM придбав популярність у всьому світі. В основі методу лежить CRAMM комплексний підхід до оцінки ризиків, поєднуючи кількісні та якісні методи аналізу. Даний метод є узагальненим і підходить для більшості організацій. Одним з найбільш важливих результатів використання методу CRAMM є отримання можливості економічного обґрунтування витрат організації на забезпечення інформаційної безпеки та безперервності бізнесу. В кінцевому підсумку, економічно обґрунтована стратегія управління ризиками дозволяє мінімізувати витрати і уникати невиправданих витрат.

Пояснимо ключові моменти управління ризиками на прикладі. Для початку викладемо загальний сценарій.

Припустимо, виникла можливість загрози несанкціонованого доступу до фінансової інформації у зв'язку з виявленою уразливістю в обліковій системі, яка приймає електронні замовлення через Інтернет. На основі інформації про уразливість інформаційної системи вивчається питання про можливість реалізації ризику та економічної доцільності визначення заходів по його мінімізації (якщо заходи щодо запобігання ризиків коштують дорожче, ніж збитки від реалізації загрози, то, швидше за все, заходи застосовувати недоцільно). Після оцінки важливості ризику плануються необхідні заходи і виділяються необхідні ресурси.

Після планування реалізуються контрзаходи відповідно до графіка робіт. Потім оцінюється їх ефективність.

Перед тим як створювати корпоративну систему управління ризиками, необхідно описати критично важливі бізнес-процеси. В рамках даного процесу виконується аналіз і коректування бізнес-процесів. У нашому прикладі це може бути процес прийому електронних замовлень, в рамках якого база клієнтів організації доступна через Інтернет.

На етапі розробки та впровадження системи управління інформаційною безпекою, крім моделей критичних бізнес-процесів, може бути використовується інструментарій Process Risk Assistant, що відноситься до сімейства продуктів ARIS [1], призначений для методологічного забезпечення та містить детальне керівництво з впровадження системи управління інформаційною безпекою.

Після більш детального аналізу процесу та виявлення потенційних загроз необхідно сформувати перелік ризиків, які необхідно мінімізувати.

Метою процесу збору (ідентифікації) ризиків є виявлення схильності організації загрозам, які можуть завдати істотної шкоди.

Для збору ризиків проводиться аналіз бізнес-процесів компанії та опитування експертів предметної області. Результатом (виходом) даного процесу є класифікований перелік (список) всіх потенційних ризиків.

У представленому прикладі загроза несанкціонованого доступу до фінансової інформації є вихідні дані для ідентифікації, наприклад, такого ризику як «Витік інформації про клієнтів до конкурентів через незахищений канал зв'язку».

У зв'язку з тим, що наслідки від різних загроз нерівноцінні, недостатньо ідентифікувати ризик. Необхідно також оцінити величину загрози і можливість реалізації ризику, наприклад, у вигляді прямих або непрямих збитків у грошовому виразі, а також ймовірність ризику.

Мета процесу оцінки ризиків полягає у визначенні характеристик ризиків в інформаційній системі та її ресурси. Основним результатом (виходом) даного

процесу є перелік (список) всіх потенційних ризиків з їх кількісними та якісними оцінками збитку і можливості реалізації. Додатковим результатом даного процесу є перелік ризиків, які не будуть відстежуватися в організації

Всі дані, які є важливими з точки зору управління ризиками, моделюються, наприклад, за допомогою вищезгаданого програмного забезпечення ARIS. Інструментарій під назвою «Портал ризиків» (Process risk portal) забезпечує користувачу можливість проведення графічного аналізу та оцінки ризиків процесів. Крім того, процеси всередині компанії стають прозорими, а дані з управління ризиками - загальнодоступними, що і допомагає співробітникам здійснювати постійний моніторинг існуючих ризиків і виявляти нові.

На основі таких даних вибираються необхідні засоби управління інформаційною безпекою. Для нашого прикладу: якщо величина і можливість збитків для ризику «Витік інформації про клієнтів до конкурентів» досить велика, то доцільно спланувати заходи щодо мінімізації ризику (наприклад, планування процесу оперативного оновлення програмного забезпечення інформаційної системи (установка «латок»), формування регламентів доступу до інформації про клієнтів, впровадження засобів захисту від витоків конфіденційних даних і т.д.).

Метою процесу планування заходів з мінімізації ризиків є визначення строків і переліку робіт по виключенню або мінімізації збитку в разі реалізації ризику.

Даний процес дозволяє сформулювати, хто, де, коли, якими ресурсами і які загрози будить мінімізувати. Результатом (виходом) процесу планування є план-графік робіт по виключенню або мінімізації збитку від реалізованого ризику.

Мало зрозуміти, що, як і коли робити, але і необхідно реалізувати все заплановане «точно в строк». Тому метою процесу реалізації заходів є виконання запланованих заходів з мінімізації ризиків, контроль якості отриманих результатів та термінів їх виконання. Результатом даного процесу є виконані роботи з мінімізації ризиків та час їх проведення. Доцільно розробити плани дій на випадок виникнення критичної ситуації або ризику. Введення в дію процесів на екстрений

випадок допоможе не допустити збитки або мінімізувати їх, а також відновити господарську діяльність як можна швидше. Потім проводиться оцінка ефективності отриманих результатів.

1.5 Моделі безпеки

Важливою концепцією в проектуванні та аналізі безпечних систем є модель безпеки, оскільки вона включає в себе політику безпеки, яка повинна бути реалізована в системі. Модель - це символічне уявлення політики. Вона перетворює бажання творців політики в набір правил, яким повинна слідувати комп'ютерна система.

У цьому домені часто згадується політика безпеки та її важливість. Це пов'язано з тим, що політика є абстрактним поняттям, що становлять цілі і завдання, які повинна дотримуватися і реалізовувати система для того, щоб вважатися безпечною і прийнятною. Як нам перейти від абстрактної політики безпеки до моменту, коли адміністратор забороняє Девіду доступ до конфігураційних файлів системи, знімаючи позначку з відповідного пункту в графічному інтерфейсі? Цей шлях складається з безлічі складних кроків, що вживаються протягом проектування і розробки системи.

Модель безпеки перетворює абстрактні цілі політики в терміни інформаційних систем, точно описуючи структури даних та засоби (методи), необхідні для реалізації політики безпеки. Модель безпеки зазвичай представляється у вигляді математичних та аналітичних ідей, які потім перетворюються в технічні вимоги до системи, а потім розробляється програмістами в коді програми. Таким чином, ми маємо політику, реалізовує цілі безпеки, типу «кожен суб'єкт повинен бути авторизований для доступу до кожного об'єкту». Модель безпеки бере ці вимоги і надає необхідні математичні формули, взаємини і структуру, яким необхідно слідувати для досягнення цілей безпеки. Виходячи з цього, розроблено технічні вимоги для кожного типу операційної системи (Unix, Windows, Mac і т.д.), і окремі виробники можуть

вирішувати, як їм реалізовувати механізми, які будуть дотримуватися ці технічні вимоги.

Наведемо дуже загальний і спрощений приклад. Якщо політика безпеки стверджує, що суб'єкти повинні бути авторизовані для доступу до об'єктів, модель безпеки повинна надати математичні взаємовідносини та формули, що пояснюють, як х може отримати доступ до у тільки за допомогою визначених і описаних методів. Потім розробляються технічні вимоги, які є мостом між тим, що це означає в комп'ютерному середовищі і тим, як це пов'язано з компонентами та механізмами, які повинні бути розроблені. Після цього розробники пишуть програмний код для реалізації механізмів, що дозволяють використовувати ACL і надають адміністраторам певний ступінь управління. Ці механізми являють адміністратора графічний інтерфейс, в якому він може налаштувати розмежування доступу в рамках операційної системи, вибираючи, які суб'єкти можуть мати доступ до яких об'єктів. Це елементарний приклад, оскільки модель безпеки може бути дуже складною. Цей приклад використовується для демонстрації взаємовідносин між політикою безпеки і моделлю безпеки.

Деякі моделі безпеки, реалізують правила, що забезпечують захист конфіденційності. Інші моделі, реалізують правила, що забезпечують захист цілісності. Формальні моделі безпеки, використовуються для надання високого рівня гарантій безпеки. Неформальні моделі, більше використовуються в якості основи для опису того, як політики безпеки повинні виражатися і виконуватися.

Політика безпеки описує цілі без конкретизації того, як вони повинні бути досягнуті. Модель - це платформа, яка надає політиці форму і вирішує проблеми безпечного доступу до інформації в конкретних ситуаціях. Багато моделей безпеки розроблені для реалізації політик безпеки. Наступні розділи надають огляд кожної з моделей.

Взаємини між Політикою безпеки і Моделлю безпеки

Якщо хтось говорить вам, що потрібно вести правильний і здоровий спосіб життя, це дуже широке, загальне, абстрактне поняття. Коли ви запитуєте цієї

людини - як це зробити, він описує вам, що вам потрібно робити і що не потрібно (не наносити іншим шкоди, не говорити неправду, їсти овочі, чистити зуби і т.д.). Аналогічно, Політика безпеки надає абстрактні цілі, а Модель безпеки каже, що потрібно і що не потрібно робити, щоб досягти ці цілі

1.6 Висновки. Постановка задачі

В даній частині роботи розглянуто загальні відомості про захист комерційної таємниці, проаналізована державна нормативно-правова база у сфері захисті комерційної таємниці, представлена загальна інформація щодо побудування інформаційної безпеки на підприємстві.

Проведений аналіз об'єкту інформаційної діяльності приватного підприємства з оцінки майна, досліджена існуюча інформаційна система та інформація, що обробляється на підприємстві та підлягає захисту.

Після визначення та аналізу представлених даних доцільним буде побудувати та навести алгоритм для впровадження політики безпеки для підприємства

Для цього потрібно розробити модель загроз 1С та модель порушника для даного підприємства.

У кінцевій стадії необхідно провести оцінку ефективності впроваджених заходів і розробити документи та інструкцій.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Загальна характеристика підприємства

Об'єкт інформаційної діяльності, що розглядається у роботі – приватне підприємство з оцінки майна.

Приватне підприємство з оцінки майна надає оціночні послуги приватним та юридичним особам на транспорт та нерухомість, оцінка майна при розмитненні, переоцінка та підтвердження балансової вартості транспорту та нерухомості. Також підприємство займається видачою довідки-рахунок для переоформлення автомобілів, будівель, маєтків, квартир, тощо.

В організації працюють сертифіковані оцінщики які належать до союзу експертів України зі значним практичним досвідом роботи в сфері оцінки, оподатковування та фінансів.

Склад співробітників підприємства:

Директор;

Бухгалтерія - 1 чоловік;

Оцінщик - 2 чоловіка;

Довідка-рахунок - 1 чоловік;

Системний адміністратор. – 1чоловік (суб.підряд)

Режим роботи підприємства:

Кожен день з 8:30 до 19:00 неділя - вихідний.

Прибиральниця (зміна у 7:30 - 8:00 у дні роботи організації).

Підприємство орендує приміщення на 1 поверсі 10-поверхової будівлі. Будівля кирпична.

Ця будівля це жилий дім на 1-2 поверхах якого розташовані приміщення, що здаються під офіси комерційних підприємств. Аналогічно до представленої у роботі організації на вказаному поверсі орендуються 2 подібні по типу комплексу приміщення. Вид діяльності сусідніх на поверсі офісів - реклама та поліграфія. З 3 по 10 поверхи знаходяться квартири у яких проживають громадяни.

Фронтальна сторона будівлі, південна – виходить на майданчик де фотографують та обстежують автомобілі для їх оцінки, де і є вхід в офіс ПП, з іншої сторони майданчика в 35 метрах знаходиться офіс експертного товариства, яке також використовують цей майданчик в своїх цілях, та співпрацюють с ПП.

Інша сторона, північна виходить на проїжджу частину вулиці Маршала Малиновського, через 50 метрів від якої берег р. Дніпро, де розташований нічний клуб.

Зі східної сторони на відстані 70 метрів розташований великий торгівельний комплекс «Вавілон», площі якого здаються в оренду під офісні приміщення та магазини. Який оточений великою площею виділеною під автостоянку та ресторан.

В західній частині йде продовження висотного дома та двір який утворений с таких самих домів.

Поверх будівлі виділений під офісні приміщення має автономний генератор електроенергії. Усе обладнання, у тому числі розподільчі щити знаходяться на майданчику між поверхами.

На самому об'єкті інформаційної діяльності (виділенні всього 2 приміщення приміщення: кабінет директора, який в свою чергу є приймальною, та робоча кімната де знаходяться фахівці з оцінки та довідки-рахунку) постійно циркулює інформація, яка містить комерційну таємницю. Втрата цієї інформації передбачає суттєву загрозу для діяльності організації.

План об'єкту інформаційної діяльності ПП приведено у Додатку В до роботи.

2.1.1 Опис інформаційної системи підприємства

Основою інформаційної системи компанії є сервер баз даних, який підтримує роботу організації її ЛОМ. Операційна система на сервері - Windows Server 2016.

Сервер виконує функцію управління мережними потоками і функції резервування даних, а також обробки і видачі даних. Доступ в Інтернет

здійснюється через Інтернет-провайдера Фрегат шляхом високошвидкісного підключення.

2.2 Аналіз можливих загроз інформаційній

При створенні загальної моделі загроз були виділенні наступні потенційні загрози, здійснення яких може призвести до порушення цілісності, конфіденційності, доступності та спостерігає мості інформації, а також представляють загрозу функціонування підприємства. Вони наведені у таблиці 2.1

Таблиця 2.1 – Загальна модель інформаційних загроз

№ п/п	Загрози (позначення)	Тип та визначення загроз	Джерело	Конфіденційність	Цілісність	Доступність	Спостереженість
Загальні загрози техногенного походження							
1	Стихія	Пожежа, землетрус, ураган, повінь	Зовн. середовище		+	+	
2	Катастрофа	Вибух, аварія	Зовн. середовище		+	+	
Випадкові загрози техногенного походження							
3	ЭМВ	Зовнішні електромагнітні випромінювання	Апаратура		+	+	
4	М-поле	Вплив сильних магнітних полів на магнітні носії	Апаратура		+	+	
5	Відмова-Л	Відмова (повний вихід із ладу, систематичне неправильне виконання своїх функцій	Люди		+	+	+
6	Відмова -А	Відмови основної апаратури, систем передачі даних, носіїв інформації	Апаратура		+	+	
7	Відмова -П	Відмови програм	Програми		+	+	+

8	Відмова -О	Відмови системи живлення, систем забезпечення умов	Зовнішнє середовище, апаратура		+	+	
		роботи апаратури та персоналу					
9	Збій-А	Збої основної апаратури систем передачі даних	Апаратура			+	
10	Збій -О	Відмови системи живлення, систем забезпечення умов роботи апаратури та персоналу	Зовнішнє Середовище, апаратура		+	+	
11	Помилка-Л	Випадкові помилки користувача, обслуговуючого персоналу	Люди	+	+	+	+
12	Помилка-П	Помилки програм	Програми	+	+	+	+
13	Поламка-А	Поламка апаратури	Люди		+	+	
14	Поламка Н	Ушкодження носіїв інформації	Люди		+	+	
15	Вірус	Ураження програмного забезпечення комп'ютерними вірусами	Люди, програми		+	+	
Спеціальні загрози техногенного походження дистанційної дії							
16	Підключення	Підключення до каналів зв'язку через штатні, або спеціально розроблені апаратні засоби	Люди, апаратура, програми	+			
17	ПЕМІН	Отримання інф. по каналу ПЕМІ основних технічних пристроїв	Апаратура	+			
18	Е-Наводки	Отримання інформації по каналу наводок у системах каналізації, в тепломережах та ін.	Апаратура	+			
19	Віброакустика	Отримання інформації по віброакустичному каналу з використанням зерних пристроїв зняття інформації	Апаратура	+		-	

20	Е-імпульс	Отримання електромагнітних імпульсів з ціллю знищення інф., засобів її обробки та зберігання	Апаратура		+	+	
21	Прослуховування-Т	Прослуховування телефонних розмов	Апаратура, люди	+			
22	Оптика	Використання оптичних засобів, дистанційне фотографування	Апаратура	+			
23	НСД-ЛОМ	Несанкціонований доступ до ЛОМ	Апаратура, програми		+	+	+
24	Переадресація	Заміна маршруту передачі даних	Люди, програми	+		+	+
25	Нав'язування	Нав'язування хибної інф. під іменем авторизованого користувача	Люди, програми		+		+
Спеціальні загрози техногенного походження контактної дії							
26	Прослуховування	Прослуховування мережі завдяки програмних чи програмно-апаратних аналізаторів	Апаратура, програми	+			+
27	Читання-Е	Огляд даних, що виводяться на екрані	Люди, апаратура	+			
28	Читання-П	Огляд даних, що друкуються, читання документів, залишених без нагляду	Люди, апаратура	+			
29	Вимкнення-З	Вимкнення чи вивід із роботи підсистем забезпечення функціонування обчислювальних систем	Люди, апаратура, програми		+	+	
30	Пошкодження	Фізичне знищення системи, пошкодження усіх чи окремих найбільш важливих компонентів лом	Люди		+	+	

31	“Жучок”	Використання закладних дистанційних пристроїв	Люди, апаратура	+			
32	Опитування	Провокування на розмову осіб, які мають відношення до інформації з ОД та засобів АС її [обробки	Люди	+			+
33	Копіювання	Копіювання вихідних документів, магнітних носіїв та ін. носіїв інф.	Апаратура, програми, люди	+			
34	Пограбування	Крадіжка магнітних носіїв та документів, виробничих відходів	Люди	+	+		
35	Маскарад	Незаконна отримання паролів та інших реквізитів розмежування доступу	Люди, програми	+	+		
36	НСД-ПК	Несанкц. використання робочих станцій та терміналів ЛОМ	Люди, програми	+	+		+
37	НСД-У	Несанкц. використання техн. засобів	Люди, програми	+		+	+
38	Злом	Обхід механізмів захисту з ціллю забезпечити у подальшому доступ порушникові	Люди, програми		+		+
39	Перехват	Перехват паролів програмою-імітатором, перехват повідомлень	Люди, програми	+	+	+	+
40	Троянський кінь	Впровадження у програми програмних закладок типу «троянський кінь», «бомба» та ін.	Люди, програми		+	+	
41	Недоліки	Використання недоліків мов програмування операційних систем	Люди, програми	+	+		+
42	Підміна	Несанкц. підміна елементів програм,	Люди, програми	+	+	+	+

		елементів баз даних, апаратури, магнітних носіїв					
43	Вербовка	Вербовка персоналу чи окремих користувачів, які мають деякі повноваження	Люди	+	+		
44	Дезорганізація	Дії відносно дезорганізації функціонування системи (саботаж)	Люди, програми		+	+	

Висновки: найбільш небезпечними являються наступні загрози - несанкціонована підміна елементів програм, елементів баз даних, апаратури, магнітних носіїв, перехват паролів програмою-імітатором, перехват повідомлень, несанкціонований дистанційний доступ до ЛОМ, випадкові помилки користувача, обслуговуючого персоналу.

2.3 Побудова моделі порушника

Порушник - особа, яка цілеспрямовано зі злим помислом чи без нього, використовує різноманітні можливості, методи та засоби, зробила намагання зробити операції, які призвели чи можуть призвести до порушення цілісності та конфіденційності інформації, що захищається.

Модель порушника відображає його практичні та потенціальні можливості, апріорні знання, час та місце дії та ін. Порушники можуть бути класифіковані по категоріях, по мотивах порушення, по рівню кваліфікації, по показнику можливості використання засобів та методів подолання системи захисту, по часу та місцю дії.

Таблиці 2.2 - Специфікація моделі порушника по категорії порушників

Позначення	Визначення категорії
Внутрішні порушники	
Н 1	Безпосередньо користувачі чи оператори інформаційної системи, у тому числі керівники різних рівнів.
Н 2	Адміністратори обчислювальних мереж та інформаційної безпеки.
Н 3	Прикладні та системні програмісти.
Н 4	Співробітники служби безпеки.

Н 5	Технічний персонал по обслуговуванню будівель та обчислювальної техніки.
Н 6	Допоміжні та тимчасові працівники.
Зовнішні порушники	
Позначення	Визначення категорії
Н 7	Клієнти.
Н 8	Запрошені відвідувачі.
Н 9	Представники конкуруючих організацій.
Н 10	Співробітники спецслужб, особи, що діють по їх завданню.
Н 11	Хакери.
Н 12	Особи, що знаходяться за межами КЗ.

Таблиця 2.3 - Специфікація моделі порушника по мотивах порушення

Позначення	Мотив порушення
М 1	Безвідповідальність.
М 2	Самоствердження.
М 3	Корисливі інтереси.
М 4	Професійний обов'язок.
М 5	Помилки користувачів та адміністраторів.
М 6	«Боротьба з системою».
М 7	Недоліки використовуємих інформаційних технологій

Таблиця 2.4 - Специфікація моделі порушника по рівню кваліфікації

Позначення	Кваліфікаційний рівень
К 1	Знає функціональні особливості системи, основні закономірності формування масивних даних та потоків запитів до них, має навички користування штатними засобами автоматизованої інформації оціночного підприємства
К 2	Володіє високим рівнем знань та практичними навичками роботи з технічними засобами системи і їх обслуговування.
К 3	Володіє високим рівнем знань у сфері програмування та обчислювальної техніки, проектування та експлуатації інформаційної АС.
К 4	Знає структуру, функції та механізми дії захисту інформації у ПП та їх недоліки.
К 5	Знає недоліки та вразливості механізмів захисту, які вбудовані в системне програмне забезпечення та його не документовані можливості.
К 6	Є розробником програмних чи програмно-апаратних засобів захисту чи системного програмного забезпечення.

Таблиця 2.5 - Специфікація моделі порушника по показнику можливості використання засобів та методів подолання системи захисту

Позначення	Характеристика можливості порушника
СМ 1	Використовує агентурні методі отримання відомостей.
СМ2	Використовує пасивні засоби (технічні засобі перехвату без модифікації компонентів системи.)
СМ3	Використовує штатні засоби та недоліки системи захисту для її подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні магнітні носії, які можуть бути непомітно пронесені.
СМ 4	Використовують методи та заходи дистанційної (з використанням штатних каналів та протоколів зв'язку) програмної закладки та спеціальних резидентських програм збору, пересилки та блокування даних, дезорганізація систем обробки інформації у АС.
СМ 5	Використає методи та засоби активного впливу (модифікація та підключення додаткових технічних засобів, підключення до каналів передачі даних)

Таблиця 2.6 - Специфікація моделі порушника по часу дії

Позначення	Час дії
В 1	До впровадження АС чи її окремих компонентів.
В 2	У час бездіяльності компонентів системи (у неробочий час).
В 3	В час функціонування АС чи її компонентів.
В 4	Як у процесі функціонування АС, так і в час припинення функціонування компонентів системи.

Таблиця 2.7 - Специфікація моделі порушника по місцю дії

Позначення	Характеристика місця дії
МД1	Без доступу на територію КЗ
МД2	З доступом на територію КЗ
МД3	З робочого місця користувача ПП.
МД4	Безпосередній фізичний контакт з обчислювальною технікою (доступ до серверу, до систем адміністрування, до програм керування системи забезпечення інформаційної безпеки)

На основі аналізу можливих загроз та порушників згідно специфікаціям, наведеним у таблицях, була побудована модель порушника

Таблиця 2.8 - Модель порушника

Порушник	Мотив порушення	Рівень кваліфікації	Можливості порушника	Місце дії	Час дії	Рівень загрози
Н 1	М 1, М3	К 1	СМ3	МД1, МД3	В 4	2
Н 2	М 1, М3, М5	К 2, К3, К4, К5	СМ3	МД 2, МД3, МД4	В 1, В 4	3
Н 3	М 1, М3, М6	К 1, К 2, К3	СМ 3, СМ 4	МД2, МД3	В 1, В4	4
Н 4	М 3, М 6	К 4, К 5	СМ 1, СМ 2, СМ3	МД2, МД3, МД4	В 1, В 4	4
Н 5	М 1, М3	К О	СМ 1, СМ 2, СМ3	МД 1, МД3	В 1, В4	1
Н 6	М 1, М3	КО, К 1	СМ 1, СМ 2, СМ3	МД 1, МД3	В 4	1
Н 7	М 1, М3	К О	СМ 1, СМ 2	МД 1	В 4	2
Н 8	М 3	К О	СМ 1, СМ 2	МД 1	В 4	2
Н 9	М 3	К 1, К 2, К3, К 4	СМ 1, СМ 2	МД 1	В 1, В 4	5
Н 10	М 4	К 3	СМ 1, СМ 2, СМ3, СМ 4, СМ 5	МД 1	В 1, В 4	5
Н 11	М2, М3, М5, М 7	К 1, К3	СМ 1, СМ 2, СМ3, СМ 4, СМ 5	МД1	В 1, В4	4
Н 12	М 1, М3	КО, К3	СМ 1, СМ 4, СМ 5	МД1	В 1, В4	1

2.4 Визначення функціонального профілю захищеності

Основні загрози для комерційної таємниці - це перш за все загрози, що пов'язані з підробкою, відмовою від отримання та порушенням технологічної

роботи, а у другу - порушення доступності та конфіденційності. У зв'язку з цим до ПБ, які входять до складу підприємницької АС, пред'являються вимоги до забезпечення захисту від указаних загроз. Окрім цього, вимоги суттєво залежать від того, чи робиться обробка у реальному часі чи відкладена обробка. Необхідно врахувати, що ІТС ПП відноситься до класу 3, тобто являється розгалуженою. В указаній АС рекомендується використовувати ПБ, яка реалізує профіль З.КЦД.2.

З.КЦД.2 = { КД-2, КА-2, КО-1, КВ-2, ЦД-1,ЦА-2, ЦО-1,ЦВ-2, ДР-1,ДВ-1,НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ- 1 }

КД – довірлива конфіденційність;

КА – адміністративна конфіденційність;

КО – повторне використання об'єктів;

КВ – конфіденційність при обміні;

ЦД – довірлива цілісність;

ЦА– адміністративна цілісність;

ЦО – відкат;

ЦВ – цілісність при обміні;

ДР – використання ресурсів;

ДВ – відновлення після збоїв;

НР – реєстрація;

НІ – ідентифікація та аутентифікація;

НК – достовірний канал;

НО – розгалуження обов'язків;

НЦ – цілісність КСЗ;

НТ – самотестування;

НВ – аутентифікація при обміні;

НП – аутентифікація отримувача.

2.5 Політика безпеки

Необхідність розробленої політики безпеки, на сьогоднішній день є очевидним фактом для будь якої, навіть достатньо невеликої компанії. Політика безпеки в цілому – це сукупність програмних, апаратних, організаційних, адміністративних, юридичних, фізичних мір, засобів і правил та інструкцій, чітко регламентуючих всі аспекти діяльності компанії, що містить інформаційну систему, та ті, що забезпечують її безпеку.

Окрім свого прямого призначення, розробка політики безпеки дає і непередбачуваний на перший погляд, побічний ефект: у результаті аналізу інформаційних потоків, інвентаризації інформаційних ресурсів та детермінації обробляємої інформації по ступеню цінності, керівництво організації отримує цілісну картину одного з самих складних об'єктів керівництва - інформаційної системи. Що позитивно впливає на якість керування бізнесом у цілому, і як наслідок, покращує його прибутковість та ефективність.

2.5.1 Захист від шкідливого програмного забезпечення (вірусів, «троянських коней»)

Для захисту від шкідливого програмного забезпечення повинні бути прийняті наступні заходи:

- Зобов'язаність використання тільки ліцензійного програмного забезпечення та заборона використання незатвердженого програмного забезпечення повинні бути закріплені документально;
- З метою зниження ризиків, зв'язаних з отриманням програмного забезпечення крізь мережі загального використання чи на носіях, цей процес повинний бути формалізований у вигляді відповідного документу;
- Всі системи повинні бути обладнані антивірусним програмним забезпеченням, яке повинно своєчасно оновлюватись. Сканування всіх систем повинно проводитися регулярно;

- Цілісність програмного забезпечення, що займається обробкою критичних даних (та самих даних) повинна регулярно перевірятися. Сканування всіх систем повинно проводитися регулярно;

- Всі точки, через які в систему поступає інформація у вигляді файлів, повідомлень та ін., повинні забезпечувати антивірусний контроль вхідної інформації;

- В організації повинний бути розроблений та задокументований механізм відновлення після вірусних атак, а саме, визначені процедури резервного копіювання програмного забезпечення та даних, моніторинг всієї інформації, що стосується шкідливого програмного забезпечення.

2.5.2 Розгалуження прав та аутентифікація користувачів

Для забезпечення розгалуження прав та строгої аутентифікації користувачів система захисту інформації ПП включає в себе механізми формування/перевірки електронно-цифрового підпису на базі несиметричного алгоритму RSA. Для забезпечення роботи цього алгоритму ПП має персональний генератор ключів з інтегрованим ідентифікатором підприємства

2.5.3 Способи боротьби за несанкціонованим доступом:

1 Періодично змінювати реквізити доступу. Робити це при будь-яких підозрах втрати конфіденційності та після доступу до комп'ютеру інших користувачів.

2 Ввести контроль над використанням логіну/паролю в рамках організації, який буде представляти собою політику використовування паролів на заданому об'єкті інформаційної діяльності.

3 Негайно ставити до уваги свого провайдеру щодо можливої втрати інформації.

4 Контроль над використанням часу при допомозі білінгової системи, або системи контролю за інтернет-трафіком.

5 Зберігати паперові, магнітні чи оптичні носії, що містять реквізити у недоступних для по сторонніх місцях.

6 Обов'язково встановлювати та використовувати на своєму комп'ютері антивірусні програми, при цьому обов'язковою умовою для надійності захисту є контроль над регулярним оновленням антивірусних баз.

У випадку несанкціонованого доступу до комерційної інформації, відповідальність, як правило, визначається згодою с провайдером. Відповідальність абоненту за доступ до такого типу інформації така ж, як у випадку крадіжки облікового запису для підключення.

2.5.4 Політика безпеки антивірусного захисту

Мета - встановити вимоги, яким повинні відповідати всі комп'ютери, підключені до мережі організації, для гарантії їх захисту від ураження вірусами.

Основні положення:

1 Всі комп'ютери даного закладу повинні мати стандартне, рекомендоване до використання у організації антивірусне програмне забезпечення. Антивірусне програмне забезпечення повинно мати найсвіжішу базу оновлень. Комп'ютери, уражені вірусом, потрібно терміново видаляти с мережі до тих пір, поки вони не будуть вилікувані.

2 Співробітники відповідальні за створення процедур, гарантуючих, що антивірусне програмне забезпечення виконує періодичну перевірку комп'ютерів та має найсвіжіші бази оновлень. Заборонена, у відповідності до політики допустимого використання, будь-яка діяльність по створенню/розповсюджуванню вірусів, «черв'яків», поштових «бомб», програм типу «Троянський кінь».

3 Ніколи не відкривати файли та не виконувати макроси, отриманні у поштових повідомленнях від невідомого чи підозрілого адресату.

4 Видаляти підозрілі вкладення, не відкриваючи їх, та очищати корзину, де зберігаються видаленні повідомлення.

5 Видаляти спам, рекламу та інші некорисні повідомлення, як описано у політиці допустимого використання.

6 Ніколи не завантажувати файли та програмне забезпечення із підозрілих та невідомих джерел.

7 Не допускати віддавання дисків у сумісне використання на читання/запис, якщо це не абсолютно необхідно.

8 Завжди перевіряти оптичні та жорсткі змінні носії на наявність вірусів.

9 Періодично резервувати важливі дані та системну конфігурацію.

10 Зберігати резервні копії у надійному місці.

11 Якщо при тестуванні трапляється конфлікт з антивірусним програмним забезпеченням, то його можна вимкнути, провести тестування та одразу ж включити знов. При відключеному антивірусному програмному забезпеченні не виконувати жодних програмних аплікацій, які можуть привезти до розповсюджуванню вірусу (наприклад, поштові програми).

12 Періодично перевіряти політику на наявність оновлень.

Кожен працівник підписує згоду про те, що прочитав цей документ та зобов'язаний слідувати його положенням.

У випадку порушення положення даного документу працівник несе адміністративну та матеріальну відповідальність.

Даний документ потрібно переглянуті через 6 місяців після вступу його до сили

2.5.6 Політика безпеки використання електронної пошти

Мета - забезпечити максимальну зручність співпрацівників при роботі з електронною поштою. При цьому знизити ризик витоку інформації завдяки електронній пошти.

Дана політика безпеки діє на всій території даного підприємства, обмежуючись лише межами території об'єкту інформаційної діяльності.

Дана політика безпеки затверджена керівником оціночного підприємства управляючим інформаційною безпекою.

Основні положення:

1 Використання електронної пошти дозволено лише у робочий час.

2 Забороняється використовувати електронну пошту для приватних цілей.

3 При завершенні роботи на робочій станції обов'язково вимикати поштовий клієнт.

4 Забороняється розголошувати свій пароль до електронної поштової скриньки співпрацівникам, стороннім особам.

5 Забороняється залишати свій пароль до електронної поштової скриньки, записаний на паперовому носії, на своєму робочому місці.

6 Рекомендується терміново повідомляти системного адміністратора чи управляючого інформаційною безпекою про всі негаразди, проблеми та порушення у роботі поштового клієнта.

7 Забороняється видаляти повідомлення із папок «Надіслані», «Відіслані» та «Корзина», якщо вони не підлягають під визначення спаму, або реклами.

8 Забороняється саджати на своє робоче місце сторонніх осіб, надавати їм доступ до електронної пошти.

9 Забороняється здійснювати доступ до електронної скриньки за допомогою web-інтерфейсу, або стороннього поштового клієнту.

Кожен працівник підписує згоду про те, що прочитав цей документ та зобов'язаний слідувати його положенням.

Виключення:

Якщо того вимагають обставини, дозволяється надавати доступ до своєї робочої станції сторонній особі, перед цим поставив до уваги управляючого інформаційною безпекою та отримав його на це згоду.

У випадку порушення положення даного документу працівник несе адміністративну та матеріальну відповідальність.

Даний документ потрібно переглянуті через 6 місяців після вступу його до сили.

2.5.7 Політика безпеки робочих станцій

Мета - створити робочі станції максимально захищеними, при цьому забезпечивши комфортну роботу на них для працівників компанії.

Дана політика безпеки діє на всій території даного підприємства, обмежуючись лише межами території об'єкту інформаційної діяльності.

Дана політика безпеки затверджена керівником оціночного підприємства, управляючим інформаційною безпекою.

Основні положення:

1 Особистий пароль працівника для входу до системи не повинен передаватися другим особам.

2 Забороняється залишати паролі та іншу інформацію з обмеженим доступом, написану на паперовому носії, на своїх робочих місцях.

3 Забороняється використовувати комп'ютери, локальну мережу, а також мережу Internet для особистих цілей, що не стосуються роботи.

4 Забороняється саджати на своє робоче місце сторонніх осіб, надавати їм доступ до робочого комп'ютера.

5 Перед покиданням свого робочого місця необхідно переконатися у завершенні сеансу роботи на своєму комп'ютері.

6 Не рекомендується встановлювати програмне забезпечення на робочу станцію, не проконсультувавшись з системним адміністратором чи управляючим інформаційною безпекою.

7 Рекомендується терміново повідомлю вати системного адміністратора чи адміністратора по безпеці про всі негаразди, проблемі та порушення у роботі робочих станцій.

Кожен працівник підписує згоду про те, що прочитав цей документ та зобов'язаний слідувати його положенням.

Виключення:

Якщо того вимагають обставини, дозволяється надавати доступ до своєї робочої станції сторонній особі, перед цим поставив до уваги управляючого

інформаційною безпекою та отримав його на це згоду.

У випадку порушення положення даного документу працівник несе адміністративну та матеріальну відповідальність.

Даний документ потрібно переглянуті через 6 місяців після вступу його до сили.

2.6 Інструкція с організації парольного захисту АС

Дана інструкція регламентує організаційно-технічне забезпечення процесів генерації, зміни та закінчення дії паролів (видалення облікових записів користувачів) у автоматизованій системі оціночного підприємства (а саме у автоматизованій системі даного об'єкту інформаційної діяльності), а також контроль за діяльністю користувачів та обслуговуванню персоналу системи при роботі з паролями.

Організаційне та технічне забезпечення процесів генерації, використання, зміни дії паролів у всіх підсистемах автоматизованої системи ПП та контроль за діями виконавців і обслуговуючого персоналу системи при роботі з паролями покладається на відповідальних за інформаційну безпеку, що впроваджують адміністративні заходи по захисту, що містять механізми ідентифікації та аутентифікації (підтвердження оригінальності) користувачів зі значеннями паролів.

Особисті паролі повинні генеруватися та розподілятися централізовано, або вибиратися користувачами автоматизованої системи самостійно за умов відповідності до наступних вимог:

- довжина паролю повинна бути не менше 8 символів;
- у числі символів паролю обов'язково повинні бути присутні букви у
- верхньому та нижньому регістрах, цифри та спеціальні символи (@, #, $, %, * та ін.);
- пароль не повинен включати у себе символи, що легко обчислюються
- (імена, прізвища та ін.), а також загальновживані скорочення (USER, COMP та ін.);

- при зміні паролю нові значення повинні відрізнятися від попередніх не менше, ніж в 6 позиціях;
- особистий пароль користувач не має права розголошувати нікому.

Власники паролів повинні бути ознайомлені з перерахованими вище вимогами та попереджені про відповідальність за використання паролів, не відповідаючи даним вимогам, а також за розголошення парольної інформації.

У випадку, якщо формування особистих паролів користувачів здійснюється централізовано, відповідальність за правильність їх формування та розподіл надається на уповноваженого співпрацівника служби забезпечення захисту інформації (у даному випадку управляючого інформаційною безпекою). Для генерації «стійких» значень паролів можуть бути використані спеціальні програмні засоби. Система централізованої генерації та розподілу паролів повинна виключати можливість ознайомлення самих уповноважених співпрацівників служби забезпечення захисту інформації, а також відповідальних за інформаційну безпеку ПП.

При наявності у випадку появи нештатних ситуацій, форс-мажорних обставин і т.і. технологічної необхідності у використанні імен та паролів деяких співробітників (виконавців) у їх відсутність, такі співпрацівники зобов'язані одразу ж змінити свої паролі, та при необхідності імена облікових записів, у відповідності з правилами генерації паролів.

1 Повна планова зміна паролів користувачів повинна проводитися регулярно, не менше одного разу на три місяці.

2 Позапланова зміна особистого паролю, або видалення облікового запису користувача автоматизованої системи у випадку завершення його повноважень (звільнення, перехід на інше місце роботи та ін.) повинна проводитися уповноваженим співпрацівником служби захисту інформації - адміністраторами відповідних засобів захисту терміново після закінчення останнього сеансу роботи даного користувача з системою.

3 Позапланова повна зміна паролів всіх користувачів повинна

проводитися у випадку завершення повноважень (звільнення, перехід на інше місце роботи та ін.) адміністраторів засобів захисту та інших співпрацівників, яким по роду діяльності були надані повноваження по управлінню парольним захистом підсистем автоматизованої системи.

4 У випадку компрометації особистого паролю користувача автоматизованої системи повинні бути терміново прийняті міри у відповідності до пунктів 6 або 7 даної Інструкції у залежності від повноважень володаря скомпрометованого паролю.

5 Зберігання співпрацівником (виконавцем) значень своїх паролів на паперовому носії не допускається.

6 Повсякденний контроль за діями виконавців та обслуговуючого персоналу системи при роботі з паролями, дотриманням порядку їх зміни, зберігання та використання доручаться на відповідальних за інформаційну безпеку ПП.

2.7 Інструкція з організації антивірусного захисту

Дана інструкція визначає вимоги до організації захисту автоматизованої системи оціночної компанії від руйнівного впливу комп'ютерних вірусів та встановлює відповідальність керівників та співробітників, експлуатуючих та супроводжуючих автоматизовану систему ПП, за їх виконання.

До використання в ПП допускається лише ліцензійні антивірусні засоби, централізовано куплені у постачальників вказаних засобів, та рекомендовані до застосування управляючим інформаційною безпекою організації.

У випадку необхідності використання антивірусних заходів, що не увійшли до переліку рекомендованих, їх застосування необхідно узгодити с управляючим інформаційною безпекою ПП.

Установка засобів антивірусного контролю на робочих станціях та сервері виконується уповноваженими співробітниками. Настройка параметрів засобів антивірусного контролю проводиться співробітниками служби забезпечення

інформаційної безпеки у відповідності з керівництвом по використанню конкретних антивірусних засобів.

Застосування засобів антивірусного контролю

Кожен день на початку роботи при загрузці комп'ютеру (для серверів - при перезапуску) у автоматичному режимі повинен проводитися антивірусний контроль для всіх дисків та файлів робочих станцій.

Обов'язковому антивірусному контролю підлягають будь-яка інформація (текстові файли любих форматів, виконуючі файли, файли даних), що отримується та передається по телекомунікаційним каналам, а також інформація на змінних носіях (оптичних дисках, жорстких змінних накопичувачах).

Файли, що потрапляють до електронного архіву повинні бути обов'язково про скановані на предмет вірусних підписів, тобто проходити попередній антивірусний контроль. Періодичні перевірки електронних архівів повинні проводитися не менше, ніж один раз на три місяці.

Встановлюване (змінюєме) програмне забезпечення повинно бути попередньо перевірено на відсутність вірусів. Безпосередньо після встановлення (змін) програмного забезпечення комп'ютера (локальної обчислювальної мережі), повинна бути виконана антивірусна перевірка:

- на серверах та персональних комп'ютерах, що захищаються - відповідальними за забезпечення інформаційної безпеки.
- на інших серверах та персональних комп'ютерах ПП не потребуючих захисту, - персоною, що встановила програмне забезпечення, - в присутності та під контролем керівника даного підрозділу чи співробітника, їм уповноваженого.

Факт виконання антивірусної перевірки після установки програмного забезпечення повинен реєструватися у спеціальному журналі за підписом особи, що встановила програмне забезпечення та особи, що його контролювала.

При виникненні підозри на наявність комп'ютерного вірусу (нетипова робота програм, поява графічних та звукових ефектів, зміна даних, зникнення файлів, системні помилки та ін.) співробітник самостійно чи разом з

відповідальним за забезпечення безпеки інформації повинний провести позачерговий антивірусний контроль власної робочої станції. При необхідності залучити спеціалістів по захисту інформації даної організації для встановлення ними факту наявності комп'ютерного вірусу.

У випадку знаходження при проведенні антивірусної перевірки уражених комп'ютерними вірусами файлів співробітники зобов'язані:

- припинити роботу;
- негайно поставити до уваги про факт знаходження уражених вірусом файлів керівника та відповідального за забезпечення інформаційної безпеки, власника уражених файлів, а також всіх співробітників, що використовують ці файли у роботі;
- разом із власником уражених файлів провести аналіз необхідності їх подальшого використання;
- провести лікування чи знищення уражених файлів;
- у випадку знайдення нового вірусу, що не піддається лікуванню засобами, що застосовуються, направити уражений вірусом файл до організації, з якою складено угоду про антивірусну підтримку;
- по факту знайдення заражених вірусом файлів створити службову записку, в якій необхідно вказати можливе джерело (відправника, володаря та ін.) ураженого файлу, тип ураженого файлу, характер інформації, що знаходиться у файлі, тип вірусу та виконання антивірусного заходу.

Відповідальність

Відповідальність за організацію антивірусного контролю у відділах, що експлуатують автоматизовану систему ПП, у відповідності до вимог даної Інструкції полягає на керівника підприємства.

Відповідальність за проведення заходів антивірусного контролю підрозділу та дотримання вимог даної Інструкції полягає на відповідального за забезпечення захисту інформації та всіх співробітників, які являються користувачами автоматизованої системи ПП.

Періодичний контроль за станом антивірусного захисту у автоматизованій системі ПП, а також за дотриманням встановленого порядку антивірусного контролю та виконанням вимог даної Інструкції співробітниками відділів ПП виконується управляючим інформаційною безпекою.

2.8 Інструкція по розподілу обов'язків працівників

Керівник підприємства відповідальний за доведення положень політики безпеки до користувачів і за контакти з ними.

Системний адміністратор забезпечує безперервне функціонування мережі і відповідає за реалізацію технічних мір, необхідних для проведення в життя політики безпеки.

Користувачі зобов'язані працювати з локальною мережею відповідно де політики безпеки, підкорятися розпорядженням осіб, що відповідають за окремі аспекти безпеки, повідомляти керівництво про всі підозрілі ситуації.

Керівник підприємства зобов'язаний:

1 Постійно тримати в полі зору питання безпеки. Стежити за тим, щоб те ж робили його підлеглі.

2 Проводити аналіз ризиків, виявляючи активи, що вимагають захисту, і вразливі місця систем, оцінюючи розмір можливого збитку від порушення режиму безпеки і вибираючи ефективні засоби захисту.

3 Організувати навчання персоналу заходам безпеки. Звернути особливу увагу на питання, пов'язані з антивірусним контролем.

4 Інформувати адміністраторів локальної мережі про зміну статусу кожного з підлеглих (перехід на іншу роботу, звільнення і тому подібне).

5 Зробити, щоб кожен комп'ютер в підрозділах мав господаря або системного адміністратора, що відповідає за безпеку і має достатню кваліфікацію для виконання цієї ролі.

6 Системний адміністратор зобов'язаний:

7 Інформувати керівництво про ефективність існуючої політики

безпеки і про технічні заходи, які можуть поліпшити захист.

8 Забезпечити захист устаткування локальної мережі, зокрема інтерфейсів ; іншими мережами.

9 Оперативно і ефективно реагувати на події, що таять загрозу. Надавати допомогу у віддзеркаленні загрози, виявленні порушників і наданні інформації для їх покарання.

10 Використовувати перевірені засоби аудиту і виявлення підозрілих ситуацій.

11 Щодня аналізувати реєстраційну інформацію, що відноситься до мережі в цілому і до файлових серверів особливо.

12 Стежити за новинками в області інформаційної безпеки, повідомляти про них користувачам і керівництву.

13 Не зловживати даними ним повноваженнями. Користувачі мають право на таємницю.

14 Розробити процедури і підготувати інструкції для захисту локальної мережі від шкідливого програмного забезпечення. Надавати допомогу у виявленні і ліквідації шкідливого коду.

15 Регулярно виконувати резервне копіювання інформації, що зберігається на файлових серверах.

16 Виконувати всі зміни в мережній апаратно-програмній конфігурації.

17 Гарантувати обов'язковість процедури ідентифікації і аутентифікації для доступу до мережевих ресурсів.

18 Виділяти користувачам вхідні імена і початкові паролі тільки після заповнення реєстраційних форм.

19 Періодично здійснювати перевірку надійності захисту локальної мережі. Не допускати отримання привілеїв неавторизованими користувачами.

Користувачі мережі зобов'язані:

1 Знати і виконувати закони, правила, політику безпеки, процедури безпеки.

2 Використовувати доступні захисні механізми для забезпечення конфіденційності і цілісності своєї інформації.

3 Використовувати механізм захисту файлів і належним чином задавати права доступу.

4 Правильно вибирати паролі, регулярно міняти їх. Не записувати паролі на папері, не повідомляти їх іншим особам.

5 Допомагати іншим користувачам дотримувати заходи безпеки. Указувати їм на упущення.

6 Інформувати адміністраторів або керівництво про порушення безпеки та інших підозрілих ситуаціях.

7 Не використовувати слабкості в захисті сервісів і локальної мережі в цілому.

8 Не здійснювати неавторизованої роботи з даними, не створювати перешкод іншим користувачам.

9 Не намагатися працювати від імені інших користувачів. Забезпечувати резервне копіювання інформації з жорсткого диска свого комп'ютера.

10 Знати принципи роботи шкідливого програмного забезпечення, шляхи його проникнення і розповсюдження, слабкості, які при цьому можуть бути використані.

11 Знати і виконувати процедури для попередження проникнення шкідливого коду, для його виявлення і знищення.

12 Знати слабкості, які використовуються для неавторизованого доступу, а також способи виявлення нештатної поведінки конкретних систем, послідовність подальших дій, точки контакту з відповідальними особами.

13 Дотримуватись правил поведінки в екстрених ситуаціях, послідовність дій при ліквідації наслідків аварій.

2.9 Інструкція по забезпеченню працездатності ЛОМ

План:

1 Введення основних понять

2 Загальний порядок роботи мережі

3 Порядок парольного захисту

4 Порядок роботи з обліковими записами

5 Порядок роботи з документами

Введення основних понять

- Апаратні засоби - це матеріальні об'єкти, що використовуються в техніці.
- Програмні засоби - це програми, а також засоби екранного і печатного представлення - інтерфейс. Це нематеріальні об'єкти.
- Технічні засоби включають апаратні і програмні засоби. У даном> документі і документах, що додаються, розглядаються тільки засоби, ще відносяться до комп'ютерів і мережі.
- Фізичними пристроями можуть бути тільки апаратні засоби.
- Логічними пристроями є програмні засоби, що ототожнюються з відповідними фізичними пристроями.
- Ресурсами є логічні пристрої і інші структури представлення даних для користувача.
- Мережевими ресурсами є ресурси доступні через мережу.
- Локальними ресурсами є ресурси доступні безпосередньо на даному комп'ютері.
- Захист інформації має на увазі захист з погляду несанкціонованого доступу і захист від випадкових збоїв.

Там де мова йде про групи, мається на увазі група користувачів, що спільно працює над якими-небудь документами. Така група може бути цілим відділом або підрозділом, або включати співробітників різних відділів і підрозділів.

Ціль даного документа.

Технічні засоби можуть надавати різний рівень захисту від несанкціонованого доступу і випадкових збоїв, а так само володіти різними можливостями. Завдання регламентуюче роботу з технічними засобами - це встановлення правил, що забезпечують ефективність роботи, необхідну безпеку і захист інформації з урахуванням цих фактів.

Загальний порядок роботи мережі

Системний адміністратор встановлює правила роботи з інформацією, технічними засобами і правила використання ресурсів згідно можливостей, функцій, призначенню і ступеню захищеності цих засобів, ресурсів і вимогам до захисту і доступності інформації, з якою проводяться роботи.

Системний адміністратор визначає і запроваджує технічні засоби і ресурси, призначені для роботи з інформацією відповідно до вимог, захисту і доступності цієї інформації, встановлюваними керівництвом.

Користувачі підкоряються правилам, що встановлюються системним адміністратором. Користувачі відповідальні за недотримання правил і як наслідок втрату і псування інформації, а також розповсюдження її за межі, що встановлюються вимогами до захисту.

Правила роботи з обліковими записами:

1 Користувачам заводяться, відключаються облікові записи і привласнюються відповідні права по розпорядженню директора.

2 Облікові записи підлеглих можуть бути заблоковані на час відпустки.

3 Обліковий запис підлеглого може бути тимчасово заблокований.

4 Адміністратор зобов'язаний записувати в журнал операції закладу, блокування, видалення облікових записів користувачів і груп.

Порядок роботи з документами

Якщо документ необхідний декільком користувачам, він може бути поміщений в папку для групової роботи. Помістити документ в існуючу папку

користувач може самостійно, а для створення нових групових папок слід звернутися до адміністратора мережі.

Поміщаючи документ в загальну папку, користувач надає доступ до нього для всіх користувачів, що мають доступ до даної папки. Відправляючи документ по електронній пошті, користувач надає доступ до документа тому одержувачеві, якому він його відправляє. Користувач, що відкрив доступ до будь-якого документу несе відповідальність за його можливе небажане відкриття.

2.10 Висновки

В спеціальній частині роботи була проаналізована інформаційна система оціночного підприємства, проаналізовані можливі загрози інформаційній безпеці, побудовано модель порушника та визначено функціональний профіль захищеності. Проаналізувавши отримані результати було запропоновано у якості рекомендацій до побудови системи управління інформаційною безпекою- впровадження політики безпеки антивірусного захисту, політики безпеки використання електронної пошти та політики безпеки робочих станцій. Запропоновано, як обов'язкові стандартні вимоги для всіх типових оціночних підприємств інструкції з організації парольного захисту, антивірусного захисту, по розподілу обов'язків працівників та інструкції по забезпеченню працездатності локально обчислюваної мережі.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

Розробка системи управління інформаційною безпекою приватного підприємства з оцінки майна передбачає розробку комплексу заходів із забезпечення інформаційної безпеки, які дозволять досягти необхідного рівня захисту конфіденційної інформації за допустимих витрат і заданого рівня обмежень видів інформаційної діяльності для запобігання витоку або порушення конфіденційності, цілісності й доступності інформації, яка циркулює в ІТС. Тому метою економічного розділу є обґрунтування економічної доцільності розробки системи управління інформаційною безпекою приватного підприємства з оцінки майна. Для цього необхідно здійснити визначення капітальних витрат на придбання і налагодження складових системи інформаційної безпеки або витрат, що пов'язані з виготовленням апаратури, приладів, програмного забезпечення; річних експлуатаційних витрат на утримання і обслуговування об'єкта проектування; річного економічного ефекту від впровадження запропонованих заходів; показників економічної ефективності впровадження системи захисту на підприємстві.

3.1 Розрахунок (фіксованих) капітальних витрат

Фіксованими витрати називаються тому, що робляться, як правило, один раз, на початкових етапах створення ІС. До фіксованих належать наступні витрати: вартість розробки і впровадження проекту; залучення зовнішніх консультантів; первинні закупівлі основного ПЗ; первинні закупівлі додаткового ПЗ; первинні закупівлі апаратного забезпечення тощо.

Витрати на забезпечення конфіденційності при передачі інформації з використанням широкосмугових хаотичних сигналів визначаються, виходячи з трудомісткості кожної операції, та належать до капітальних витрат.

Визначення трудомісткості розробки системи управління інформаційною безпекою

Трудомісткість розробки системи управління інформаційною безпекою на підприємстві визначається тривалістю кожної робочої операції, до яких належать наступні:

– тривалість складання технічного завдання на розробку засобів підвищення рівня інформаційної безпеки, $t_{тз}$=12 годин;

– аналіз можливих загроз безпеки інформації, $t_{аз}$=20 годин;

– аналіз нормативних документів у сфері інформаційної безпеки, $t_{нд}$=10 години;

– обрання функціонального профілю захищеності і класу АС, $t_{пз}$=16 годин;

– розробка системи захисту від несанкціонованого доступу, $t_{знд}$=14 годин;

– створення домену на основі ОС Windows Server, $t_{знд}$=4 години;

– розробка правила доступу до інформації, $t_{рпд}$=15 годин;

– аналіз існуючих програм розмежування доступу, $t_{апрд}$=8 годин;

– розробка підсистеми розмежування доступу, $t_{рпрд}$=4 годин;

– налаштування існуючих на підприємстві засобів захисту інформації $t_{нзз}$=12 годин;

– впровадження розроблених засобів та заходів, $t_{врз}$=8 години;

– проведення випробування і аналіз отриманих результатів, $t_{вар}$=6 години;

– підготування технічної документації для впровадження, $t_{техд}$=4 години;

– оформлення і затвердження акту про передачу на впровадження, $t_{оа}$=2 години.

Отже,

$$t = t_{тз}+ t_{аз}+ t_{нд}+ t_{пз}+ t_{знд}+ t_{знд}+ t_{рпд} +t_{апрд}+ t_{рпрд}+ t_{нзз}+ t_{врз}+ t_{вар}+ t_{техд}+ t_{оа}=$$

$$= 12+20+10+16+14+4+15+8+6+4+12+8+6+4+2= 141 \text{ години.}$$

Розрахунок витрат на розробку системи захисту інформації на підприємстві

Витрати на розробку системи захисту інформації на підприємстві *Крп* складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки *Ззп* і вартості витрат машинного часу, що необхідний для розробки політики безпеки інформації *Змч*.

$$К_{рп} = З_{зп} + З_{мч}\ .$$

$$К_{рп} = З_{зп} + З_{мч} = 22842 + 723{,}33 = 23565{,}33 \text{ грн.}$$

$$З_{зп} = t\ З_{пр} = 141*162 = 22842 \text{ грн.}$$

де t – загальна тривалість розробки політики безпеки, годин;

Зіб – средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину.

Вартість машинного часу для розробки політики безпеки інформації на ПК визначається за формулою:

$$З_{мч} = t*С_{мч} = 141*5{,}13 = 723{,}33 \text{ грн.}$$

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

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

Вартість 1 години машинного часу ПК визначається за формулою:

$$См ч = 0{,}7 \cdot 2 \cdot 1{,}68 + \frac{7100 \cdot 0{,}5}{1920} + \frac{8900 \cdot 0{,}2}{1920} = 5{,}13 \text{ грн.}$$

Основою інформаційної системи компанії є сервер баз даних, який підтримує роботу організації її ЛОМ. Операційна система на сервері – Windows Server 2016.

Захист від можливого витоку інформації за рахунок НСД в ІТС підприємства та забезпечення зазначеного рівня послуг безпеки здійснюється за рахунок функціональних можливостей та сервісів безпеки сертифікованої в контексті національних нормативних документів системи технічного захисту інформації ОС Windows 7, яка вже впроваджена на підприємстві. Також з метою реалізації системи захисту інформації в ІТС підприємства та забезпечення заданих технічних показників, згідно основним критеріям до вибору засобів захисту використано функціональні можливості ОС Windows Server 2016, які вже впроваджений на підприємства.

Таким чином, витрати у зв'язку з придбанням апаратного забезпечення не виникають.

Витрати на навчання технічних фахівців і обслуговуючого персоналу складуть 8000 грн.

Витрати на встановлення обладнання та налагодження системи інформаційної безпеки складуть 12000 грн.

Таким чином, капітальні (фіксовані) витрати на розробку засобів підвищення рівня інформаційної безпеки складуть:

$$К = К_{рп} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н} =$$
$$= 23565,33+8000+12000 = 43565,33 \text{ грн.}$$

де $К_{рп}$ – вартість розробки політики інформаційної безпеки та залучення для цього зовнішніх консультантів, тис. грн;

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), тис. грн;

$К_{пз}$ – вартість створення основного й додаткового програмного забезпечення, тис. грн;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу,

$К_н$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки.

3.1.1 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_в + С_к + С_{ак}, \quad грн.$$

де $С_в$ - вартість відновлення й модернізації системи ($С_в = 0$);

$С_к$ - витрати на керування системою в цілому;

$С_{ак}$ - витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак} = 0$ грн.).

Витрати на керування системою інформаційної безпеки ($С_к$) складають:

$$С_к = С_н + С_а + С_з + С_{ел} + С_о + С_{тос}, \text{ грн.}$$

Витрати на навчання адміністративного персоналу й кінцевих користувачів визначатимуться сукупною величиною витрат на організаційні заходи, які відповідно до запропонованих рішень включать наступні заходи (табл. 3.1.):

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_з$), складає:

$$С_з = З_{осн} + З_{дод}, \text{ грн.}$$

Таблиця 3.1 – Витрати на організаційні заходи

Організаційні заходи	Кількість	Ціна, грн.	Вартість, грн.
Захист від шкідливого програмного забезпечення (вірусів, «троянських коней»)	1	2000	2000
Розгалуження прав та аутентифікація користувачів	1	2000	2000
Способи боротьби за несанкціонованим доступом	1	2000	2000
Політика безпеки антивірусного захисту	1	2000	2000
Політика безпеки використання електронної пошти	1	2000	2000
Політика безпеки робочих станцій	1	2000	2000
Разом:			12000

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата – в розмірі 8-10% від основної заробітної плати.

Основна заробітна плата одного спеціаліста з інформаційної безпеки на місяць складає 16100 грн. Додаткова заробітна плата – 10% від основної заробітної плати. Виконання роботи щодо впровадження системи захисту інформації на підприємстві потребує залучення спеціаліста інформаційної безпеки на 0,25 ставки. Отже,

$$С_з = (16100*12 + 16100*12*0,1)*0,25= 53130 \text{ грн.}$$

Ставка ЄСВ для всіх категорій платників з 01.01.2021 р. складає 22%.

$$С_{єв} = 53130*0,22 = 11689 \text{ грн.}$$

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_{ел}$), визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е, \text{ грн.},$$

де Р – встановлена потужність апаратури інформаційної безпеки, (Р=1,1 кВт);

$F_р$ – річний фонд робочого часу системи інформаційної безпеки ($F_р$ = 1920 год.);

$Ц_е$ – тариф на електроенергію, ($Ц_е$ = 1,68 грн./кВт за годину).

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року:

$$С_{ел} = 0,8*6*1920*1,68 = 15483 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат - 2% ($С_{тос}$ = 43565,33*0,02=871,33 грн).

Витрати на керування системою інформаційної безпеки ($С_к$) визначаються:

$$С_к = 12000+53130+= 71503,72 \text{ грн.}$$

Таким чином, річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = 14976+71503,72+11689+15483+871,33 = 114523,1 \text{ грн.}$$

3.2 Оцінка можливого збитку від атаки на вузол або сегмент мережі

Для розрахунку вартості такого збитку можна застосувати наступну спрощену модель оцінки для умовного підприємства.

Необхідні *вихідні дані* для розрахунку:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, 2 години;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 4 години;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, 4 години;

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), 16100 грн./міс.;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 14000 грн./міс.;

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.), 1 особи;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 5 осіб.;

О – обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 730 тис. грн. у рік;

$П_{зч}$ – вартість заміни встаткування або запасних частин, 6000 грн;

I – число атакованих сегментів корпоративної мережі, 1;

N – середнє число атак на рік, 11.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить:

$$U = П_п + П_в + V,$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

$П_в$ – вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки:

$$П_П = \frac{\sum Зс}{F} \cdot t_п = \frac{14000 \cdot 5}{176} \cdot 2 = 795{,}45 \text{ грн},$$

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить 176 ч).

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_в = П_{ви} + П_{пв} + П_{зч},$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн.;

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{ви} = \frac{\sum Зс}{F} \cdot t_{ви} = \frac{14000 \cdot 5}{176} \cdot 4 = 1590{,}91 \text{ грн.}$$

Витрати на відновлення сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{пв} = \frac{\sum Зо}{F} \cdot t_в = \frac{16100 \cdot 1}{176} \cdot 4 = 365{,}91 \text{ грн.}$$

Тоді витрати на відновлення працездатності вузла або сегмента корпоративної мережі складуть:

$$П_в = 1590{,}91+365{,}91+6000 = 7956{,}82 \text{ грн.}$$

Втрати від зниження очікуваного обсягу прибутків за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи із средньогодинного обсягу прибутку і сумарного часу простою сегмента корпоративної мережі:

$$V = \frac{O}{Fг} \cdot (t_П + t_В + t_{ВИ})$$

$$V = \frac{730000}{2080} \cdot (2+4+4) = 3509{,}62 \text{ грн.}$$

де $F_г$ – річний фонд часу роботи філії (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько 2080 год.

$$U = 795{,}45+7956{,}82+3509{,}62=12261{,}89 \text{ грн.}$$

Таким чином, загальний збиток від атаки на сегмент корпоративної мережі організації складе:

$$B = \sum_i \sum_n U = \sum_1 \sum_{16} 12261{,}89 = 196190{,}2 \text{ грн.}$$

3.2.1 Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної:

$$E = B \cdot R - C \text{ грн.},$$

де B – загальний збиток від атаки у разі перехоплення інформації, тис. грн.;

R – вірогідність успішної реалізації атаки на сегмент мережі, частки одиниці (70%);

С – щорічні витрати на експлуатацію системи інформаційної безпеки.

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки:

$$E = 196190,2*0,7 - 114523,1 = 22810,07 \text{ грн.}$$

3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки:

$$ROSI = \frac{E}{K}, \quad \text{частки одиниці,}$$

де E – загальний ефект від впровадження системи інформаційної безпеки грн.;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Коефіцієнт повернення інвестицій ROSI:

$$ROSI = \frac{22810,07}{43565,33} = 0,52, \quad \text{частки одиниці,}$$

Проект визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції:

$$ROSI > (N_{деп} - N_{інф})/100),$$

де $N_{деп}$ – річна депозитна ставка, (6%);

$N_{інф}$ – річний рівень інфляції, (5%).

Розрахункове значення коефіцієнта повернення інвестицій:

$$0,52 > (6 - 5)/100 = 0,52 > 0,01.$$

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$T_O = \frac{K}{E} = \frac{1}{ROSI} = \frac{1}{0,52} = 1,91 \quad \text{років.}$$

3.4 Висновок

Розробка системи управління інформаційною безпекою приватного підприємства з оцінки майна може вважатися економічно доцільною, оскільки коефіцієнт повернення інвестицій складає 0,52 грн./грн. (ROSI=0,52), що вищим доходності альтернативного вкладення коштів та дозволяє отримати 0,52 грн. економічного ефекту на 1 грн. капітальних витрат. Капітальні витрати складуть 43565,33 грн., експлуатаційні витрати – 114523,1 грн. Економічний ефект – 22810,07 грн. Термін окупності – майже 2 роки.

ВИСНОВКИ

В першій частині роботи охарактеризовані та проаналізовані типові оціночні підприємства, розглянуто загальні відомості про управління інформаційною безпекою, її мету та основні задачі. Проаналізована державна нормативно-правова база у сфері захисту комерційної таємниці, конфіденційної інформації та нормативно-правова база оціночної діяльності.

Обґрунтована необхідність розробки системи управління інформаційною безпекою для здійснювання роботи. Основними заходами по підвищенню інформаційної безпеки підприємства, що досліджується стала розробка інструкцій для персоналу та правил користування програмним забезпеченням.

Всі рекомендації, наведені у спеціальній частині роботи, було впроваджено та введено до статусу апробації на реальному об'єкті інформаційної діяльності – оціночному приватному підприємстві, в результаті чого було досягнуто поставленої на початку проекту мети - підвищенню рівня інформаційної безпеки даного підприємства.

Доведено економічну доцільність впровадження рекомендацій та заходів, поданих у роботі.

Проаналізувавши отриманий результат роботи, була зроблена спроба подання послідовних заходів зі створення проблемно-орієнтованої політики інформаційної безпеки у вигляді алгоритму, який можна застосувати на малих приватних підприємствах аналогічного роду діяльності та структури.

ПЕРЕЛІК ПОСИЛАНЬ

1. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. -К.: ООО ТИД ДС ISBN: 966-7992-02-0, 2001. -688 с.

2. Закон України № 80/94-ВР від 5 липня 1994 р. «Про захист інформації в інформаційно-телекомунікаційних системах».

3. Інформаційна безпека/ Спосіб доступу: URL: http://www.dstszi.gov.ua/dstszi/doccatalog/document;jsessionid=5422822BF139A55D C96EB775E6E227DB?id=49949.

4. Реферат: інформаційна безпека України / Спосіб доступу: URL: http://www.securily.ukjTiet.net/modules/sections/index.php?op^iewarticle&artid=946

5. Зміст основних заходів щодо політики ІБ / Спосіб доступу: URL: http ://www. security. ukrnet.net/modules/sections/index.php?op=vie warticle&artid= 101

6. Визначення суті політики інформаційної безпеки / Спосіб доступу: URL: http://www.security.ukrnet.neiymodules/sections/index.php?opiewaiticle &artid=95

7. Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України НД ТЗІ 1.1-002-99 від 28.04.99р. №22 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу».

8. Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України НД ТЗІ 1.4-001-2000 від 04.12.00 №53 «Типове положення про службу захисту інформації в автоматизованій системі».

9. Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України НД ТЗІ 3.6-001-2000 від 20.12.00 №60 «Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу».

10. Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України НД ТЗІ 3.7-001-99 від 28.04.99 №22 «Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі».

11. Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України НД ТЗІ 3.7-003-05 від 08.11.05 №125 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі».

12. Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України НД ТЗІ 2.5-004-99 від 28.04.99 №22 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу».

13. Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України НД ТЗІ 2.5-005-99 від 28.04.99 №22 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу».

14. Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України НД ТЗІ 1.1-003-99 від 28.04.99 №22 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу».

15. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення.; Чинний від 01.01.97.

16. ДСТУ 3396.1-96 Захист інформації. Технічний захист інформації. Порядок проведення робіт.; Чинний від 01.07.97.

17. ДСТУ 3396.1-96 Захист інформації. Технічний захист Інформації. Терміни та визначення.; Чинний від 01.01.98.

18. Постанова Кабінету Міністрів України №373 від 29.03.06 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах».

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	1 Розділ	37	
6	А4	2 Розділ	28	
7	А4	3 Розділ	12	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	
14	А4	Додаток Д	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Титульна сторінка.doc

2 Завдання.doc

3 Реферат.doc

4 Список умовних скорочень.doc

5 Зміст.doc

6 Вступ.doc

7 Розділ 1.doc

8 Розділ 2.doc

9 Розділ 3.doc

10 Висновки.doc

11 Перелік посилань.doc

12 Додаток А.doc

13 Додаток Б.doc

14 Додаток В.doc

15 Додаток Г.doc

16 Додаток Д.doc

Презентація.pptx

ДОДАТОК В. ПЛАН ОБ'ЄКТУ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

ДОДАТОК Г. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Д. ВІДГУК
на кваліфікаційну роботу бакалавра на тему:
Розробка системи управління інформаційною безпекою приватного підприємства з оцінки майна
Данильченка Олексія Ігоровича

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на___сторінках та містить __ рисунків,___таблиць,___джерел та___додатка.

Об'єкт досліджень: інформаційна система приватного підприємства з оцінки майна.

Мета роботи: розробка алгоритму для підвищення рівня інформаційної безпеки приватного підприємства з оцінки майна.

В першій частині роботи розглянуто загальні відомості про інформаційної безпеки, її мету та основні задачі. Проаналізована державна нормативно-правова база у сфері захисту комерційної таємниці, конфіденційної інформації та оціночної діяльності.

У спеціальній частині роботи розроблено технічне завдання на роботу по розробці політики інформаційної безпеки приватного підприємства з оцінки майна.

Студент показав достатній рівень володіння теоретичними положеннями з обраної теми, показав здатність формувати власну точку зору (теоретичну позицію).

Робота оформлена та написана грамотною мовою. Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

В цілому робота задовольняє усім вимогам і може бути допущена до захисту, а його автор заслуговує на оцінку «_____».

Керівник