ЗАТВЕРДЖЕНО
Наказ Вищого навчального закладу Укоопспілки
«Полтавський університет економіки і торгівлі»
18 квітня 2019 року № 88-Н

Форма № П-4.03

Вищий навчальний заклад Укоопспілки
«ПОЛТАВСЬКИЙ УНІВЕРСИТЕТ ЕКОНОМІКИ І ТОРГІВЛІ»
Інститут економіки, управління та інформаційних технологій
Форма навчання заочна
Кафедра документознавства та інформаційної діяльності в економічних системах

Допускається до захисту
Завідувач кафедри _____Т. В. Оніпко
(підпис)
«____» грудня 2019 р.

ДИПЛОМНА РОБОТА

на тему:

«Управління забезпеченням ефективності системи інформаційної безпеки підприємства»
(за матеріалами товариства з обмеженою відповідальністю спільного підприємства «Полтавська газонафтова компанія»)

зі спеціальності 029 Інформаційна, бібліотечна та архівна справа
освітня програма «Документознавство та інформаційна діяльність»

Виконавець роботи Пухай Іван Андрійович

_____
(підпис, дата)

Науковий керівник д. фіз.-м. н., професор Колєчкіна Людмила Миколаївна

_____
(підпис, дата)

Рецензент

Полтава 2019

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ПЗ – Програмне забезпечення;

НБ – Національна безпека

САД – Система автоматизації діловодства та документообігу

СЗІ – Система захисту інформації

СЗІБ – Система забезпечення інформаційної безпеки

СУІБ – Система управління інформаційною безпекою

ІС – Інформаційна система

ЗУ – Закон України

ЗМІ – Засоби масової інформації

ІТ – Інформаційні технології

ЗОТ – Засоби обчислювальної техніки

ЗІ – Захист інформації

ІАС – Інформаційно-аналітична система

БД – База даних

ТЗІ – Технічний захист інформації

ПЕОМ – Персональна електроно-обчислювальна машина.

ВСТУП

З огляду на стабільний розвиток демократичних процесів, стан соціально-політичної та економічної ситуації в країні існуючий стан інформаційного забезпечення державного управління як одного з елементів системи забезпечення інформаційної безпеки держави потребує значного покращення.

Входження України до євроатлантичних структур, прагнення вступу до Всесвітньої торговельної організації, а також намагання створити регіональну систему безпеки, яка стала б основою загальноєвропейської системи безпеки, потребують дієздатної системи органів виконавчої влади. Причому дана система повинна відповідати вимогам сьогодення, тобто при її моделюванні має застосовуватись сучасна методологія дослідження динамічних об’єктів.

Серед цілої гами цих елементів чільне місце посідають питання правового та організаційного забезпечення інформаційної безпеки органів виконавчої влади. Таким чином, інформаційне забезпечення органів виконавчої влади є одним із складових елементів загальної системи забезпечення державного управління, а з урахуванням того, що Українська держава потребує застосування саме вказаної системи заходів, розроблення теоретичних і практичних питань адміністративно-правового регулювання, набуває неабиякого значення. Передусім потребують уваги теоретичні питання інформаційного забезпечення як такого, що є життєво необхідним для сильної держави та її сталого розвитку.

Слід зазначити, що на сьогодні становлення ефективної державної влади є пріоритетним напрямом в загальній стратегії розвитку України, водночас інформаційне забезпечення органів виконавчої влади є його основою і має розглядатися як один з основних. Більш того, аналіз спеціальної літератури, а також масивів практичної інформації дає змогу говорити про відсутність єдиної концепції підходу до інформаційного забезпечення системи органів виконавчої

влади. Частими залишаються випадки неефективного використання сил і засобів органів виконавчої влади в процесі забезпечення їх інформаційної безпеки.

Все це потребує запровадження змін у структурі центральних органів виконавчої влади відповідно до пріоритетних напрямів та першочергових завдань діяльності Кабінету Міністрів України з чітким визначенням та недопущенням дублювання їх функцій.

Досі відсутня цілісна система поглядів на захист інформаційного суверенітету держави, що відповідними чином позначається на рівні реалізації конституційних прав і свобод громадян, суспільства і держави в інформаційні сфері.

Невирішеною сьогодні залишається проблема забезпечення органів виконавчої влади своєчасною достовірною інформацією, яка є необхідною для прийняття рішень в сфері державного управління.

Зважаючи на сучасний стан розробленості теми, актуалізується потреба виконання дослідження для визначення особливостей забезпечення інформаційної безпеки органів державного управління.

На основі результатів дослідження чітко виявлено загрози інформаційній безпеці,основи формування і функціонування системи забезпечення, цілі і задачі системи інформаційної безпеки, її недоліки, та шляхи вдосконалення сучасної інформаційної безпеки.

Актуальність проблеми інформаційної безпеки визначається сучасними тенденціями в області інформаційних, комп’ютерних технологій, у сфері формування нового типу суспільства і економіки, що характеризується різними економістами, соціологами по-різному. Просування України до інформаційного суспільства вимагає ефективного управління усіма видами інформаційних ресурсів та елементами інформаційно-телекомунікаційної інфраструктури, державної підтримки вітчизняного інформаційного виробництва, ринку інформаційних технологій, засобів, продуктів і послуг.

Питання забезпечення інформаційної безпеки сьогодні для України стоять на одному рівні із захистом суверенітету і територіальної цілісності, забезпеченням її економічної безпеки. Рівень інформаційної безпеки активно впливає на стан політичної, економічної, оборонної та інших складових національної безпеки України, бо найчастіше реалізація інформаційних загроз - це нанесення шкоди в політичній, військовій, економічній, соціальній, екологічній сферах тощо.

В сучасних ринкових умовах господарювання інформаційна безпека в умовах глобального інформаційного суспільства відіграє провідну роль. Широка інформатизація всіх сфер життя суспільства, зокрема сфери забезпечення безпеки особи, суспільства, економіки і фінансів, державної інфраструктури, ставить питання про комплексний підхід до проблеми інформаційної безпеки.

Мета дослідження полягає у всебічному вивченні стану забезпечення ефективності системи інформаційної безпеки підприємтва, а саме – спільного підприємства «Полтавська газонафтова компанія» (СП ПГНК), розробці пропозицій щодо формування управління забезпечення ефективності системи інформаційної безпеки і виробленні на основі цих пропозицій, рекомендацій, спрямованих на удосконалення захисту інформації на підприємстві.

Реалізація поставленої мети зумовила необхідність вирішень завдань:

– дослідити поняття та зміст інформаційної безпеки, що дає можливість зрозуміти реальну ситуацію з інформаційною безпекою на підприємствах;

– розглянути характеристику загроз інформаційній безпеці підприємства;

– дослідити нормативно-правові аспекти захисту інформації на підприємстві;

– проаналізувати діяльності товариства з обмеженою відповідальністю спільного підприємства «Полтавська газонафтова компанія»;

– дослідити основні принципи та методи забезпечення інформаційної безпеки на спільному підприємстві «Полтавська газонафтова компанія»;

– оцінити стан забезпечення інформаційної безпеки в спільному підприємстві «Полтавська газонафтова компанія»;

– визначити принципи захисних заходів від несанкціонованого доступу в автоматизованих системах;

– дослідити засоби забезпечення захисту інформації в автоматизованих інформаційних системах в спільному підприємстві «Полтавська газонафтова компанія»;

– вивчити методи захисту електронної корпоративної інформації на підприємстві.

Об’єктом дослідження виступає процес управління забезпеченням захисту інформаційних процесів на підприємстві.

Предметом дослідження дипломної роботи є теоретичні засади та прикладні аспекти проблеми захисту інформаційних процесів на підприємстві.

Суб’єкт дослідження – товариство з обмеженою відповідальністю спільне підприємство «Полтавська газонафтова компанія».

Методи дослідження. В основі дослідження лежить широкий спектр сучасних філософських, загальнонаукових та спеціальних методів пізнання державно-правових процесів та явищ.

У основу дипломного дослідження покладено загальнонаукові та спеціальні методи дослідження як порівняння (у підпункті 1.2 при характеристиці загроз інформаційній безпеці), узагальнення (у підпункті 2.3 при обґрунтуванні оцінки інформаційної безпеки у місцевому органі державного управління); метод класифікації (у підпункті 3.1 для систематизації методів захисту інформації), аналізу та синтезу (у підпункті 2.2 при формуванні цілей і задач системи інформаційного безпеки органу державного управління) та інші загальноприйняті методи.

Наукова новизна отриманих результатів дослідження полягає в наступному: удосконалено:

– підхід до раціональної організації ефективності системи інформаційної безпеки підприємства, а саме товариство з обмеженою відповідальністю спільне підприємство «Полтавська газонафтова компанія».

Отримало подальший розвиток:

– раціональний підхід до організації управління забезпеченням ефективності системи інформаційної безпеки підприємства товариство з обмеженою відповідальністю спільне підприємство «Полтавська газонафтова компанія».

Практичне значення роботи полягає в розробці рекомендацій щодо вдосконалення управління забезпечення ефективності системи інформаційної безпеки підприємства, а саме товариства з обмеженою відповідальністю спільне підприємство «Полтавська газонафтова компанія».

Апробація теми дослідження. Результати дослідження щодо організації діловодства у видавництві відображено у науковій статті: Пухай І.А. Управління забезпечення ефективності системи інформаційної безпеки підприємства / І.А.Пухай, Л.М.Колєчкіна // Збірник наукових статей магістрів. Інститут економіки, управління та інформаційних технологій. – Полтава: ПУЕТ, 2019. – С. 32-36.

Робота складається зі вступу, трьох розділів, висновків; містить 109 сторінок тексту, 7 рисунків, 5 таблиць, 3 додатків. Список джерел включає 85 найменувань літератури, 11електронних публікацій.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

1.1 Поняття та зміст інформаційної безпеки підприємства

Захист інформації – є практичною реалізацією комплексної програми (концепції) інформаційної безпеки установи і являє собою жорстко регламентований і динамічний технологічний процес, що попереджає порушення доступності, цілісності, достовірності та конфіденційності цінних інформаційних ресурсів і в кінцевому рахунку забезпечує досить надійну безпеку інформації в процесі управлінської та виробничої діяльності установи. В даному випадку безпека розцінюється як реального результат, досягнутий за рахунок функціонування обраної системи захисту інформації. Передбачається, що захист конфіденціальної інформації (або захист секретів) здійснюється від різного виду загроз безпеки інформації, і насамперед несанкціонованого доступу до неї зловмисника [1]. Захисту підлягає будь документована інформація, неправомірне поводження з якою може завдати шкоди її власнику, власнику, користувачеві або іншій особі. Захисту потребує не тільки конфіденційний документ. Часто звичайний відкритий правовий акт важливо зберегти в цілісності та безпеці від викрадача чи стихійного лиха.

Характерною ознакою сучасного етапу економічного і науково-технічного прогресу є стрімкий розвиток інформаційних технологій, їх якнайширше використання у повсякденному житті та в управлінні державою. Інформація і інформаційні технології все більше визначають розвиток суспільства та слугують новими джерелами національної могутності. В умовах становлення інформаційного суспільства радикально змінюються політична, екологічна і соціальна сфери життєдіяльності людства. Крім того, формування інформаційного суспільства змінює предмет праці на інформацію та знання. У свою чергу основою глобалізації

стають інтеграція інформаційних систем різних держав до єдиної загальносвітової інформаційної системи, формування єдиного інформаційного простору, створення глобальних інформаційно-телекомунікаційних тенет, інтенсивне впровадження нових інформаційних технологій в усі галузі суспільного життя, включаючи й державне управління.

Глобальний процес інформатизації суспільства охопив майже усі країни світу і нині є стрижнем науково-технічного і соціально-економічного розвитку. Інформатизація являє собою організаційний соціально-економічний і науково-технічний процес створення оптимальних умов для всебічного задоволення інформаційних потреб і реалізації прав громадян, суспільства, органів державної влади і управління на основі формування та використання інформаційних ресурсів, а також інформаційних систем, тенет, ресурсів та інформаційних технологій із використанням обчислювальної і комунікаційної техніки. Основними завданнями інформатизації органів виконавчої влади є: всебічне інформаційне забезпечення потреб органів виконавчої влади всіх рівнів; створення єдиного інформаційного простору для усієї системи органів виконавчої влади; створення, впровадження і використання інформаційних систем, інформаційних технологій і інформаційних продуктів загального значення; підготовка кадрів, підвищення їхньої кваліфікації в сфері інформатизації. Таким чином, органи виконавчої влади є суб’єктом інформатизації. Відповідно основними напрямами державної політики в сфері інформатизації можна вважати: забезпечення умов для розвитку і захисту усіх форм власності на інформаційні ресурси; формування та захист державних інформаційних ресурсів; створення та розвиток державних, регіональних і локальних інформаційних систем і тенет, забезпечення їх сумісності і взаємодії в єдиному інформаційному просторі; створення умов для якісного й ефективного інформаційного забезпечення органів державного управління на основі державних інформаційних ресурсів; забезпечення національної безпеки в сфері

інформатизації, а також забезпечення взаємної реалізації прав як громадян, так і органів виконавчої влади в умовах інформатизації; сприяння формуванню ринку інформаційних ресурсів, послуг, інформаційних систем, технологій і засобів їх забезпечення. В результаті розгляду змісту інформаційного забезпечення органів виконавчої влади, суб'єктів та об'єктів інформаційного забезпечення функціонування органів виконавчої влади цілком логічно випливає наступне визначення поняття та змісту інформаційної безпеки як певної діяльності, спрямованої на гарантування достатнього рівня захищеності національних інтересів в інформаційній сфері.

У ширшому розумінні йдеться про забезпечення інформаційного суверенітету України; вдосконалення державного управління інформаційною сферою, впровадження інноваційних технологій у цій сфері; наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну; активне залучення ЗМІ до боротьби з корупцією, зловживаннями службовим становищем, іншими явищами, що загрожують національній безпеці України; неухильне дотримання конституційного права громадян на свободу слова, доступу до інформації; недопущення неправомірного втручання органів виконавчої влади, їх посадових осіб у діяльність засобів масової інформації, дискримінації в інформаційній сфері та переслідування журналістів за політичні позиції; застосування комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України [2].

Інформаційна безпека є складовою загальної проблеми інформаційного забезпечення функціонування системи органів виконавчої влади.

Зазначимо, що розвиток інформаційних технологій – дуже важлива державна функція, а обов'язковою умовою забезпечення ефективного використання накопичених суспільством інформаційних ресурсів є створення розвиненого і захищеного інформаційного середовища. Цій меті слугує організація

функціонування системи інформаційної безпеки, складовими якої є сама інформаційна безпека як об’єкт управління органами виконавчої влади, система забезпечення інформаційної безпеки, тобто суб’єкт управління, зв’язки між ними, а також внутрішнє та зовнішнє середовище.

Зрозуміло, що інформаційна безпека забезпечується цілим комплексом заходів, вивченню яких відповідно приділяють певну увагу науковці. Осягнення суті предмета, з’ясування змісту поняття «інформаційна безпека» – важливі завдання наукового аналізу. Будь-яке вчення лише тоді досягає цілісності і досконалості, коли розкриває зміст досліджуваних явищ, має можливість передбачати майбутні зміни не лише в сфері явищ, а й у сфері сутностей. Пізнання сутності інформаційної безпеки можливе лише на основі абстрактного мислення, створення теорії досліджуваного предмета, з’ясування внутрішнього змісту, виявлення характерних ознак, розкриття суттєвих характеристик поняття, що вивчається. В історичному процесі складається структура предмета, тобто єдність внутрішнього змісту і зовнішніх проявів, співпадаючих і неспівпадаючих суперечливих сутностей. Сутність – сукупність глибинних зв’язків, відносин і внутрішніх законів, які визначають основні риси і тенденції розвитку системи. Сутність може вважатися пізнаною, коли відомі причини виникнення та джерела розвитку об’єкта, що розглядається, шляхи його формування або технічного репродукування, якщо в теорії чи на практиці створена його достовірна модель. Одна й та ж сутність може мати множину різних явищ. Сутність виражається і осягається в дефініції, яка виражає родове поняття. Щодо інформаційної безпеки таким є поняття безпеки, що характеризує певний стан захищеності від внутрішніх та зовнішніх загроз. Відповідно видове поняття «інформаційна безпека» означає стан захищеності національних інтересів в інформаційній сфері від внутрішніх і зовнішніх загроз. Саме тому інформаційна безпека є невід’ємною частиною загальної безпеки - чи то національної, чи то регіональної, чи то міжнародної.

Варто зазначити, що у науковій літературі поки відсутній єдиний консолідований підхід до змісту поняття «інформаційна безпека». Для одних воно відображає стан, для інших процес, діяльність, здатність, систему гарантій, властивість, функцію. З метою упорядкування різних поглядів ми вирішили їх класифікувати за критерієм ознаки, що визначає зміст даного поняття. Таким чином, нами були виокремлені такі напрями підходів. Наприклад, деякі науковці характеризують інформаційну безпеку як «стан захищеності інформаційного середовища, який відповідає інтересам держави, якого забезпечується формування, використання і можливості розвитку незалежно від впливу внутрішніх та зовнішніх інформаційних загроз». А також деякі українські дослідники, які вважають за необхідне визначати інформаційну безпеку як стан захищеності. Інші дослідники визначають інформаційну безпеку як стан захищеності життєво важливих інтересів особи, суспільства та держави, який виключає можливість заподіяння їм шкоди через неповноту, невчасність і недостовірність інформації, через негативні наслідки функціонування інформаційних технологій або внаслідок поширення законодавчо забороненої чи обмеженої для поширення інформації, тоді як Додонов О.Г. визначає інформаційну безпеку як стан захищеності інформаційного простору, що забезпечує формування та розвиток цього простору в інтересах особистості, суспільства та держави [3]. Ряд представників цього напряму розглядають інформаційну безпеку як стан, що характеризується відсутністю небезпеки, тобто чинників та умов, які загрожують безпосередньо індивіду, спільноті, державі з боку інформаційно-комунікаційного середовища. Прибічники такого підходу вважають інформаційну безпеку станом і процесом захищеності особи, суспільства, держави від реальних або потенційних загроз . Водночас, на нашу думку, розглядати безпеку лише в якості стану не зовсім доречно, тому що це не відображає динамізму як самої безпеки, так і тієї системи, для якої безпека виступає функцією її подальшого розвитку та існування [4].

Застосування дієвого підходу, на наш погляд, більш адекватне при описі інформаційної безпеки, і ми в певній мірі підтримуємо дане визначення в загальному плані, однак не можемо погодитись із деталізацією напрямів діяльності, які з часом змінюватимуться, отже закладатимуть потенціал нестійкості як до самого визначення, так і до функціонування відповідних суб'єктів. Хрипков М.П. вважає, що діяльність щодо гарантування особи, суспільства та держави виникає в процесі вирішення суперечностей між такою об'єктивною реальністю, як небезпека, і потребою розумної сутності, соціального індивіда, соціальної групи попередити її можливі шкідливі наслідки. Водночас за даного випадку функціонування системи забезпечення інформаційної безпеки зводиться лише до реагування, тоді як превенція лишається поза увагою. Саме тому, на наше переконання, інформаційна безпека являє собою діяльність органів державного управління в цілому і органів виконавчої влади зокрема. Звідси випливає важливий висновок, що слід діяти активно, впливаючи на джерела інформаційної небезпеки. При цьому щодо змісту інформаційної безпеки доцільно використовувати не поняття «інтереси», а більш фундаментальнее – «цінності», через те що у цінностях знаходять відображення інтереси суб'єктів суспільних відносин, зіткнення яких породжує загрози. Наступний напрям передбачає, що у самому загальному вигляді під інформаційною безпекою можна розуміти здатність суб'єкта зберігати свої системоутворюючі властивості, основні характеристики при ТОВогенних дезорганізуючих, деструктивних впливах на кіберпростір, інформаційно-комунікаційні технології [5]. На думку прибічників даної концепції, безпека та забезпечення безпеки – різні поняття, тому що безпека виражає характеристику стану соціальної спільноти, а забезпечення безпеки – дієву характеристику, тобто діяльність органів виконавчої влади й управління по підтриманню безпеки. У цьому разі безпека усвідомлюється як основа цілепокладання політики, а забезпечення безпеки – діяльність по досягненню безпечного стану суспільства чи

соціальної групи. Цікаве судження з цього приводу відомого українського дослідника проблем інформаційної безпеки Калюжного Р.А. Він вважає, що інформаційна безпека – вид суспільних інформаційних правовідносин щодо створення, підтримки, охорони та захисту бажаних для людини, суспільства і держави безпечних умов життєдіяльності; суспільних правовідносин пов'язаних із створенням, поширенням, зберіганням та використанням інформації . У цілому ж інформаційна безпека спрямована на забезпечення реалізації національних інтересів за допомогою всього арсеналу засобів, що є в її розпорядженні. У цьому аспекті ми вважаємо, що найвищий сенс політики інформаційної безпеки – вільний розвиток і процвітання суспільства. Отже інформаційна безпека являє собою одне з найважливіших понять у науці і різних сферах людської діяльності. Сутність і комплексність цього поняття виявляється характером сучасного інформаційного суспільства. Аналіз різних підходів до визначення змісту поняття «інформаційна безпека» дає змогу зауважити про недоцільність жорсткого обрання тієї чи іншої позиції. Наведені вище погляди, а вірніше, підходи до визначення поняття інформаційної безпеки дають змогу розглядати дану проблему комплексно та системно, додати знань про цей багатогранний феномен. Більш того, на наше переконання, найприйнятніщим є інтегральний підхід, відповідно до якого інформаційна безпека визначатиметься за допомогою окреслення найважливіших її сутнісних ознак з урахуванням постійної динаміки інформаційних систем. Такий підхід дав нам можливість зробити висновок, що інформаційна безпека не може розглядатися лише в якості окремого стану. Безперечно, вона є і властивістю, і атрибутом інформаційного суспільства, і діяльністю, і результатом діяльності людини, спрямованої на забезпечення певного рівня безпеки в інформаційній сфері [6].

Інформаційна безпека має враховувати майбутнє, отже вона є не станом, а процесом. Таким чином, інформаційну безпеку слід розглядати крізь органічну

єдність ознак, таких як стан, властивість, а також управління загрозами і небезпеками, за якого забезпечується обрання оптимального шляху їх усунення та мінімізації впливу негативних наслідків, зокрема у сфері інформаційної діяльності органів виконавчої влади. Також наголосимо на тому, що не підтримуємо позицій тих дослідників, які вважають інформаційну безпеку лише захистом інформації. Інформаційна безпека за своєю суттю є більш широким поняттям. Отже інформаційна безпека – багатогранна сфера діяльності, успіх в якій може принести лише системно-комплексний підхід.

При дослідженні сутності інформаційної безпеки має враховуватися той факт, що сутність є внутрішнім змістом предмету, який знаходить відображення у сталій єдності усіх багатоманітних і суперечливих форм буття. Базовою характеристикою інформаційної безпеки слід вважати імовірність підвищеного ризику реалізації загрози або небезпеки для діяльності органів виконавчої влади в цілому і для кожного її структурного елементу зокрема. Критерієм ефективності забезпечення інформаційної безпеки є високий рівень безпеки при мінімумі відповідних затрат. Отже можна говорити про структуру поняття інформаційної безпеки. Основним її елементом є життєво важливі інтереси соціальної системи, які співвідносяться із зовнішніми чинниками у вигляді інтересів наднаціональних або інших національно-державних структур в рамках міжнародного співтовариства. Зсередини національно-державного утворення його життєво важливі інтереси взаємодіють з інтересами його складових елементів. В якості останніх виступають соціальні групи, еліта, організації, партії, релігійні та етнічні утворення, рухи тощо. Сукупність внутрішніх і зовнішніх інформаційних загроз створює передумови для порушення безпечного функціонування системи органів виконавчої влади. Значущість інформаційно-комунікаційних процесів у сучасному світі дає підстави розглядати забезпечення інформаційної безпеки як одне з глобальних і пріоритетних завдань функціонування органів виконавчої влади, вирішенню якого

мають бути підпорядковані політична, економічна, воєнна, культурна та інші сфери системи державного управління нашої країни. Як нами вже зазначалося, національні інтереси в інформаційній сфері є похідними від національних цінностей. Отже інтереси інформаційної безпеки походять від таких цінностей, як права людини, свобода, економічне процвітання. Саме тому, головним інтересом для України є її виживання як вільної незалежної держави при збереженні її фундаментальних цінностей і інститутів безпеки.

До характеристик, що дають змогу описати дану систему можна віднести такі: доступність – можливість за прийнятний час отримати необхідну інформаційну послугу будь-яким суб'єктом виконавчої влади; цілісність – актуальність і несуперечливість інформації, її захищеність від руйнування та несанкціонованої зміни; конфіденційність – захист від несанкціонованого ознайомлення [7]. Сутність і зміст інформаційної безпеки проявляються по-особливому на кожному з рівнів системи органів виконавчої влади, зокрема на: стратегічному – Кабінет Міністрів України; тактичному – центральні органи виконавчої влади; оперативному – місцеві органи виконавчої влади, провідне місце серед яких посідають місцеві державні адміністрації. Таким чином, можна говорити і про прояви інформаційної безпеки у самому процесі її забезпечення. У зв'язку з цим можна виділити такі її рівні: нормативно-правовий – закони, нормативно-правові акти, тощо; адміністративний – дії загального характеру, що вживаються органами виконавчої влади; процедурний – конкретні процедури забезпечення інформаційної безпеки; програмно-технічний – конкретні технічні заходи забезпечення інформаційної безпеки. Для розкриття сутності і змісту інформаційної безпеки важливим є зв'язок останньої із політикою держави. Складовою політики держави як регулятора суспільних відносин відповідно до гуманістичних засад є обов'язок забезпечення інформаційної безпеки особи, суспільства і державних органів. Необхідність у координації інформаційних

потоків системи органів виконавчої влади виникає саме тоді, коли суперечності та конфлікти у середовищі функціонування створюють загрозу її існуванню взагалі. Інформаційна безпека як одна з характеристик сталого розвитку виступає в якості базової цінності держави. Водночас ціннісні орієнтації, що ґрунтуються на уявленнях про інформаційну безпеку у різних суспільних груп і окремих осіб, почасти не співпадають. Саме у цьому знаходить своє безпосереднє відображення вплив держави, що за допомогою цілої гами методів, чільне місце серед яких посідають адміністративно-правові, виражає загальні цінності в сфері інформаційної безпеки. Система ціннісних орієнтацій тієї чи іншої країни в області інформаційної безпеки знаходить своє вираження в державній інформаційній політиці.

У ході організації (в тому числі створення алгоритмів (методик) захисту інформації технічними засобами) завдання суб'єктів полягає не тільки в удосконаленні існуючих засобів технічного захисту інформації, а й урахуванні можливих новацій. При цьому переважно має реалізовуватися принцип агрегації новацій до наявної системи захисту. Найкраще, коли можна інтегрувати через новації засоби захисту і вилучити із системи захисту застаріле обладнання. Але водночас не слід забувати, що старі засоби захисту, які можуть функціонувати автономно в системі захисту, не повинні "зніматися з озброєння" бездумно.

Організовуючи захист інформації в автоматизованих системах, слід враховувати, що хоч в основі автоматизованої системи є технічний пристрій, який обробляє інформацію, але при його використанні так чи інакше присутній людський фактор. При цьому людина виступає в ролі або безпосередньо (як користувач автоматизованої системи), або опосередковано (як розробник системи).

На основі вище сказаного, можна зробити висновок, що на надійність системи захисту інформації в автоматизованих комп'ютерних системах впливають дві групи взаємопов'язаних факторів: людські (соціальні) та інженерно–технологічні.

В аспекті теорії систем організація захисту інформації в автоматизованих системах передбачає обумовлене виокремлення внутрішньо– і зовнішньо–системних ознак, які утворюють діалектичну гіперсистему організації рубежів безпеки [15, с. 210].

1.2. Загальна характеристика загроз інформаційній безпеці підприємства

Визначальним у проблематиці теорії організації інформаційної безпеки є з'ясування її напрямків на засадах комплексного підходу щодо методів захисту. Умовно можна визначити такі напрямки організації захисту: правові, управлінські, інженерно–технологічні. У складі останніх як автономні визначаються програмно-математичні (комп'ютерні програмні продукти захисту).

Аналіз науково-практичних джерел та іншого емпіричного матеріалу дав змогу сформулювати предметний метод ("метод застосування методів", метод - принцип) – комплексне застосування управлінських, правових та інженерно-технічно-технологічних методів захисту інформації в автоматизованих комп'ютерних системах.

На основі зазначених положень можна зробити висновок про наявність потреби формування проблематики окремих аспектів (інститутів) загальної теорії і практики інформаційної безпеки щодо захисту інформації в автоматизованих комп'ютерних системах. У зв'язку з цим є можливість виокремлення двох частин теорії: загальної (фундаментальних, загальних положень) та особливої частин (відносин щодо окремих напрямків функцій на основі загальних положень) [16, с. 144].

На загальнотеоретичному рівні визначимося в таких ключових, особливих проблемах інформаційної безпеки щодо організаційного аспекту захисту інформації в автоматизованих системах:

- проблеми організації доступу до інформації;

- проблеми організації забезпечення цілісності інформації щодо загроз її порушення;

- проблеми організації сумісності систем захисту інформації в автоматизованих (комп'ютерних) системах з іншими системами безпеки відповідної організаційної структури;

- проблеми організації виявлення можливих каналів несанкціонованого витоку інформації (фізичних, соціотехнічних, соціальних);

- проблеми організації блокування (протидії) несанкціонованого витоку інформації;

- проблеми організації виявлення, кваліфікації, документування порушення інформаційної безпеки (як стану у визначеному просторі, часі і колі осіб);

- формулювання відповідальності та правове визначення санкцій та організація притягнення винних до відповідальності (дисциплінарної, цивільної, адміністративної, кримінальної) [17, с. 88].

На базі аналізу накопиченого емпіричного матеріалу пропонується узагальнити на рівні теоретичних засад (основ) організацію захисту інформації в автоматизованих (комп'ютерних) системах як функції. Задля цього органі–зацію захисту інформації в автоматизованих системах умовно поділяють на три види функцій. За основу поділу визначено такий критерій, як середовище, в якому пере-буває інформація:

- соціальне (окрема людина, спільноти людей, держава);

-інженерно–технікологічне (машинне,апаратно–програмне, автоматичне);

- соціотехнічне (людино-машинне).

Кожен названий рівень щодо середовища об'єктивно доповнює і взаємозумовлює інші функції, в основі утворюючи триєдину гіперсистему: організація інформаційної безпеки. У цій гіперсистемі визначними є такі напрямки

(підрізні), що визначаються на основі інтегративного підходу протилежностей (антиподів) – воздії і протидії:

Рисунок 1.1 – Організація інформаційної безпеки [34]

На названі напрямки організації інформаційної безпеки відповідного об'єкта захисту впливають такі визначальні фактори:

- фактор рівня досягнень науково-технічного прогресу (переважно в галузі розвитку, удосконалення технічних засобів);

- технологічний фактор (в окремих джерелах його ще називають алгоритмічним фактором, коли техніка може бути одна, а технології її застосування різні, цей фактор ще є визначальним для формування методик: як отримання інформації, так і захисту її);

- соціальний (людський) фактор.

Названі елементи основ теорії організації захисту інформації зумовлюють необхідність формування і розвитку окремих теорій інформаційної безпеки (зокрема її складової – теорії організації захисту інформації в автоматизованих системах) у таких аспектах: організаційному, інженерно–технологічному та

пов'язаному з ними правовому. Як відомо, інженерно–технологічний аспект поєднує взаємопов'язані технічний (апаратний) та алгоритмічний (програмний) аспекти (саме тому ми вжили раніше категорію "інженерно–техніко–технологічний").

Враховуючи міжгалузевий характер теорії організації інформаційної безпеки, в ній поєднуються методи пізнання традиційних фундаментальних наук: соціології та фізики. Це зумовлено безпосереднім предметом теорії: людино–машинними (соціотехнічними) системами, якими є автоматизовані комп'ютерні інформаційні системи [19, с. 15].

Звичайно сферою дослідження теорії є практика захисту інформації в автоматизованих (комп'ютерних) системах: її закономірності, принципи, різного рівня проблеми і завдання вирішення їх. Нині проблема і завдання формалізують переважно за допомогою методів евристики: формально–ев–ристичного та інтуїтивно–евристичного. Домінуюче становище серед цих методів мають методи експертних оцінок та оцінки критичної маси інформації, за допомогою яких, зокрема, оцінюють функціонування систем захисту інформації..

Подоланню цих недоліків допомагає когнітологія – наука про знання. Відповідно до положень цієї науки в загальній теорії захисту інформації визначаються як аксіоми когнітологічні положення про рівень і відносність ентропії (невизначеності) системи пізнання (людини, спільноти та ін.) і її вплив на формування теоретичних положень, відносну істинність їх (у часі та колі осіб). Відносність істини визначається кількісними і якісними характеристиками множини знань, якими володіє певний суб'єкт відносин, навичками застосування їх, інтелектуальним потенціалом та швидкістю розумових реакцій на відповідні ситуації. Відносність захисту інформації визначається віднос–ністю знань суб'єкта захисту і відносністю загроз захисту, зокрема знань зловмисника [20, с. 166].

У контексті визначення об'єктивності експертної оцінки організації захисту

інформації, подолання суб'єктивізму, наприклад при визначенні стану інформаційної безпеки об'єкта, застосовують метод залучення кількох експертів. Але, як справедливо зазначають деякі дослідники, при цьому виникає питання, хто може вважатися висококваліфікованим експертом (кваліфікаційні ознаки експерта) і скільки таких експертів потрібно для істинності висновків, подолання суб'єктивізму.

За природою організації захист інформації має комплексний характер, тобто між окремими її складовими є певний зв'язок. У рамках теорії організації захисту інформації чітко визначився постулат, що організація захисту інформації повинна враховувати не тільки складність технічної і технологічної компонент системи, а й людський фактор. Тобто, формуючи конкретну систему технічного захисту, слід враховувати якісні індивідуально– і соціально–психологічні, моральні, етичні та інші особисті характеристики людей, задіяних у системі захисту інформації.

У такому аспекті визначається також напрямок теорії щодо оцінки, характеристики зловмисників, які посягають на безпеку інформаційної системи. У цьому аспекті теорія захисту інформації має зв'язок з кримінологією, її складовими вченнями: віктимологією та теорією формування соціально–психологічного портрету зловмисника [21, с. 105].

Масове впровадження нових технічних засобів, на основі яких здійснюється інформатизація у всьому світі, робить прозорими державні кордони і формує нові геополітичні парадигми у розумінні глобальних соціотехнічних систем. Міжнародна інформаційна сфера стає не тільки однією з важливих сфер співробітництва, а й середовищем конкуренції між окремими особами, державами, міждержавними політичними та економічними угруповуваннями. Електронно-комунікаційна інфраструктура, як і інші інформаційні ресурси, стає об'єктом міждержавної боротьби за світове лідерство або об'єктом недобросовісної конкуренції у підприємницькій діяльності чи інших суспільних інформаційних відносин.

Все це зумовлює необхідність формування такого аспекту інформаційної культури, як культура інформаційної безпеки, культура організації інформаційної безпеки. Зазначений аспект розвитку інформаційної культури набуває відображення у такій прикладній науковій дисципліні, як теорія організації (тектологія) інформаційної безпеки.

Аналіз наукової думки та емпіричного матеріалу дає змогу визначити такі принципові положення організації захисту інформації в умовах інформатизації у контексті інформаційної безпеки (рис. 1.2)

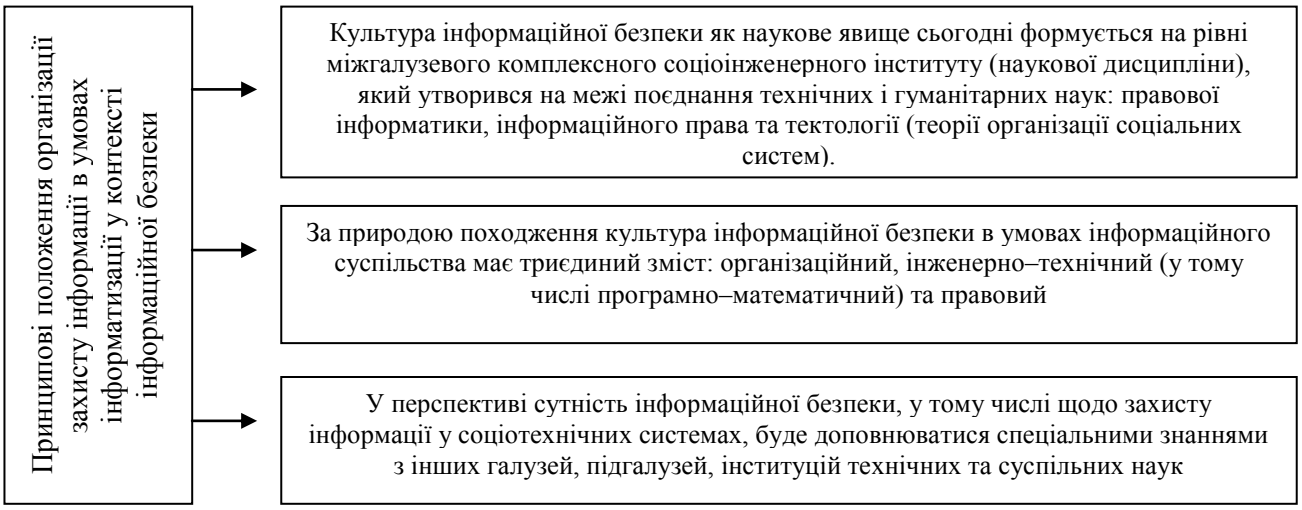

Рисунок 1.4 – Принципові положення організації захисту інформації в умовах інформатизації у контексті інформаційної безпеки [45]

З погляду теорії організації і теорії систем, у науковому синтезі їх – теорії організації систем управління – формування цілеспрямованих, керованих систем (у тому числі будь-яких практичних заходів) передбачає визначення елементів системи та осмислення проблематики предметної галузі (її природу) в цілому.

На мою думку, провідними елементами системи інформаційної безпеки, у тому числі щодо захисту інформації в автоматизованих комп'ютерних системах, є такі найважливіші чинники [23, с. 144].

Суб'єкти – окремі люди, спільноти їх, різного роду організації, суспільство, держава, інші держави, союзи їх, світове співтовариство.

Об'єкт – правовідносини між суб'єктами (суспільні відносини), які визначаються за певними об'єктивно існуючими критеріями.

Суб'єктів щодо інформаційної безпеки можна поділити на кілька категорій:

- щодо правового статусу регулювання відносин: суб'єкти регулювання відносин та учасників відносин;

- щодо мети учасників правовідносин: правомірні учасники та правопорушники тощо.

Визначальними також є тектологічні (організаційні) критерії: організаційно-управлінські, організаційно-правові та організаційно-технічні (у числі останніх виокремлюють ще організаційно-технологічні) [25, с. 22].

У суспільно-правовому змісті правовідносини інформаційної безпеки щодо захисту інформації мають сутність організовування нормального (безпечного) функціонування інформаційних систем, у тому числі тих, технічну основу яких становлять засоби комп'ютерної техніки та базовані на них електронні інформаційні технології (у тому числі технології телекомунікації).

Провідна системна мета правовідносин – захист суспільних інформаційних відносин від негативних впливів соціальних, техногенних та природних (стихійних) впливів.

Залежно від науково-практичних потреб організаційної діяльності (організовування) принципи інформаційної безпеки можуть поділятися на групи другого та наступних порядків.

Загальний аналіз проблем організовування захисту інформації в автоматизованих комп'ютерних системах дає можливість визначити три агреговані організаційні моделі заходів:

- організація запобіжних заходів;

- організація блокування (протидії) реальним загрозам, що реалізуються;

- організація подолання наслідків загроз, які не вдалося блокувати або запобігти їм [26, с. 12].

Важливий елемент організації інформаційної безпеки – захисту інформації – поділ заходів на групи щодо протидії. У теорії і практиці майже однозначно виокремлюють три такі групи: активні засоби захисту (наприклад, розвідка, дезінформація, зашумлення тощо); пасивні засоби захисту (наприклад, встановлення екранів несанкціонованому витоку інформації тощо); комплексні засоби захисту (органічне поєднання названих груп).

Всі заходи організації інформаційної безпеки, у тому числі в умовах застосування автоматизованих комп'ютерних систем, базуються на знаннях і використанні певних фізичних явищ, що характеризують відповідні форми по–дання (виразу) інформації. Завдання організовування інформаційної безпеки щодо захисту інформації в автоматизованих системах визначаються за напрямком, протилежним до загроз безпеки. При реалізації заходів захисту інформації важливим аспектом є визначення і перевірка стану безпеки. За допомогою метрологічної діяльності з'ясовують рівень розробки і наявність відповідних засобів, норм і методик, які дають можливість оцінити якість функціонування системи захисту інформації, тобто визначити, чи задовольняє чинним нормам система захисту на певний момент часу [27, с. 36].

Формалізація норм і методів метрології стану безпеки об'єкта набуває втілення у відповідних нормативних актах. Застосовуючи визначені в них нормативи слід враховувати природну властивість таких нормативів з часом втрачати актуальність. Це пов'язано з тим, що в міру розвитку науково-технічного прогресу можуть змінюватися норми і методи контролю захищеності інформації у відповідному середовищі її існування. Практика свідчить, що, як правило, норми і методи контролю мають тенденцію до удосконалення. Попередні нормативи

виступають як орієнтири, точки опори для формування нових нормативів. Сама назва "норматив" свідчить про те, що є фундаментальні межі можливостей існуючих фізичних приладів метрології на певному етапі пізнання людством законів природи [28, с. 140].

1.3. Нормативно-правові аспекти захисту інформації на підприємстві

Правове становище підприємств в українському законодавстві, що почало формуватися після здобуття Україною державної незалежності, вперше було визначено Законом України від 27.03.1991 р. "Про підприємства в Україна", більшість положень якого була врахована при розробці Господарського кодексу України (набув чинності з 01.01.2004 р.). Слід зазначити, що в новому Цивільному кодексі поняття підприємства дається в главі 12 "Загальні положення про об'єкти цивільних прав" у ст. 191 "Підприємство як єдиний майновий комплекс". Відповідно до цієї статті "підприємство є єдиним майновим комплексом, що використовується для здійснення підприємницької діяльності", і як така є сукупністю нерухомих і рухомих речей, майнових та інших прав, а також може бути в цілому чи в частині об'єктом купівлі-продажу, застави, оренди та інших правочинів. На відміну від Цивільного кодексу, Господарський кодекс (статті 62-72) визначає підприємство самостійним суб'єктом господарювання, якому притаманні такі риси:

- належність до основної ланки економіки;

-безпосереднє здійснення виробничої, науково-дослідницької і комерційної діяльності та іншої господарської діяльності - як комерційної (підприємницької), так і некомерційної;

- можливість функціонування на будь-якій формі власності:

державній (державні та казенні підприємства), комунальній (комунальні

підприємства), колективній (підприємства у формі виробничих кооперативів, господарських товариств, колективних підприємств), приватній (приватні підприємства);

- установчий документ – зазвичай статут, якщо інше не встановлено законом (так, для підприємств, що діють у формі повного чи командитного товариства, установчим документом буде засновницький договір - ч. 1 ст. ГК 82);

- функціонування на базі відокремленого майна, що знаходить вираз у наявності самостійного балансу та рахунку в банку, це майно може бути закріплено за підприємством на праві власності (підприємства у формі господарських товариств і виробничих кооперативів, приватне підприємство, якщо засновник (власник майна) сам (без найманого керівника) управляє цим підприємством), праві господарського відання (державні підприємства, комунальні підприємства, приватні підприємства з найманим керівником, а також підприємства громадських, релігійних, кооперативних організацій, якщо засновник застосував цей правовий титул при закріпленні за підприємством виділеного йому майна), праві оперативного управління (казенні підприємства, а також інші унітарні - зазвичай некомерційні - підприємства, якщо власник для закріплення за останніми майна обирає цей правовий титул), праві користування (може застосовуватися як додатковий правовий титул до одного з вищеназваних, як це має місце, наприклад, в орендному підприємстві);

- індивідуалізація підприємства як самостійного суб'єкта господарювання забезпечується наявністю у нього власного найменування (фірмової назви), що відображається в його вихідних документах, печатці; як платник податку підприємство повинно мати ідентифікаційний код;

- ступінь самостійності підприємства (обсяг його прав та обов'язків) залежить від правового режиму майна підприємства:

- щодо підприємств – невласників (правовий титул майна такого

підприємства або право повного господарського відання, або право оперативного управління) стратегічні питання створення та діяльності таких підприємств вирішуються власниками їхнього майна (їх представниками), які затверджують статут підприємства, призначають його керівника, визначають правовий титул майна та межі майнової самостійності підприємства, в т. ч. порядок використання його прибутку, вирішують питання реорганізації та ліквідації підприємства тощо. Частина питань погоджується з власником майна (створення філій, представництв підприємства, випуск облігацій підприємства тощо). Лише деякі питання вирішуються підприємством самостійно (формування виробничої програми, прийняття (неприйняття) державного замовлення, встановлення господарських зв'язків, наймання та звільнення працівників, організація виробничого процесу і т; ін.). Таке підприємство має додаткові обов'язки, крім вже названих: виконувати вказівки власника або погоджувати з ним питання діяльності підприємства у передбачених законом Та статутом підприємства випадках (якщо це не суперечить вимогам законодавства), відраховувати власникові визначену ним частину чистого прибутку підприємства; використовувати закріплене за підприємством майно лише в межах, визначених законом та статутом підприємства [29, с. 188].

Відповідно до ч. 1 ст. 55 Господарського кодексу України суб'єктами господарювання визнаються учасники господарських відносин, які здійснюють господарську діяльність, реалізуючи господарську компетенцію (сукупність господарських прав та обов'язків), мають відокремлене майно і несуть відповідальність за своїми зобов'язаннями в межах цього майна, крім випадків, передбачених законодавством.

Стаття 56 Господарського кодексу України визначає загальні засади створення суб'єкта господарювання, в т. ч. правові підстави, форми створення, необхідність додержання вимог чинного законодавства.

Суб'єкт господарювання створюється і діє на підставі установчих документів

(документа), які мають відповідати встановленим вимогам. Загальні вимоги до установчих документів визначаються ст. 57 Господарського кодексу України, а спеціальні – в законах, які визначають особливості правового статусу суб'єктів господарювання з виключними видами діяльності: "Про банки і банківську діяльність" (статті 17-18, 22)); "Про цінні папери і фондову біржу" (ст. 34); "Про державне регулювання ринку цінних паперів в Україні" (пункти 13-14 ч. 2 ст. 7); "Про інститути спільного інвестування (пайові та корпоративні інвестиційні фонди)" (статті 9, 23-24), "Про страхування" (статті 2, ЗО, 31) та ін.

Загальні вимоги щодо установчих документів стосуються:

- видів установчих документів: рішення про утворення суб‘єкта господарювання (приймається при створенні господарської організації унітарного типу), засновницький договір (укладається у разі заснування суб'єкта господарювання двома і більше особами), статут (приймається в передбачених законом випадках – при створенні підприємства; господарських товариств, що належать до об'єднань капіталів; виробничого кооперативу), положення (філії, представництва, інші відокремлені підрозділи господарських організацій зі статусом юридичної особи);

- змісту установчих документів (в них мають бути зазначені найменування та місцезнаходження суб'єкта господарювання, мета і предмет господарської діяльності, склад і компетенція його органів управління, порядок прийняття ними рішень, порядок формування майна, розподілу прибутків та збитків, умови його реорганізації та ліквідації, якщо інше не передбачено законом);

- спеціальні вимоги до засновницького договору, статуту, положення.

У засновницькому договорі засновники зобов'язуються утворити суб'єкт господарювання, визначають порядок спільної діяльності щодо його утворення, умови передачі йому свого майна, порядок розподілу прибутків і збитків, управління діяльністю суб'єкта господарювання та участі в ньому засновників,

порядок вибуття та входження нових засновників, інші умови діяльності суб'єкта господарювання, які передбачені законом, а також порядок його реорганізації та ліквідації відповідно до закону; статут суб'єкта господарювання повинен містити відомості про його найменування і місцезнаходження, мету і предмет діяльності, розмір і порядок утворення статутного та інших фондів, порядок розподілу прибутків і збитків, про органи управління і контролю, їх компетенцію, про умови реорганізації та ліквідації суб'єкта господарювання, а також інші відомості, пов'язані з особливостями організаційної форми суб'єкта господарювання, передбачені законодавством); положенням визначається господарська компетенція органів державної влади, органів місцевого самоврядування, відокремлених підрозділів господарської організації зі статусом юридичної особи [32, с. 41].

Права та обов'язки суб'єктів господарювання можна поділити на дві категорії – загальні права та обов'язки, які притаманні всім суб'єктам господарювання, і спеціальні – які характерні лише для певних видів суб'єктів господарювання.

Спеціальні права необхідні суб'єктам господарювання з виключними видами діяльності (банківські операції, страхування, спільне інвестування, біржові операції) і передбачаються у відповідних законах – "Про банки і банківську діяльність" (ст. 9 – право комерційних банків створювати та брати участь у банківському об'єднанні, ст. 47 – право здійснювати на підставі банківської ліцензії банківські операції та ін.), "Про страхування" (статті 3,10–11 – право страховиків здійснювати на договірних засадах страхування, співстрахування, перестрахування; ст. 12 – право створювати та брати участь в об'єднаннях страховиків; ст. 14 – право здійснювати страхування через страхових посередників (страхових агентів і страховик брокерів).

Загальні обов'язки суб'єктів господарювання досить численні, а саме:

- дотримуватися вимог антимонопольного – конкурентного законодавства;
- вести бухгалтерський облік і звітність;

- сплачувати податки та інші обов'язкові платежі;

- забезпечувати безпеку виробництва (екологічну, пожежну, радіаційну, санітарно-епідеміологічну, щодо охорони праці тощо);

- не порушувати права та законні інтереси інших осіб;

- виконувати інші вимоги, передбачені законодавством. Спеціальні Обов'язки притаманні для суб'єктів господарських правовідносин із спеціальним (виключним) предметом діяльності. Такі комерційні банки, страхові компанії, інститути спільного інвестування зобов'язані дотримуватися вимог відповідних законів щодо розміру та складу майна, видів діяльності (операцій), контролю за використанням активів та ін. [35, с. 87].

Основні засади припинення діяльності суб'єктів господарювання визначаються Господарським кодексом України (статті 59-Є1), а спеціальні –законами, що визначають особливості правового статусу суб'єктів господарювання зі спеціальним (виключним) видом діяльності.

Основні засади, закріплені в Господарському кодексі України, передбачають:

- форми припинення (реорганізація шляхом злиття, приєднання, поділу, перетворення чи ліквідація);

- принцип публічності прийняття рішення про припинення діяльності суб'єкта господарювання (оголошення про реорганізацію чи ліквідацію господарської організації або припинення діяльності індивідуального підприємця підлягає опублікуванню реєструючим органом у спеціальному додатку до газети "Урядовий кур'єр" та/або в офіційному друкованому виданні органу державної влади або органу місцевого самоврядування за місцезнаходженням суб'єкта господарювання протягом десяти днів з дня припинення діяльності суб'єкта господарювання – ч. 8 ст. 59 ГК);

- форми захисту інтересів кредиторів (щодо реорганізації визначення правонаступників суб'єкта господарювання, який Припиняє свою діяльність в

результаті реорганізації; щодо ліквідації встановлення порядку ліквідації та задоволення вимог кредиторів (задоволення претензій кредиторів з майна суб'єкта господарювання, що ліквідується; повернення майна. Що залишилося після задоволення претензій кредиторів, його власникові (учасникам суб'єкта господарювання, що ліквідується). Стаття 112 ЦК більш ґрунтовно регулює питання задоволення вимог кредиторів, встановлюючи черговість (чотири черги). Спеціальні порядки черговості встановлюються законами: "Про відновлення платоспроможності боржника або визнання його банкрутом" (ст. 31); "Про інституту спільного інвестування (пайові та корпоративні інвестиційні фонди)" (частини 2–4 ст. 21) [36, с. 190].

Питання припинення діяльності суб‘єктів господарювання, крім статей 59-61 Господарського кодексу, регулюються Цивільним кодексом (стосовно юридичних осіб - статті 104–112), а також низкою законів: "Про банки і банківську діяльність" (статті 26, 28, 87–98); "Про цінні папери і фондову біржу" (ст. 36); "Про інститути спільного інвестування (пайові та корпоративні інвестиційні фонди)" (статті 20–21); "Про страхування" (ст. 43); "Про відновлення платоспроможності боржника або визнання його банкрутом" (статті 22–34) та ін.

У контексті проблематики слід звернути увагу на стан правового регулювання питань захисту інформації, зумовлюваний в Україні такими чинниками:

- нормативною невизначеністю понять та категорій, зокрема на рівні юридичних актів (документів);

- недосконалістю правового регулювання в інформаційній сфері, зокрема у сфері захисту таємниць (крім державної), конфіденційної інформації та відкритої інформації, важливої для особи, суспільства та держави;

- недостатністю нормативно–правових актів і нормативних документів з питань проведення досліджень, розроблення та виробництва засобів забезпечення захисту;

- незавершеністю створення системи сертифікації засобів забезпечення

технічного захисту інформації (ТЗІ);

- недосконалістю системи атестації на відповідність вимогам ТЗІ об'єктів, робота яких пов'язана з інформацією, що підлягає технічному захисту;

- недостатньою узгодженістю чинних в Україні нормативно–правових актів та нормативних документів з питань ТЗІ з відповідними міжнародними договорами України [38, с. 163].

З аналізу нормативно-правової бази захисту інформації в автоматизованих системах впливає, що в сучасних умовах важливе значення щодо захисту інформаційних відносин надається створенню системи технічного захисту інформації. У публічному праві України під системою ТЗІ розуміють сукупність суб'єктів, об'єднаних цілями та завданнями захисту інформації інженерно–технічними заходами, нормативно-правову та матеріально–технічну базу.

Система організації технічного захисту інформації – це множина комплексних заходів, що здійснюються визначеними в нормативних актах, на основі наявної матеріально–технічної бази, відповідними суб'єктами, об'єднаних цілями та завданнями захисту інформації інженерно-технічними засобами.

Система ТЗІ –це множина інженерно-технічних засобів, що визначають заходи на основі наявної матеріально-технічної бази у суб'єктів, об'єднаних цілями та завданнями захисту інформації у порядку, визначеному у відповідних нормативно-правових документах (законах та підзаконних актах).

З аналізу чинного законодавства та підзаконних нормативних актів можна зробити узагальнення, що в Україні є національна система правового регулювання захисту інформації в автоматизованих системах. Правову основу забезпечення захисту інформації в Україні як інституції права становлять Конституція України, Концепція (основи державної політики) національної безпеки України, закони України "Про інформацію", "Про захист інформації в автоматизованих системах", "Про державну таємницю", "Про науково-технічну інформацію", інші нормативно-

правові акти, в тому числі міжнародні договори України (які відповідним чином ратифіковані Україною), що стосуються сфери інформаційних відносин [39, с. 51].

Виходячи із зазначеного, можна зробити висновок, що проблематика захисту інформації в автоматизованих системах у науці й практиці України перебуває на стадії становлення і потребує ґрунтовного наукового забезпечення, зокрема систематизації, в тому числі на рівні організаційно-правового аспекту.

У зв'язку з цим є потреба формування комплексної наукової дисципліни теорії організації (тектології) інформаційної безпеки, а в її складі – субінституту захисту інформації в автоматизованих системах [40, с. 16].

РОЗДІЛ 2
АНАЛІЗ РОБОТИ ТОВАРИСТВА З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ СПІЛЬНОГО ПІДПРИЄМСТВА «ПОЛТАВСЬКА ГАЗОНАФТОВА КОМПАНІЯ» ТА ОЦІНКА МОЖЛИВИХ ПРИЧИН ВИНИКНЕННЯ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

2.1 Характеристика діяльності товариства з обмеженою відповідальністю спільного підприємства «Полтавська газонафтова компанія»

Спільне підприємство «Полтавська газонафтова компанія» (СП ПГНК), спільне українсько-британське підприємство, було створене у 1994 році. СП ПГНК є лідером серед недержавних нафтогазовидобувних підприємств України. Сфера діяльності компанії – пошук, розвідка, видобуток та переробка нафти та газу. Серед наших основних задач: соціальна відповідальність, запровадження інноваційних технологій і передового досвіду у нафтогазовій галузі.

Спільне підприємство ПГНК у своїй діяльності дотримується міжнародних етичних стандартів та повністю задовольняє вимоги охорони праці, навколишнього середовища та безпеки. Полтавська газонафтова компанія, використовуючи найсучасніші технології і методи, робить свій внесок у досягнення Україною енергетичної незалежності.

Метою діяльності спільного підприємства «Полтавська газонафтова компанія» є задоволення потреб ринку у продукції, роботах та послугах, розширення їх асортименту, підвищення конкурентоспроможності, ефективне управління майном, що належить Товариству, одержання прибутку, його використання та/або розподіл для розвитку Товариства, забезпечення інтересів акціонерів Товариства і задоволення економічних інтересів і соціальних потреб працівників.

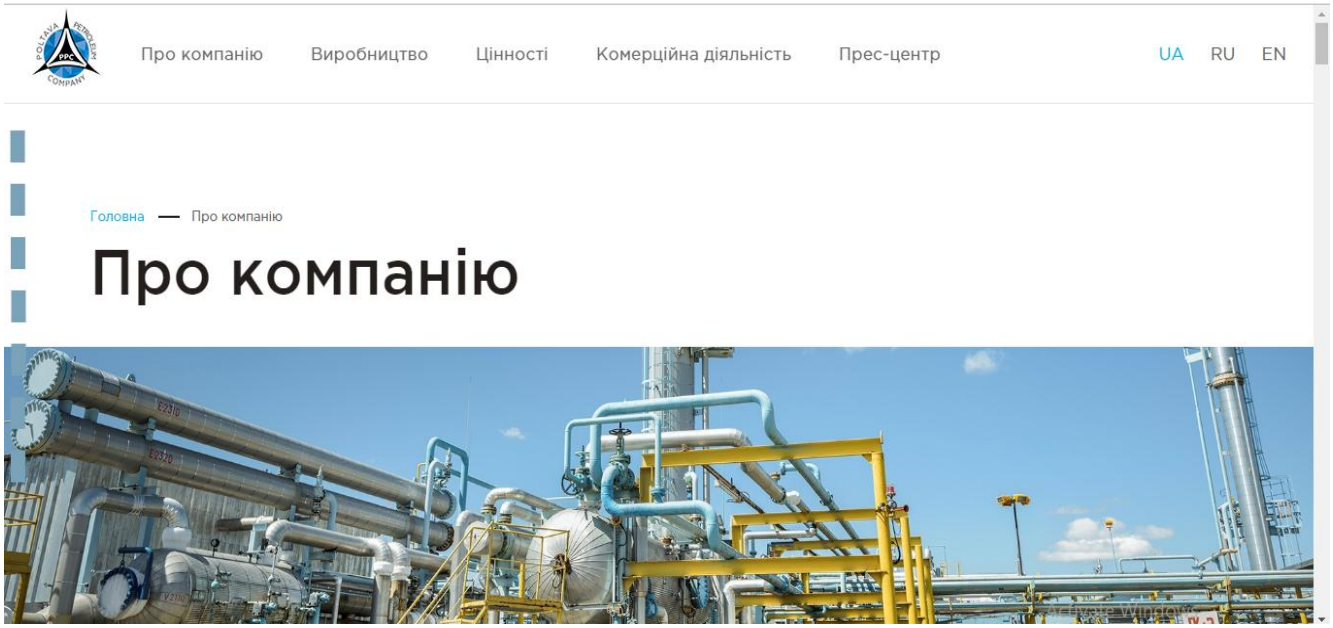

Рисунок 2.1 – Сайт спільного підприємства «Полтавська газонафтова компанія»»

СП ПГНК зареєстровано у формі товариства з обмеженою відповідальністю. Засновники: британська нафтогазова компанія „JP Kenny Exploration & Production Ltd.” і два українські підприємства – „Полтавагазпром” і “Полтаванафтогазгеологія”.

Отримали ліцензію на пошук і розвідку на Новомиколаївській площі та ліцензії на експлуатацію чотирьох родовищ.

Предметом діяльності Товариства є:

– видобування нафти і газу;

– проектування, будівництво, розширення, реконструкція, технічне переозброєння і капітальний ремонт електричних мереж, будівель, споруджень, машин і механізмів;

– надання побутових послуг населенню та виробництво товарів народного споживання;

– комерційно-посередницька діяльність, що сприяє меті діяльності Товариства;

– зовнішньоекономічна діяльність,

– надання юридичних послуг;

– добування газу та нафти;

– газопостачання;

– транспортування, зберігання, постачання природного газу та нафти;

– постачання холодної, гарячої води та водовідведення, в тому числі централізоване;

– постачання і передача тепла;

– надання послуг з освітлення;

– надання послуг у житлово-експлуатаційній сфері, в тому числі з централізованого опалення;

– утримання будинків і споруд та прибудинкових територій, в тому числі: прибирання внутрішньобудинкових приміщень та прибудинкової території, санітарно-технічне обслуговування, обслуговуваннявнутрішньобудинкових мереж, утримання ліфтів, поточний і капітальний ремонт, заміна та підсилення елементів конструкцій та мереж, їх реконструкція, відновлення несучої спроможності несучих елементів конструкцій, вивезення побутових відходів;

– експлуатація водосховищ, водогосподарських каналів, меліоративних систем, гідротехнічних споруд та надання відповідних послуг;

– надання медичних послуг;

– оптова та роздрібна торгівля промисловими та продовольчими товарами власного, вітчизняного та іноземного виробництва, включаючи реалізацію паливно-мастильних матеріалів, сировинних ресурсів, автотранспорту, торгівлю

алкогольними напоями та тютюновими виробами, сільськогосподарською продукцією;

– заготівля та закупка готової продукції, сировини та напівфабрикатів у виробників, в тому числі й за готівковий рахунок, а також шляхом форвардних контрактів та опціонних угод;

– організація робіт з питань охорони праці, техніки безпеки, впровадження безпечних методів роботи в процесі виробничо-господарської діяльності;

– емісія, покупка, продаж цінних паперів [61].

Спільного підприємства «Полтавська газонафтова компанія»» має складну організаційну структуру, її умовно можна поділити на структуру органів управління, структуру правління (рис.2.1)

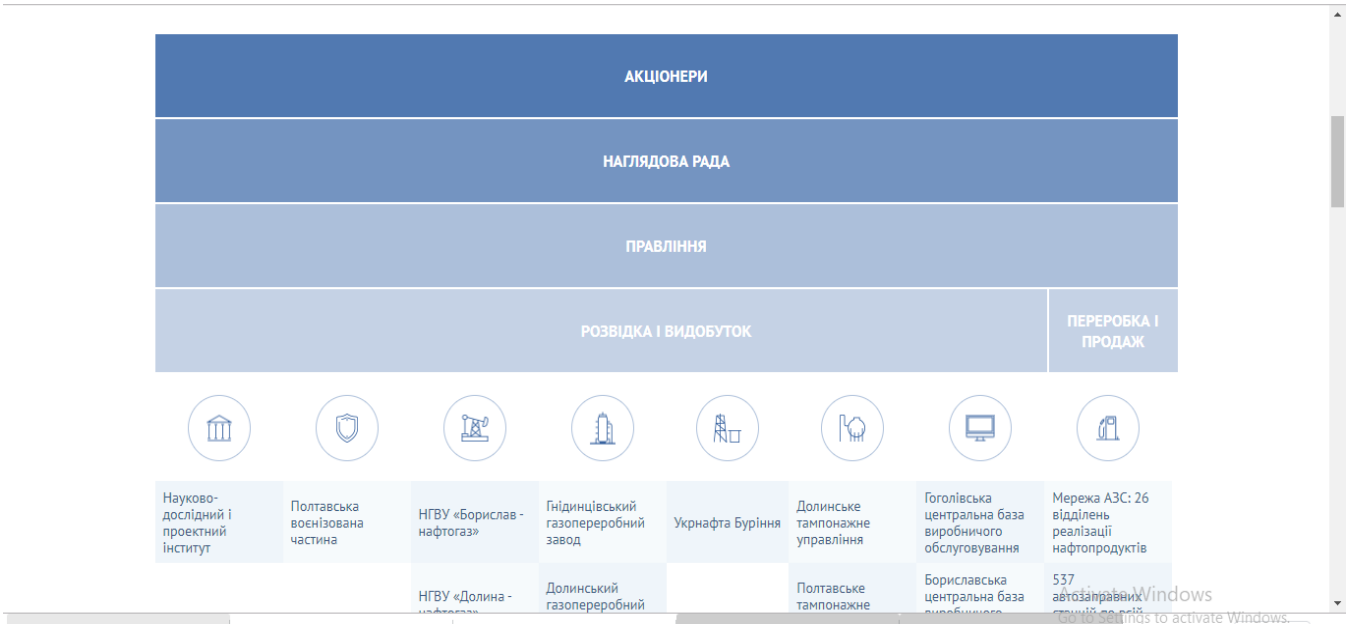

Рисунок 2.2 – Загальна структура «Спільного підприємства «Полтавська газонафтова компанія»», складено автором за даними підприємства

Товариство самостійно планує напрямки діяльності та здійснює господарську, у тому числі зовнішньоекономічну, діяльність, використовує грошові кошти у національній та іноземній валюті згідно з вимогами законодавства.

Відносини між Товариством та іншими юридичними особами (підприємствами, установами, організаціями) та фізичними особами в усіх сферах господарської діяльності здійснюються на основі договорів [61].

Оскільки підприємство є публічним акціонерним, то і вся інформація висвітлюється на сайті «Спільного підприємства «Полтавська газонафтова компанія»» для акціонерів та користувачів.На сайті можна знайти: установчі документи товариства такі як: статут, положення про загальні збори акціонерів, про наглядову раду, про Правління, про ревізійну комісію, про кожну з філій, протоколи загальних зборів, свідоцтво про державну реєстрацію випуску акцій, особливу інформацію про Товариство. Із сайту можна звернутися до Кол-центру або до інформаційно-консультаційного центру, який працює цілодобово, зареєструватися на сайті для отримання інформації для побутових споживачів, переглянути останні новини, графіки аварійних відключень. Також на сайті є інтерактивна карта «Організаційна структура» (додаток Е). Можна перейти на вкладку «Ваша абонентська книжка», що надає споживачеві доступ до свого особового рахунку через Інтернет, де споживач без зусиль може отримати всю інформацію по особовому рахунку, передати покази лічильника або провести звірку, сплатити заборгованість за спожиту електроенергію [61].

На кожному підприємстві діловодство займає провідне місце у роботі апарату управління і «Спільного підприємства «Полтавська газонафтова компанія»» не виняток, оскільки це діяльність, яка охоплює питання документування і організації роботи з документами в процесі здійснення управлінських дій. Тобто діловодство впорядковує роботу з документами, носіями інформації на підприємстві, забезпечуючи економію ресурсів управлінської ланки [22].

Основним завданням служби діловодства в «Спільного підприємства «Полтавська газонафтова компанія»» є встановлення порядку документування і роботи з документами на підприємстві з використанням сучасної комп'ютерної техніки, автоматизації технологічних процесів оброблення документів та скорочення кількості документів.

Служба діловодства виконує такі функції:

– реалізовує державну політику з організації діловодства в межах товариства;

– розробляє і впроваджує індивідуальну інструкцію з діловодства та зведену номенклатуру справ підприємства;

– забезпечує документацій не та організаційно-технічне обслуговування роботи колегіальних органів;

– організовує підготовку проектів організаційно-розпорядчих документів, забезпечує їх оформлення і видання;

– бере участь у розробленні, впровадженні та виконанні системи електронного діловодства та електронного документообігу в установі;

– здійснює контроль за підготовкою документів у структурних підрозділах та їх своєчасного виконання;

– здійснює приймання, реєстрацію, облік, поточне зберігання, оперативних пошук, доставку документів та інформування за ними;

– організовує забезпечення збереженості документального фонду установи;

– здійснює організаційно-методичне керівництво роботою з документами в структурних підрозділах;

– організовує підвищення кваліфікації працівників служби діловодства[2, с. 67].

Підприємство має велику кількість партнерів.

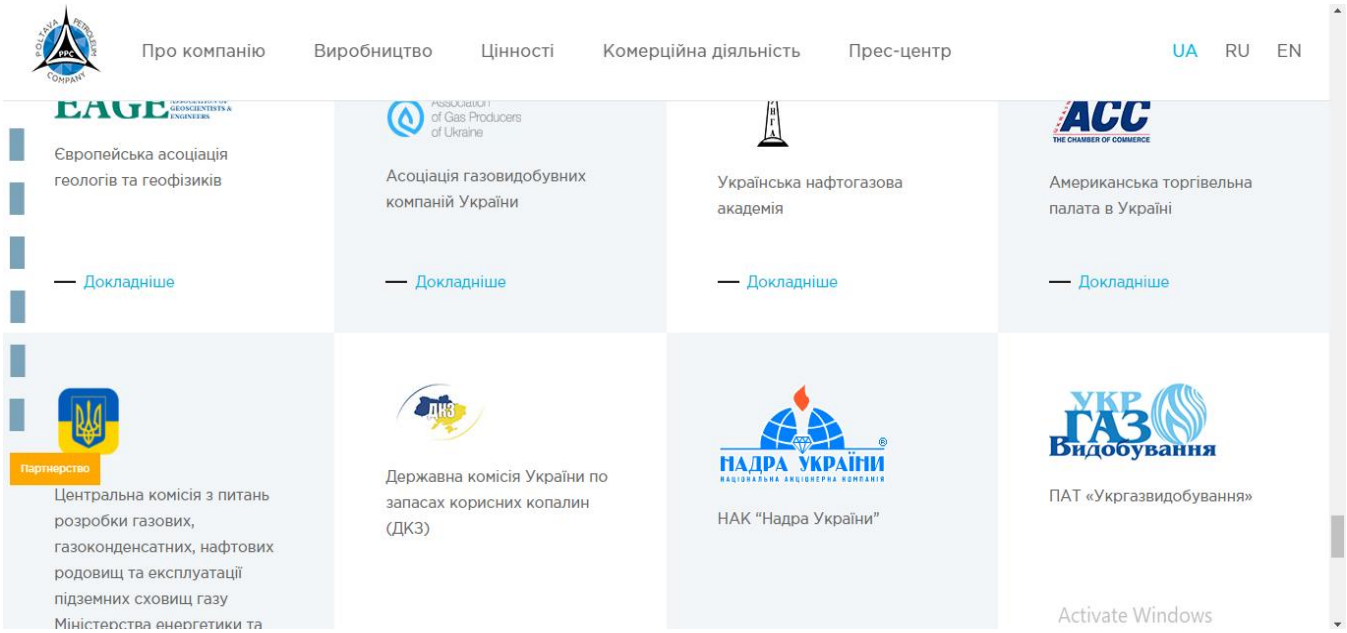

Рисунок 2.3 – Партнери компанії

ПАТ «Укрнафта» володіє 85 спеціальними дозволами на видобування (промислову розробку родовищ) вуглеводнів.

Видобуток нафти та газу здійснюють шість нафтогазовидобувних управлінь: «Охтирканафтогаз», «Полтаванафтогаз», «Чернігівнафтогаз» у Дніпровсько-Донецькій западині та «Бориславнафтогаз», «Долинанафтогаз», «Надвірнанафтогаз» у Передкарпатському прогині.

Станом на кінець 2018 р. «Укрнафта» експлуатувала 1928 нафтових та 165 газових свердловин (включаючи основну та спільну діяльність).

У 2018 р. ПАТ «Укрнафта» видобула 1,4 млн т нафти та конденсату і 1,1 млрд м3 газу.

В «Спільного підприємства «Полтавська газонафтова компанія»» реєстрація та контроль за виконанням документів відбувається в системі «Мотив», що дає змогу раціонально використовувати робочий час.

Реєстрації підлягають усі документи, що потребують обліку, виконання і подальшого використання в довідкових цілях. Документи реєструються один раз. Реєстрація здійснюється в межах груп залежно від назви виду документа, підрозділу і змісту[28].

Контроль здійснюється за виконанням усіх зареєстрованих документів у яких встановлено завдання, а також виконання яких підлягає обов'язковому контролю, за переліком документів затверджених керівником підприємства.

Отже, відбувається якісний контроль за виконанням документів, оскільки керівник слідкує за ходом виконання поставлених задач в системі.

В «Спільного підприємства «Полтавська газонафтова компанія»» є паперовий та електронний документообіг – це сукупність процесів створення, оброблення, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності та у разі необхідності з підтвердженням факту одержання таких документів [48, с. 4]. Електронний документообіг представлено системою оперативного управління підприємством «Мотив» – це система електронного документообігу, система контролю доручень, система управління проектами та CRM-система .

Система «Мотив» створює єдиний інформаційний простір організації: користувачі ведуть спільну роботу над документами і обговорюють їх в режимі реального часу. Документи, що надходять на підприємство направляють до керівництва на розгляд, після накладення резолюції за допомогою системи «Мотив» в електронному вигляді відправляють до виконавців [37].

Таким чином оптимізовано бізнес-процеси. Процес узгодження документа прискорився; зросла виконавча дисципліна, так як працівник не має права не виконати задачу, бо це контролюється керівником; документи не втрачаються у процесі роботи з ними; можна здійснювати оперативний пошук документів за певний період.

2.2 Основні принципи та методи захисту інформаційних процесів в спільному підприємстві «Полтавська газонафтова компанія»

Організаційно групи служби інформаційної безпеки в «Спільного підприємства «Полтавська газонафтова компанія»» відокремлені від всіх відділів або груп, що займаються управлінням самою системою, програмуванням та іншими відносяться до системи завданнями щоб уникнути можливого зіткнення інтересів.

Для ефективної роботи служби інформаційної безпеки в ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» надається адміністративна підтримка, яка полягає у відображенні основних положень прийнятої політики безпеки у відповідних інструкціях і розпорядженнях. У них в першу чергу в ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» визначені:

- посадові обов’язки груп користувачів;
- правила доступу (розмежування доступу) до інформації;
- заходи щодо забезпечення контролю та функціонування системи захисту інформації;
- заходи реагування на порушення режиму безпеки;
- планування та організація відновлювальних робіт.

Для забезпечення успішної роботи СІБ в ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» визначені права і обов’язки служби, а також правила її взаємодії з іншими підрозділами з питань захисту інформації на об’єкті.

Ефективний захист економічних інтересів підприємства може бути забезпечений лише у разі об’єднання зусиль її персоналу: адміністрації, інженерно-технічних працівників, службовців, робітників.

Комплексність підходів до інформаційної безпеки та пов’язаних з нею проблем зумовлює обов’язкове виділення особливої діяльності, що закладає інтелектуальні підвалини успішного розвитку національних інформаційних систем. Такою

діяльністю є професійна освіта та організація наукових досліджень у галузі інформаційної діяльності, визначена ст.15 та ст.16 Закону України «Про інформацію» [50].

Напрями забезпечення безпеки – це нормативно-правові категорії, що визначають комплекстні заходи захисту інтересів комерційного підприємства. Модель забезпечення інформаційної безпеки підприємства ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» зображено в додатку Ж.

ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» як система має певні структурні ланки:

- органи управління підприємством;
- бухгалтерію;
- відділи – функціональні ланки підприємства;
- допоміжні служби;
- службу безпеки.

Кожна структурна ланка в ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» має свої функціональні обов'язки і вирішує своє конкретне завдання. Водночас кожна структурна ланка і кожен співробітник працюють для досягнення загальної мети: підвищення добробуту підприємства, збільшення його прибутку. Від того, як буде реалізована ця мета, залежатиме їх особисте благополуччя, їх особистий прибуток.

Система захисту інформації на ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» представляє собою комплекс організаційних, технічних і технологічних засобів, методів і мір, які перешкоджають несанкціонованому (незаконному) доступу до інформації [18, с. 44].

Система захисту інформації в ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» є багаторівневою з ієрархічним доступом до інформації, гранично конкретизована і прив'язана до специфіки підприємства по структурі

методів та засобів захисту, що використовуються, відкритою для регулярного оновлення, надійної як в звичайних, так і в екстремальних ситуаціях. СЗІ не повинна створювати співробітникам підприємства серйозні незручності в роботі. Комплексність системи захисту досягається її формуванням з різних елементів – правових, організаційних, технічних та програмно-математичних [17, с. 34].

Елемент правового захисту інформації в ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» передбачає: наявність в засновницькій та організаційних документах підприємства, контрактах, що укладаються із співробітниками, і в посадових інструкціях положень та зобов'язань по захисту відомостей, що складають таємницю підприємства і її партнерів, формулювання і доведення до відома всіх співробітників підприємства механізму правової відповідальності за розголошення конфіденційних відомостей. В правовий елемент системи захисту може також включатись страхування цінної інформації від різних ризиків [17, с. 35].

Елемент організаційного захисту інформації в ТОВ «Спільного підприємства «Полтавська газонафтова компанія»»містить міри управлінського та обмежувального характеру, які спонукають персонал дотримуватися правил захисту конфіденційної інформації і включає в себе: формування і регламентацію діяльності служби безпеки підприємства, забезпечення цієї служби нормативно-методичними документами по організації і технології захисту інформації; регламентацію та регулярне оновлення переліку (списку) цінної, конфіденційної інформації, яка підлягає захисту, складання і ведення переліку конфіденційних документів підприємства; регламентацію системи (ієрархічної схеми) обмеження доступу персоналу до конфіденційної інформації; регламентацію технології захисту і обробки конфіденційних документів підприємства; побудова захищеного традиційного або електронного документообігу; побудова технології документування цінної інформації, складання, оформлення, виготовлення і

видавництва конфіденційних документів; побудова технологічної системи обробки і збереження конфіденційних; документів; організацію архівного зберігання конфіденційних документів; регламентацію захисту цінної інформації підприємства від несанкціонованих дій персоналу; порядок і правила роботи персоналу з конфіденційними документами і інформацією, контроль за виконанням всіма співробітниками цього порядку і правил; відбір персоналу для роботи з конфіденційною інформацією, навчання та інструктування співробітників; порядок захисту інформації при веденні переговорів, проведенні нарад по конфіденційним питанням, прийомі відвідувачів, здійснення рекламної, виставочної та іншої діяльності; регламентацію аналітичної роботи по виявленню загроз цінній інформації підприємства і каналів витоку інформації; обладнання і атестацію приміщень і робочих зон, виділених для здійснення конфіденційної діяльності, ліцензування технічних систем і засобів захисту інформації та охорони; регламентацію пропускного режиму на території, в будівлях і приміщеннях підприємства, ідентифікацію персоналу та вантажу; регламентацію системи охорони території, будівлі, приміщень, обладнання, грошових засобів, транспорту і персоналу підприємства; регламентацію організаційних питань експлуатації технічних засобів захисту інформації і охорони; регламентацію дій служби безпеки і персоналу в екстремальних ситуаціях; регламентацію роботи по управлінню системою захисту інформації підприємства [17, с. 36].

Елемент технічного захисту в ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» включає: засоби захисту технічних каналів витоку інформації, що виникають під час роботи персональних комп’ютерів, засобів зв’язку, копіювальних апаратів, принтерів, факсів та інших приладів і обладнання; засоби захисту приміщень від візуальних та акустичних способів технічної розвідки; засоби охорони будівель і приміщень від проникнення сторонніх осіб (засоби спостереження, сповіщення, сигналізації, інформування і ідентифікації,

інженерні споруди); засоби протипожежної охорони; засоби виявлення приладів і пристроїв технічної розвідки (підслуховувальних та передавальних пристроїв,звукозаписувальної та телевізійної апаратури) [17, с. 38].

Елемент програмно-математичного захисту інформації в ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» включає: регламентацію доступу до електронних документів персональними паролями, що ідентифікуються командами та іншими найпростішими методами захисту; регламентацію спеціальних засобів і продуктів програмного захисту; регламентацію криптографічних методів засобів захисту інформації в ПК та мережах, криптографування (шифрування) тексту під час передачі їх по каналам звичайного та факсимільного зв'язку, під час листування поштою. В кожному елементі захисту можуть бути реалізовані на практиці тільки окремі складові частини [17, с. 39].

Джерела зовнішніх загроз ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» можуть бути випадковими і запланованими та мати різний рівень кваліфікації. До них відносяться:

- кримінальні структури;
- потенційні злочинці і хакери;
- нечесні партнери;
- технічний персонал постачальників послуг, тощо.

Внутрішні суб'єкти (джерела), як правило, представлені висококваліфікованими фахівцями у галузі розробки та експлуатації програмного забезпечення і технічних засобів, знайомі зі специфікою розв'язуваних завдань, структурою та основними функціями та принципами роботи програмно-апаратних засобів захисту інформації, мають можливість використання штатного устаткування і технічних засобів мережі[62, с. 94].

До них відносяться:

- основний персонал (користувачі, програмісти, розробники);

- представники служби захисту інформації;
- допоміжний персонал (прибиральники, охорона);
- технічний персонал.

Технічні засоби, що є джерелами потенційних загроз безпеці інформаціїТОВ «Спільного підприємства «Полтавська газонафтова компанія»», також можуть бути зовнішніми:

- засоби зв’язку;
- мережі інженерних комунікації;
- транспорт.

Та внутрішніми:

- неякісні технічні засоби обробки інформації;
- неякісні програмні засоби обробки інформації;
- допоміжні технічні засоби (охорони, сигналізації, телефонії);
- інші технічні засоби, що застосовуються в установі.

Відповідно, дії, які можуть завдати шкоди інформаційній безпеці організації, можна також розділити на кілька категорій:

- дії, які здійснюються авторизованими користувачами. У цю категорію потрапляють: цілеспрямована крадіжка або знищення даних на робочій станції або сервері; пошкодження даних користувачів у результаті необережних дій;
- «електронні» методи впливу, які здійснюються хакерами. До таких методів відносяться: несанкціоноване проникнення в комп’ютерні мережі, атака на відмову в обслуговуванні (DOS атаки);
- комп’ютерні віруси. Окрема категорія електронних методів впливу – комп’ютерні віруси та інші шкідливі програми. Проникнення вірусу на вузли корпоративної мережі може призвести до порушення їх функціонування, втрат робочого часу, втрати даних, викраденні конфіденційної інформації і навіть прямим розкраданням фінансових коштів. Вірусна програма, яка проникла в

корпоративну мережу, може надати зловмисникам частковий або повний контроль над діяльністю підприємства.

− «природні» загрози. На інформаційну безпеку компанії можуть впливати різноманітні зовнішні фактори. Так причиною втрати даних може стати неправильне зберігання, крадіжка комп'ютерів і носіїв, форс-мажорні обставини[62, с. 95].

Таким чином, у сучасних умовах наявність розвиненої системи інформаційної безпеки ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» стає однією з найважливіших умов конкурентоспроможності і життєздатності будь-якогопідприємства.

На сьогоднішній день існує великий арсенал методів забезпечення інформаційної безпекиТОВ «Спільного підприємства «Полтавська газонафтова компанія»»:

− засоби ідентифікації і аутентифікації користувачів;

− засоби шифрування інформації, що зберігається на комп'ютерах і що передається по мережах;

− міжмережеві екрани;

− віртуальні приватні мережі;

− засоби контентної фільтрації;

− інструменти перевірки цілісності вмісту дисків;

− засоби антивірусного захисту;

− системи виявлення вразливостей мереж і аналізатори мережевих атак.

Кожний з перерахованих засобів може використовуватись як самостійно, так і в інтеграції з іншими. Це робить можливим створення систем інформаційного захисту для систем будь-якої складності та конфігурації, незалежно від використовуваних платформ.

Ефективний засобом захисту від втрати конфіденційної інформації в ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» є фільтрація вмісту

вхідної і вихідної електронної пошти. Перевірка поштових повідомлень на основі правил, встановлених в організації, дозволяє також забезпечити безпеку компанії від відповідальності за судовими позовами і захистити їх співробітників від спаму.

Засоби контентної фільтрації вТОВ «Спільного підприємства «Полтавська газонафтова компанія»» дозволяють перевіряти файли всіх розповсюджених форматів, у тому числі стислі і графічні. При цьому пропускна здатність мережі практично не змінюється.

Всі зміни на робочій станції або на сервері ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» можуть бути відслідковані адміністратором мережі або іншим авторизованим користувачем завдяки технології перевірки цілісності вмісту жорсткого диска. Це дозволяє виявляти будь-які дії з файлами та ідентифікувати активність вірусів, несанкціонований доступ або крадіжку даних авторизованими користувачами. Контроль здійснюється на основі аналізу контрольних сум файлів (CRC сум).

Сучасні антивірусні технології, які використовує ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» дозволяють виявити практично всі вже відомі вірусні програми через порівняння коду підозрілого файлу із зразками, що зберігаються в антивірусній базі. Крім того, розроблені технології моделювання поведінки, що дозволяють виявляти новостворювані вірусні програми[62, с. 98].

Для протидії природним загрозам інформаційної безпеки в ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» має бути розроблений і реалізований набір процедур щодо запобігання надзвичайних ситуацій (наприклад, щодо забезпечення фізичного захисту даних від пожежі) та мінімізації збитків у тому випадку, якщо така ситуація все-таки виникне. Один з основних методів захисту від втрати даних – резервне копіювання з чітким дотриманням встановлених процедур (регулярність, типи носіїв, методи зберігання копій.

Основними принципами інформаційної безпеки в ТОВ «Спільного підприємства

«Полтавська газонафтова компанія»» є:

− забезпечення цілісності і збереження даних, тобто надійне їх зберігання в неспотвореному вигляді;

− дотримання конфіденційності інформації (її недоступність для тих користувачів, які не мають відповідних прав);

− доступність інформації для всіх авторизованих користувачів за умови контролю за всіма процесами використання ними отриманої інформації;

− безперешкодний доступ до інформації в будь-який момент, коли вона може знадобитися підприємству[30, с. 34].

Ці принципи неможливо реалізувати без особливої інтегрованої системи інформаційної безпеки., що виконує наступні функції:

− вироблення політики інформаційної безпеки;

− аналіз ризиків (тобто ситуацій, в яких може бути порушена нормальна робота інформаційної системи, а також втрачені або розсекречені дані);

− планування заходів щодо забезпечення інформаційної безпеки;

− планування дій в надзвичайних ситуаціях;

− вибір технічних засобів забезпечення інформаційної безпеки [30, с. 34].

Отже, етапи проведення робіт із забезпечення інформаційної безпеки в ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» виглядають таким чином:

− проведення обстеження підприємства на предмет виявлення реальних загроз несанкціонованого доступу до конфіденційної інформації;

− розробка політики безпеки, організаційно-розпорядчих документів і заходів щодо забезпечення інформаційної безпеки системи відповідно до вимог по захищеності технічних і програмних засобів від витоку конфіденційної інформації;

− проектування системи інформаційної безпеки;

− розробка зразка системи інформаційної безпеки;

− впровадження системи інформаційної безпеки в діючу структуру підприємства;

− навчання персоналу;

− атестація системи інформаційної безпеки підприємства[30, с. 35].

Отже, метою комплексної інформаційної безпеки в ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» є збереження інформаційної системи підприємства, захист і гарантування повноти і точності виданої нею інформації, мінімізація руйнувань і модифікація інформації, якщо такі трапляються.

Проте сама інформаційна безпека є достатньо абстрактним поняттям. Має бути деякий додаток інформаційної безпеки (ІБ), тобто необхідні систематизація і правила, що дозволяють зробити технології ІБ застосовними до реального середовища, де і повинна бути забезпечена безпека інформаційного простору. Тому й виникає поняття політики інформаційної безпеки.

2.3 Оцінка стану забезпечення захисту інформаційних процесів у пільному підприємстві «Полтавська газонафтова компанія»

На сьогоднішній день існує дві основні методики оцінки ризиків інформаційної безпеки: метод оцінки ризиків, оснований на побудові моделі загроз і вразливості та метод оцінки ризиків, оснований на побудові моделі інформаційних потоків.

Для проведення повного аналізу інформаційних ризиків, перш за все, необхідно побудувати повну модель інформаційної системи з точки зору ІБ. Для вирішення цього завдання використовується програма «Гриф», на відміну від досить громіздких представлених на ринку західних систем аналізу ризиків, має простий і інтуїтивно зрозумілий для користувача інтерфейс. Він має складний алгоритм

аналізу ризиків, що враховує більше ста параметрів, який дозволяє на виході дати точну оцінку існуючих в інформаційній системі ризиків, засновану на аналізі особливостей практичної реалізації інформаційної системи. Принцип роботи системи «Гриф» та можливі збитки через загрози конфіденційності, цілісності та доступності зображено в додатку И. Збиток повинен бути менше або дорівнює вартості інформації[6, с. 165].

Основне завдання системи «Гриф» – дати можливість ІТ-менеджеру самостійно (без залучення сторонніх експертів) оцінити рівень ризиків в інформаційній системі та ефективність існуючої практики по забезпеченню безпеки компанії, а також надати можливість доказово (в цифрах) переконати керівництво компанії в необхідності інвестицій у сферу її інформаційної безпеки.

Комплексний засіб «Гриф» здійснює аналіз ризиків інформаційної безпеки за допомогою побудови моделі інформаційної системи організації. Розглядаючи засоби захисту ресурсів з цінною інформацією, взаємозв’язок ресурсів між собою, вплив прав доступу груп користувачів, досліджується захищеність кожного виду інформації [6, с. 166].

Дана методика оцінки ризиків заснована на методі «Гриф», дозволяє змінювати основні характеристики інформаційних ресурсів і підбирати відповідні адекватні засоби захисту з урахуванням специфіки підприємства, не потребує спеціалістів івеликих затрат. Оцінка стану забезпечення інформаційної безпеки вТОВ «Спільного підприємства «Полтавська газонафтова компанія»» наведено в додатку Б.

Провівши дослідження стану інформаційної безпеки з використанням можливостей програми «Гриф» можна узагальнити, що рівень інформаційної безпеки знаходиться на достатньо високому рівні захисту. Недоліками в системі захисту інформації ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» є недостатня захищеність програмного забезпечення від хакерських

атак, оскільки підприємство використовує застарілі версії програм захисту своєї інформації[67, с. 284].

Інформаційно-аналітична робота вТОВ «Спільного підприємства «Полтавська газонафтова компанія»» – це одна із основних внутрішньовиробничих функціональні складових безпеки підприємства.

Інформаційна складова полягає у здійсненні ефективного інформаційно-аналітичного забезпечення господарської діяльності ТОВ «Спільного підприємства «Полтавська газонафтова компанія»».

Належні служби ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» виконують певні функції, які в сукупності характеризують процес створення та захисту інформаційної складової безпеки підприємства. До таких належать вТОВ «Спільного підприємства «Полтавська газонафтова компанія»»:

- збирання всіх видів інформації, що має відношення до діяльності того чи іншого суб'єкта господарювання;
- аналіз одержуваної інформації з обов'язковим дотриманням загальноприйнятих принципів і методів;
- прогнозування тенденцій розвитку науково-технологічних, економічних і політичних процесів;
- оцінка рівня економічної безпеки за всіма складовими та в цілому, розробка рекомендацій для підвищення цього рівня на конкретному суб'єкті господарювання;
- інші види діяльності з розробки інформаційної складової безпеки [38, с. 65].

На ТОВ «Спільного підприємства «Полтавська газонафтова компанія»»постійно надходять потоки інформації, що розрізняються за джерелами їхнього формування.

Заведено відокремлювати:

- відкриту офіційну інформацію;
- вірогідну нетаємну інформацію, одержану через неформальні контакти

працівників підприємства з носіями такої інформації;

− вірогідну нетаємну інформацію, одержану через неформальні контакти працівників підприємства з носіями такої інформації [38, с. 66].

Оперативна реалізація заходів з розробки та охорони інформаційної складової економічної безпеки вТОВ «Спільного підприємства «Полтавська газонафтова компанія»» здійснюється послідовним виконанням певного комплексу робіт за напрямками:

− збирання різних видів необхідної інформації;

− обробка та систематизація одержаної інформації;

− аналіз одержаної інформації;

− захист інформаційного середовища підприємства, що традиційно охоплює:

− заходи для захисту суб'єкта господарювання від промислового шпіонажу з боку конкурентів або інших юридичних і фізичних осіб;

− технічний захист приміщень, транспорту, кореспонденції, переговорів, різної документації від несанкціонованого доступу заінтересованих юридичних і фізичних осіб до закритої інформації;

− збирання інформації про потенційних ініціаторів промислового шпіонажу та проведення необхідних запобіжних дій з метою припинення таких спроб;

− зовнішня інформаційна діяльність [38, с. 67].

Основне завдання в ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» – збір інформації:

− про економічний стан підприємства, регіону, своєї країни, країн, в яких є партнери і т.д.;

− про політичну ситуацію в регіоні і країні;

− про морально-психологічний клімат в колективі;

− про конкурентів і методи конкуренції (добросовісною і недобросовісною);

− про кримінальні структури і можливі терористичні погрози;

− постановка завдань по перевірці потенційних партнерів, клієнтів, конкурентів;

− розробка програм протидії промисловому шпигунству, терористичним погрозам і іншим методам недобросовісної конкуренції;

− розробка програм дезінформації конкурентів:

− через засоби масової інформації;

− через інформаційно-телекомунікаційні канали;

− через постачальників, суміжників, партнерів, клієнтів;

− шляхом організації псевдопросочування конфіденційної інформації;

− розробка програм захисту конфіденційної інформації.

Першою і найважливішою операцією в ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» є аналіз, який служить додатковим фільтром, що відкидає непотрібне і що є захистом від шуму без підстави. Ця операція полягає перш за все у визначенні важливості, точності і значущості інформації. Інформація є важливою, якщо вона зв’язана, тобто має зв’язок з елементами бази, і якщо вона здатна внести внесок до організації. Коли внесок значимий і безпосередній, інформація вимагає термінових дій.

Інформація, що не має значення, в ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» виключається, щоб уникнути втрати часу і енергії. Не завжди легко встановити, є інформація достовірною або помилковою, особливо якщо вона містить відомості про події, які ще не відбулися.

Потреба в інформації варіюється залежно від здійснюваної або планованої діяльності в ТОВ «Спільного підприємства «Полтавська газонафтова компанія»». ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» може мати довгострокові (стратегічні) плани, тактичні або короткострокові, плани і поточні операції; всі вони вимагають добре вивіреної інформації. У широкому друці іноді намагалися змалювати ділову розвідку про конкурентів як «шпигунство».

Можливо, до деякої міри це дійсно так. Проте слід зазначити, що сьогодні переважна маса ділової інформації може бути отримана з відкритих джерел без порушення етичних норм [38, с. 65].

Для того, щоб розробити раціональну структуру служби інформаційної безпеки на ТОВ «Спільного підприємства «Полтавська газонафтова компанія»», достатню за складом і оснащення засобами безпеки, необхідно ретельно проаналізувати обрану політику безпеки, співвіднести ймовірні загрози і втрати в разі їх реалізації з ефективністю системи захисту інформації та фінансовими витратами на їх реалізацію. Тільки після цього керівництво підприємства зможе обґрунтовано прийняти рішення на створення відповідної служби інформаційної безпеки [3, с. 162].

До завдань служби безпеки ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» належать:

− визначення переліку відомостей, що становлять комерційну таємницю, а також кола осіб, які в силу займаного службового положення на підприємстві мають до них доступ;

− визначення ділянок зосередження відомостей, що становлять комерційну таємницю; технологічного обладнання, вихід з ладу якого (в тому числі уразливого в аварійному відношенні) може привести до великих економічних втрат;

− формування вимог до системи захисту в процесі створення і участь у проектуванні системи захисту, її випробування і приймання в експлуатацію;

− планування, організація та забезпечення функціонування системи захисту інформації [70, с. 120];

− розподіл між користувачами необхідних реквізитів захисту, включаючи установку (періодичну зміну) паролів, управління засобами захисту комунікацій і крипто захист зраджувати, збережених і оброблюваних даних;

− координація дій з аудиторською службою, спільне проведення аудиторських

перевірок, контроль функціонування системи захисту і її елементів, тестування системи захисту;

− організація навчання співробітників СІБ відповідно до їх функціональних обов'язків; навчання користувачів АС правилам безпечної обробки інформації;

− визначення кола підприємств, пов’язаних з даним кооперативними зв’язками, на яких можливий вихід з-під контролю відомостей, що становлять комерційну таємницю підприємства; виявлення осіб на підприємстві підприємств (у тому числі іноземних), зацікавлених в оволодінні комерційною таємницею;.

− розслідування відбулися порушень захисту, вжиття заходів реагування на спроби несанкціонованого доступу до інформації та порушенням правил функціонування системи захисту;

− виконання відновлювальних процедур після фактів порушення безпеки;

− вивчення, аналіз, оцінка стану та розробка пропозицій щодо вдосконалення системи забезпечення інформаційної безпеки підприємства;

− впровадження в діяльність підприємства новітніх досягнень науки і техніки, передового досвіду в галузі забезпечення інформаційної безпеки.

− спільна робота з представниками інших організацій з питань безпеки – безпосередній контакт або консультації з партнерами або клієнтами;

− постійна перевірка відповідності прийнятих в організації правил безпечної обробки інформації існуючим правовим нормам, контроль за дотриманням цієї відповідності [70, с. 121].

Додатково до обов’язків співробітників СІБ в ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» входить виконання директив вищестоящого керівництва, участь у виробленні рішень з усіх питань, пов’язаних з процесом обробки інформації з точки зору забезпечення його захисту. Більш того, всі ці розпорядження, що стосуються цієї галузі, обов’язкові для виконання співробітниками всіх рівнів і організаційних ланок.

Склад і розмір групи безпеки в ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» залежать від конкретного підприємства і завдань, які ставляться перед нею.

При розгляді питань безпеки інформації в комп'ютерних системах (КС) завжди говорять про наявність деяких бажаних станів системи. Ці бажані стани описують захищеність системи. Поняття захищеності принципово не відрізняється від інших властивостей технічної системи, наприклад надійної роботи.

Особливістю поняття захищеність є його тісний зв'язок з поняттям загроза (те, що може бути причиною виведення системи із захищеного стану).

Отже, виділяються три компоненти, що пов'язані з порушенням безпеки системи ТОВ «Спільного підприємства «Полтавська газонафтова компанія»»:

- загроза – зовнішнє, відносно системи, джерело порушення властивості захищеність;
- об'єкт атаки – частина системи, на яку діє загроза;
- канал дії – середовище перенесення зловмисної дії[10, с. 18].

Інтегральною характеристикою, яка об'єднує всі ці компоненти, є політика безпеки – якісний (або якісно-кількісний) вираз властивостей захищеності в термінах, що представляють систему. Опис ПБ повинен включати або враховувати властивості загрози, об'єкта атаки та каналу дії.

За означенням, під ПБ інформації розуміється набір законів, правил, обмежень, рекомендацій тощо, які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз.

Термін політика безпеки може бути застосований до організації комп'ютерної системи, операційної системи, послуги, що реалізується системою (набору функцій) для забезпечення захисту від певних загроз, і т. ін. Чим дрібніший об'єкт, щодо якого вживається цей термін, тим конкретніші й формальніші стають правила[70, с. 130].

ПБ інформації в КС є частиною загальної ПБ ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» і може успадковувати, зокрема, положення державної політики у сфері захисту інформації. Для кожної системи ПБ інформації може бути індивідуальною і залежати від конкретної технології обробки інформації, що реалізується, особливостей операційної системи, фізичного середовища та багатьох інших чинників.

Частина ПБ, яка регламентує правила доступу користувачів і процесів до ресурсів комп'ютерної системи, становить правила розмежування доступу ТОВ «Спільного підприємства «Полтавська газонафтова компанія»».

Розробка і підтримка ПБ ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» завжди означає досягнення компромісу між альтернативами, які обирають власники цінної інформації для її захисту. Отже, будучи результатом компромісу, ПБ ніколи не задовольнить усі сторони, що беруть участь у захисті інформації[70, с. 131].

Водночас, вибір ПБ для ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» – це остаточне рішення: що добре й що погано в поводженні з цінною інформацією. Після прийняття такого рішення можна будувати захист, тобто систему підтримки виконання правил ПБ. Тоді цілком природним критерієм якості системи захисту інформації (СЗІ) стає такий: «побудована СЗІ вдала, якщо вона надійно підтримує виконання правил ПБ, і, навпаки, СЗІ невдала, якщо вона ненадійно підтримує ПБ».

Такий розв'язок проблеми захищеності інформації і проблеми побудови СЗІ ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» дає змогу залучити до теорії захисту точні математичні методи, тобто доводити, що певна СЗІ в заданих умовах підтримує ПБ. Саме в цьому полягає суть доказового підходу щодо захисту інформації, який дозволяє говорити про гарантовано захищену систему.

Зважаючи на технічні та програмно-апаратні проблеми ТОВ «Спільного

підприємства «Полтавська газонафтова компанія»», що виникають при організації захисту в захищених АС, у багатьох випадках належний рівень захищеності досягається за рахунок вдало реалізованої ПБ, причому іноді ПБ може залишитися майже єдиним засобом забезпечення захисту. Тому розробка, дослідження та правильне застосування ПБ є надзвичайно актуальною проблемою сучасних СЗІ[70, с. 132].

Формальний вираз політики безпеки в ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» називають моделлю ПБ. Основна мета створення ПБ інформаційної системи й опису її у вигляді формальної моделі – це визначення умов, яким має підпорядковуватися поведінка системи, вироблення критерію безпеки і проведення формального доведення відповідності системи цьому критерію при додержанні встановлених правил і обмежень. На практиці це означає, що тільки уповноважені користувачі можуть отримати доступ до інформації і здійснювати з інформацією тільки санкціоновані дії[13].

ПБ в ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» задається у вигляді правил, відповідно до яких мають виконуватися всі взаємодії між суб’єктами та об’єктами. Взаємодії, що призводять до порушень цих правил, припиняються засобами контролю доступу й не можуть бути здійснені.

ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» використовує дискреційну модель політики безпеки. Основою дискреційної політики безпеки є дискреційне управління доступом (Discretionary Access Control – DAC), яке визначається двома властивостями:

- усі суб’єкти й об’єкти мають бути однозначно ідентифіковані;
- права доступу суб’єкта до об’єкта системи визначаються на основі певних зовнішніх відносно системи правил[23].

Назва пункту є дослівним перекладом з англійської терміна Discretionarypolicy (ДПБ), ще один варіант перекладу – розмежувальна політика. Ця політика одна з

найпоширеніших в світі, в системах по замовчуванню мається на увазі саме ця політика. ДПБ реалізується за допомогою матриці доступу, яка фіксує множину об'єктів та суб'єктів, доступних кожному суб'єкт вТОВ «Спільного підприємства «Полтавська газонафтова компанія»» доцільно розділити на три рівні. До верхнього рівня можна віднести рішення, що торкаються організації в цілому. Вони носять дуже загальний характер і, як правило, виходять від керівництва організації. Наприклад, список подібних рішень може включати в себе:

− формування або перегляд самої комплексної програми забезпечення інформаційної безпеки, призначення відповідальних за реалізацію цієї програми;

− формулювання цілей у сфері інформаційної безпеки та визначення загальних напрямів їх досягнення;

− забезпечення технічної бази для дотримання відповідних законів і правил;

− формулювання управлінських рішень з тих питань реалізації програмної безпеки, які повинні розглядатися на рівні організації в цілому[70].

На політику верхнього рівня в ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» впливають цілі організації в галузі інформаційної безпеки: вони формулюються, як правило в термінах цілісності, доступності та конфіденційності. Якщо організація відповідає за підтримку критично важливих баз даних, то на першому плані може стояти зменшення випадків втрат, пошкоджень або спотворень даних. Для організації, що займається наданням послуг, імовірно, важлива актуальність інформації про ці послуги та їх ціни, а також доступність послуг максимальному числу потенційних покупців. Режимна організація в першу чергу піклується про захист від несанкціонованого доступу – конфіденційності[40].

Нарешті, політика інформаційної безпеки верхнього рівня в ТОВ «Спільного підприємства «Полтавська газонафтова компанія»», очевидно, повинна вписуватися в існуючі закони держави, а щоб бути впевненими в тому, що їй точно

й акуратно слідує персонал підприємства, доцільно розробити систему відповідних заохочень і покарань. А взагалі-то кажучи, на верхній рівень слід виносити мінімум питань. До середнього рівня можна віднести окремі аспекти інформаційної безпеки, проте важливі для різних систем, експлуатованих організацією[8].

Політика середнього рівня в ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» по кожному подібному аспекту передбачає вироблення відповідного документованого управлінського рішення, в якому зазвичай є:

− опис аспекта. Якщо користувачізастосовуютьнеофіційне програмне забезпечення, то про нього обов'язково має бути повідомлено, адже це забезпечення, яке не було схвалено і закуплено на рівні організації;

− вказівка на область її застосування (розповсюдження політики інформаційної безпеки). Іншими словами має бути сертифіковано, де, коли, як, по відношенню до кого і чого застосовується дана політика безпеки;

− чіткий розподіл відповідних ролей та обов'язків. У «політичний» документ необхідно включити інформацію про посадових осіб, відповідальних за проведення політики безпеки в життя.

− механізм забезпечення «законослухняності»[29].

Політика безпеки нижнього рівня в ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» відноситься до конкретних сервісів. Вона включає в себе всього два аспекти – мети і правила їх досягнення, тому її часом важко відокремити від питань реалізації (надання послуг з інформаційного забезпечення). На відміну від двох верхніх рівнів, розглянута політика нерідко буває набагато більш детальною. Є багато питань, специфічних для окремих сервісів, які не можна єдиним чином регламентувати в рамках всієї організації. У той же час ці питання настільки важливі для забезпечення режиму безпеки, що рішення, які належать до них, повинні прийматися на управлінському, а не технічному рівні [11].

В другому розділі проаналізовано діяльність ТОВ «Спільного підприємства

«Полтавська газонафтова компанія»», визначено основні принципи та методи забезпечення інформаційної безпеки на підприємстві, оцінено стан забезпечення інформаційної безпеки.

При формулюванні цілей, політика безпеки в ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» може виходити з міркувань цілісності, доступності та конфіденційності, але вона повинна розвиватися. Її цілі мають бути конкретними. Якщо мова йде про систему розрахунку зарплати, можна поставити мету, щоб тільки працівникам відділу кадрів і бухгалтерії дозволялося вводити і змінювати інформацію. З цілей зазвичай виводяться правила безпеки.

Відповідно до вище сказаного можна зробити висновок, що керівництву ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» необхідно знайти розумний компроміс для організації політики безпеки, коли за оптимальні затрати буде забезпечено належний рівень інформаційної безпеки.

РОЗДІЛ 3
УДОСКОНАЛЕННЯ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ В ТОВАРИСТВІ З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ СПІЛЬНОГО ПІДПРИЄМСТВА «ПОЛТАВСЬКА ГАЗОНАФТОВА КОМПАНІЯ»

3.1 Принципи захисних заходів від несанкціонованого доступу в автоматизованих системах

Процес управління електронним документообігом спирається на зрозумілі для людей електронні документи, що містять інструкції для співробітників організації. Електронний документообіг – єдиний механізм по роботі із документами, представленими в електронному вигляді, з реалізацією концепції «безпаперового діловодства»[42, с. 145].

Системи електронного документообігу – це складний комплекс технічних і організаційних рішень, які сприяють збереженню і раціональному використанню людських ресурсів і підвищенню ефективності управління потоками корпоративних документів та інформації [58, с. 12].

Поряд з традиційними документопотоками, СЕД мають низку переваг,серед яких найважливішими є вирішення проблеми централізованого відслідкування руху документів в реальному масштабі часу, висока компактність архіву, економія паперу та висока швидкість пошуку і одержання інформації [31].

Переваги використання систем електронного документообігу в ТОВ «Спільного підприємства «Полтавська газонафтова компанія»»:

1. Продуктивність праці персоналу збільшується на 20-25%.
2. Вартість архівного збереження електронних документів на 80%, що нижче в порівнянні із вартістю збереження паперових архівів.
3. Звільненням фізичного місця для збереження документів.

4. Зменшенням витрат на копіювання і доставку документів у паперовому вигляді.

5. Зниженням витрат на персонал і устаткування.

6. Поява можливості колективної роботи над документами (що неможливо при паперовому діловодстві).

7. Значне прискорення пошуку і вибірки документів (по різних атрибутах).

8. Підвищення безпеки інформації за рахунок того, що робота в СЕД з незареєстрованної робочої станції неможлива, а кожному користувачеві СЕД призначаються свої повноваження доступу до інформації.

9. Поліпшення контролю за виконанням документів.

10. Документальна підтримка роботи з клієнтами і діловими партнерами.

11. Економія часу на обробку документів.

Недоліком використання СЕД – введення електронних документів у практику роботи підприємств тісно пов’язано з необхідністю реформування практичної роботи персоналу. Занадто кардинальний, революційний перехід від традиційного до електронного документообігу спричинить зниження ефективності праці у спеціалістів діловодних служб та призведе до серйозних проблем в управлінні і навіть до дезорганізації діяльності на підприємстві. В той же час поступовий перехід до інформатизації діловодних процесів потребує спеціальної підготовки та значних фінансових затрат [35, с. 45].

Та все ж існують значні проблеми повноцінного впровадження електронного документообігу в системі управліннящідприємства:

1. Неузгодженість українського законодавства з міжнародним у сфері електронного документообігу. Закон України «Про електронний цифровий підпис»[47, с. 1] не відповідає європейським вимогам. Відсутність чіткого визначення понятійно-категоріального апарату щодо властивостей та можливостей елетронного підпису («посиленний електронний підпис», «кваліфікований цифровий підпис» тощо), як

основного реквізиту електронного документа, ускладнює процес якісного впровадження СЕД.

2. Недоопрацювання законодавчої нормативної бази у питанні надання електронному документу як об'єкту електронного документообігу юридичної сили. Електронний документ має юридичну силу лише за наявності обов'язкових реквізитів, наявність яких є підставою для обліку такого документа. Проте переліку таких реквізитів, окрім електронного підпису у базових нормативних актах не наведено [41, с. 303].

3. Практика паралельної маршрутизації паперового та електронного документообігу досить часто спричиняє порушення основних принципів документообігу, зокрема принцип однократності у реєструванні документів. Досить часто електронні документи, що мають правові наслідки, супроводжують паперовими копіями з «реальним підписом». Та варто розуміти, що метою СЕД є не викорінення паперових документів, а створення ефективного середовища керування і функціонування підприємства (установи). Тому важливо роздруковувати виключно кінцеві продукти роботи – повністю підготовленні паперові документи [41, с. 304].

4. Складна схема фінансування проекту впровадження СЕД (вимоги по проведенню конкурсів, складна схема прийняття рішень та інше), викликають особливі складності на початкових етапах [15].

Таким чином, перед розгортанням СЕД необхідно виважено оцінити готовність всіх суб'єктів прийняття рішень до нових інформаційних технологій.

Функціональність СЕД:

- підтримка функцій діловодства (вхідні, вихідні, розпорядчі, внутрішні);
- бібліотечні послуги зі створення, зберігання і пошуку документів;
- мережеві послуги з організації спільної роботи;
- підтримка безпеки і автентичної ідентифікації при роботі з документами;

- повнотекстовий пошук по загальному масиву документів;
- послуги зі створення і супроводу сховища документів;
- підтримка архівації документів;
- ведення історії змін і пропозицій по зміні документів [68, с. 64].

Отже, СЕД в ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» реалізують функції з автоматизації традиційних діловодних процесів і передбачають паралельне функціонування електронного і паперового документообігу. Водночас вони можуть успішно здійснювати повноцінний електронний документообіг.

На відміну від традиційного програмного забезпечення – систем орієнтованих на автоматизацію конкретних ділянок бізнесу (бухгалтерія, складський облік, кадри та ін.) Системи автоматизації документообігу пропонують рішення задач менш очевидних і більш комплексних. Загалом справи впровадження системи автоматизації документообігу зачіпає всі рівні управління компанії і покликане змінити способи управління. Складність даної задачі, як правило, недооцінюється керівництвом компанії. Наринку склалася певна диспропорція: постачальники програмного забезпечення намагаючись вирішувати завдання, з якими вони стикаються на практиці, ускладнюють програмне забезпечення. Це призводить до додаткових складнощів при його впровадженні і, відповідно, збільшує вартість проекту. А покупці систем, як правило, не готові до такого рівня складності, прагнуть отримати більш легке рішення за меншу ціну[58, с. 13].

Таким чином, для впровадження платформи комплексної автоматизації документообігу в ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» повинні сформуватися такі принципи:

– усвідомлення необхідності вирішення комплексу задач в області автоматизації документообігу з метою істотного поліпшення керованості

організації.

– наявність волі керівництва і розуміння тривалості і трудомісткості процесу впровадження системи.

– наявність кваліфікованих кадрів, які зможуть здійснювати координацію послідовної розробки та впровадження програм на базі платформи [29, с. 17].

Автоматизація паперового документообігу є проміжним рішенням, що використовуються для підвищення ефективності роботи системиділоводства[66, с. 168].

Можна зробити висновок, що перед будь-якою організацією постає питання автоматизації документообігу. Задачі, які вирішуються в процесі автоматизації документообігу установи, залежать від характеру комерційної діяльності, інфраструктури, адміністративної організації та інших факторів.

В ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» використовують систему оперативного управління підприємством «Мотив». 1200 компаній використовують «Мотив» для спільної і віддаленої роботи, ведення електронного архіву, управління проектами і взаємодії з клієнтами.

Автоматизована система контролю виконання доручень «Мотив» належить до Web-орієнтованих додатків і є потужним організуючим інструментом управління для будь організації. Програмний продукт поєднує в собі можливість ефективної організації спільної роботи співробітників (workflow) і управління електронними документами [37].

Система містить засоби колективної роботи, що дозволяють автоматизувати постановку доручень і завдань, а також контроль за їх виконання. Отримання звітів допомагає скласти повну картину діяльності окремих співробітників, підрозділу або компанії в цілому.

Можна інтегрувати «Мотив» з електронною поштою або корпоративним порталом. Система створить завдання по кожній заявці, заповнить поля і додасть

відповідальних співробітників. Завдання забезпечать оперативний доступ до інформації про клієнта, історії відносин і планом робіт. Завдання автоматично сортуються за відповідальним співробітниками, галузями, регіонам і стадіями роботи з клієнтом. По кожному запланованому події відправляються email-оповіщення та SMS.

Для повноцінної роботи в автоматизованій системі «Мотив» не потрібні витрати на тривале навчання персоналу, інтерфейс програми простий у розумінні і обігу – необхідні лише базові навички роботи зі стандартними офісними додатками [37].

АС «Мотив» дозволяє керівному складу організувати строгу структуру підпорядкованості персоналу, контролювати своєчасне виконання завдань і доручень, створювати для вирішення окремих завдань робочі групи з організацією додаткових зв’язків підпорядкованості.

Накопичення статистики за виконуваними діями кожного співробітника компанії дозволяє керівництву оперативно реагувати на труднощі, що виникають під час вирішень поставлених завдань. Тим самим досягається високий рівень управління і тактичного планування, який необхідний для отримання виробничого прибутку і подальшого розвитку компанії [37].

Отже, в ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» значними перевагами автоматизованої системи «Мотив» є:

- відсутність серверної ліцензії та прихованих платежів;
- низька вартість – безстрокова ліцензія COMPLETE за доступну ціну;
- максимальний комплект поставки для кожної ліцензії (електронний документообіг, виконання доручень, мобільний інтерфейс, інструментарій адміністратора, потокове сканування, підписання електронним цифровим підписом і звітність);
- поєднання функціональності кількох систем (СЕД, СКИП, ECM, PM і CRM) в одному продукті;

– швидке (від трьох робочих днів) і недороге впровадження;

– інтуїтивно зрозумілий інтерфейс – навіть найбільш консервативні співробітники зможуть звикнути до роботи в системі «Мотив» за кілька днів;

– можливість самостійного впровадження системи і подальшої підтримки в зручному графічному інтерфейсі;

– легке адміністрування – для 100 активних користувачів досить штатного системного адміністратора [37].

Таким чином, АС «Мотив» покликана контролювати та істотно прискорювати процес виконання завдань, впливати на підготовку, узгодження і виконання документів.

У ТОВ «Спільного підприємства «Полтавська газонафтова компанія»», не менш важливим фактором в системі є захист від несанкціонованого доступу до документів, що реалізується адміністратором системи захисту інформації.

В рамках вказаної програми прийнято розрізняти пасивні об’єкти захисту (файли, прикладні програми, термінали, ділянки оперативної пам’яті) і активні суб’єкти (процеси), котрі можуть виконувати над об’єктами визначені операції. Захист об’єктів здійснюється операційною системою засобами контролю за виконанням суб’єктами сукупності правил, які регламентують вказані операції. Вказану сукупність правил інколи називають статусом захисту.Під час свого функціонування суб’єкти генерують запити на виконання операцій над захищеними об’єктами[37].

В АС «Мотив» є пункт меню «Політика безпеки», що включає в себе політику мережевої безпеки та політику безпеки паролів. На вкладці «Політика мережевої безпеки» адміністратор задає фільтри мережевих адрес для контролю доступу до системи користувачів із різних ділянок мережі.

Доступ до АС визначається виходячи з параметрів, заданих для:

– Довірених вузлів – списку вузлів мережі, з яких дозволений доступ користувачів в систему;

– Заборонених вузлів – списку вузлів мережі, з яких заборонений доступ користувачів в Систему;

– Інших вузлів – вузлів мережі, не зазначених в якості довірених або заборонених [37].

Доступ до Системи заборонений:

1) якщо параметри входу користувача потрапляють під параметри, зазначені в списку Заборонених вузлів;

2) якщо параметри входу користувача не потрапляють під параметри, зазначені в списку Довірених вузлів та в Інших вузлах встановлено заборону для всіх користувачів.

Доступ до Системи дозволений:

1) якщо параметри входу користувача потрапляють під параметри, зазначені в списку Довірених вузлів;

2) якщо параметри входу користувача не потрапляють під параметри, зазначені в списку Заборонених вузлів, і в Інших вузлах встановлено дозвіл для всіх користувачів.

Якщо параметри входу користувача потрапляють одночасно і в заборонені, і дозволені, то доступ визначається параметрами Інших вузлів [37].

Доступ до ресурсів операційної системи «Мотив» в ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» обмежується засобами захисту, паролями. Пароль може бути використаним також, як ключ для шифрування-дешифрування інформації в користувацьких файлах. Самі паролі також зберігаються в зашифрованому виді, що ускладнює їх виявлення і використання зловмисниками. Пароль може бути змінений користувачем, адміністратором системи або самою системою після встановленого інтервалу часу.

Відповідно до вище сказаного, можна зробити висновок про те, що в АС «Мотив» відбувається чітке розмежування доступу користувачів до системи, щоб запобігти викраденню, знищенню, пошкодженню, тобто несанкціонованого доступу до документів та інших важливих даних, що містяться в системі.

3.2 Засоби забезпечення захисту інформації в автоматизованих інформаційних системах в спільному підприємстві «Полтавська газонафтова компанія»

В автоматизованих інформаційних системах ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» комп'ютерні системи зазвичай використовують стандартне та спеціалізоване обладнання і програмне забезпечення захисту інформації, що виконує певний набір функцій для обробки інформації. До їх складу входять такі функції: цілісність інформації і захист, обмеження доступу до неї забезпечується спеціалізованими компонентами системи. Автоматизована інформаційна система як об'єкт інформаційної безпеки (додаток Л).

Слід зазначити, що в процесі функціонування системи неможлива поява в ній нової функції, навіть в результаті виконання будь-якої комбінації із заданих при розробці функцій.

При використанні системи її функціональність не повинна змінюватися, для цього необхідно забезпечити:

- цілісність системи в момент її запуску;
- цілісність системи в процесі функціонування.

Особливу увагу слід приділити аутентифікації користувача. Автоматизована система ідентифікує користувача, перевіряє його повноваження і виконує запит або задачу з обробки інформації[8].

Надійність захисту інформації в АІС визначається:

- переліком і властивостями функцій АІС;
- методами, що використовують у функціях;
- способом реалізації функцій.

Перелік функцій, що використовуються відповідає класу захищеності, присвоєному комп'ютерній системі в процесі сертифікації і є ідентичним для систем з однаковим класом. Тому при розгляді конкретної системи необхідно звернути увагу на методи, що використовуються і спосіб реалізації найбільш важливих функцій: аутентифікації та перевірки цілісності системи[9, с. 43].

В ТОВ «Спільного підприємства «Полтавська газонафтова компанія»»,більшість функцій сучасних комп'ютерних систем реалізовані у вигляді програм, підтримка цілісності яких в процесі запуску системи і особливо в процесі функціонування є важким завданням. Для порушення цілісності програми немає необхідності в додатковому устаткуванні. Велика кількість користувачів в тій чи іншій мірі вміють програмувати і розуміються в операційних системах, знають їх помилки . Тому ймовірність атаки на програмне забезпечення досить висока .

Перевірка цілісності програм програмним чином (за допомогою інших програм) не є надійною. Необхідно чітко уявляти, як забезпечується цілісність самої програми перевірки цілісності. Якщо вона знаходиться на тих же носіях, що і перевіряються програми, то довіряти результатам перевірки роботи такої програми не можна. Таким чином, чисто програмним способом не може бути надійно забезпечена цілісність системи, Тому до програмних систем захисту від НСД слід ставиться з особливою обережністю[8].

Використання апаратних засобів для захисту інформації в ТОВ «Спільного підприємства «Полтавська газонафтова компанія»», знімає проблему забезпечення цілісності системи. У більшості сучасних систем захисту від несанкціонованого доступу застосовується зашивання програмного забезпечення в постійний запам'ятовуючий пристрій або в аналогічну мікросхему. Таким чином, щоб

змінити ПЗ, необхідно отримати доступ до відповідної плати і замінити мікросхему. Якщо використовується універсальний процесор, то для заміни або зміни ПЗ необхідне спеціальне обладнання, що ще більш ускладнює атаку на завантажене в процесор ПЗ. Використання спеціалізованого процесора з реалізацією алгоритму роботи у вигляді інтегральної мікросхеми повністю знімає проблему порушення цілісності алгоритму роботи.

На практиці в ТОВ «Спільного підприємства «Полтавська газонафтова компанія»», функції аутентифікації користувача, перевірки цілісності, криптографічні функції, що утворюють ядро системи безпеки, реалізуються апаратно, всі інші функції – програмно. Будь-яка система захисту будується на відомих розробнику можливості ОС, причому для побудови надійної комп'ютерної системи потрібні повні знання всіх можливостей ОС. Зараз вітчизняні роробники мають у своєму розпорядженні повні знання лише про одну операційну систему– DOS.

Таким чином, до повністю контрольованих систем вТОВ «Спільного підприємства «Полтавська газонафтова компанія»» можна віднести КС, що працюють з операційною системою DOS, або КС власної розробки.В якостіодного з апаратних (а він не може бути програмним) модулів безпеки можуть використовуватися плати серії Криптон, що забезпечують:

- захист ключів шифрування та електронного цифрового підпису;
- незмінність алгоритму шифрування і ЕЦП.

Електронний цифровий підпис – вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа[47, с. 1].

Особистий ключ – параметр криптографічного алгоритму формування електронного цифрового підпису, доступний тільки підписувачу.

Відкритийключ – параметркриптографічногоалгоритму перевірки електронного цифровогопідпису,доступнийсуб'єктамвідносин у сфері використання електронного цифрового підпису[47, с. 2].

Всі ключі, які використовуються всистемі, можуть шифруватися в майстер-ключі і зберігатися на зовнішньому носії в зашифрованому вигляді. Вони розшифровуються тільки всередині плати. У використовуваних зараз апаратно-програмних системах захисту від несанкціонованого доступу для частково контрольованих систем серйозно розглядати можна тільки функції доступу на персональний комп'ютер, що виконуються до завантаження операційної системи, і апаратні функції блокування портів ПК. Таким чином, залишається велике поле діяльності по розробці модулів безпеки для захисту обраних процесів в частково контрольованих системах[8].

Використання криптографічного захисту інформації під час побудови політики безпеки комп'ютерної системи в ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» значно посилює безпеку роботи в системі, але за умови, що система захисту створена належним чином та має безпечну систему розподілу криптографічних ключів.

Криптографічні методи захисту інформації – це методи захисту даних із використанням шифрування.

Головна мета шифрування (кодування) інформації – її захист від несанкціонованого читання. Системи криптографічного захисту (системи шифрування інформації) для банківських on-line -сисгем можна поділити за різними ознаками:

– за принципами використання криптографічного захисту (вбудований у систему або додатковий механізм, що може бути відключений);

– за способом реалізації (апаратний, програмний, програмно-аларатний);

– за криптографічними алгоритмами, які використовуються (загальні, спеціальні);

– за цілями захисту (забезпечення конфіденційності інформації (шифрування) та захисту повідомлень і даних від модифікації, регулювання доступу та привілеїв користувачів);

– за методом розподілу криптографічних ключів (базових/сеансових ключів, відкритих ключів) тощо.

Вбудовані механізми криптографічного захисту входять до складу системи, їх створюють одночасно з розробленням системи. Такі механізми можуть бути окремими компонентами системи або бути розподіленими між іншими компонентами системи[8].

Додаткові механізми криптозахисту – це додаткові програмні або апаратні засоби, які не входять до складу системи. Така реалізація механізмів криптозахисту має значну гнучкість і можливість швидкої заміни. Для більшої ефективності доцільно використовувати комбінацію додаткових і вбудованих механізмів криптографічного захисту.

За способом реалізації криптографічний захист можна здійснювати різними способами: апаратним, програмним або програмно-апаратним. Апаратна реалізація криптографічного захисту – найбільш надійний спосіб, але й найдорожчий. Інформація для апаратних засобів передається в електронній формі через порт обчислювальної машини всередину апаратури, де виконується шифрування інформації. Перехоплення та підробка інформації під час її передачі в апаратуру може бути виконана за допомогою спеціально розроблених програм типу «вірус».

Програмна реалізація криптографічного захисту значно дешевша та гнучкіша в реалізації. Але виникають питання щодо захисту криптографічних ключів від перехоплення під час роботи програми та після її завершення. Тому, крім захисту від «вірусних» атак, потрібно вжити заходів для забезпечення повного звільнення пам’яті від криптографічних ключів, що використовувались під час роботи програм «збирання сміття»[9, с. 44].

Крім того, можна використовувати комбінацію апаратних і програмних механізмів криптографічного захисту. Найчастіше використовують програмну реалізацію криптоалгоритмів з апаратним зберіганням ключів. Такий спосіб криптозахисту є досить надійним і не надто дорогим. Але, обираючи апаратні засоби для зберігання криптографічних ключів, треба пам’ятати про забезпечення захисту від перехоплення ключів під час їх зчитування з носія та використання в програмі.

В основу шифрування покладено два елементи: криптографічний алгоритм і ключ.

Криптографічний алгоритм – це математична функція, яка комбінує відповідний текст або іншу зрозумілу інформацію з ланцюжком чисел (ключем) з метою отримання незв’язаного (шифрованого) тексту.

Усі криптографічні алгоритми можна поділити на дві групи: загальні і спеціальні.

Спеціальні криптоалгоритми мають таємний алгоритм шифрування, а загальні криптоалгоритми характерні повністю відкритим алгоритмом, і їх криптостійкість визначається ключами шифрування. Спеціальні алгоритми найчастіше використовують в апаратних засобах криптозахисту[64].

Загальні криптографічні алгоритми часто стають стандартами шифрування, якщо їхня висока криптостійкість доведена. Ці алгоритми оприлюднюють для обговорення, при цьому навіть призначають премію за успішну спробу його

«злому». Криптостійкість загальних алгоритмів визначається ключем шифрування, який генерується методом випадкових чисел і не може бути повторений протягом певного часу. Криптостійкість таких алгоритмів буде вищою відповідно до збільшення довжини ключа.

Є дві великі групи загальних криптоалгоритмів: симетричні і асиметричні. До симетричних криптографічних алгоритмів належать такі алгоритми, для яких шифрування і розшифрування виконується однаковим ключем, тобто і відправник, і отримувач повідомлення мають користуватися тим самим ключем. Такі алгоритми мають досить велику швидкість обробки як для апаратної, так і для програмної реалізації. Основним їх недоліком є труднощі, пов’язані з дотриманням безпечного розподілу ключів між абонентами системи. Для асиметричних криптоалгоритмів шифрування і розшифрування виконують за допомогою різних ключів, тобто, маючи один із ключів, не можна визначити парний для нього ключ. Такі алгоритми часто потребують значно довшого часу для обчислення, але не створюють труднощів під час розподілу ключів, оскільки відкритий розподіл одного з ключів не зменшує криптостійкості алгоритму і не дає можливості відновлення парного йому ключа[64].

Усі криптографічні алгоритми можна використовувати з різними цілями, зокрема:

- для шифрування інформації, тобто приховування змісту повідомлень і даних;
- для забезпечення захисту даних і повідомлень від модифікації.

З найпоширеніших методів шифрування можна виділити американський алгоритм шифрування DES (Data Encryption Standart, розроблений фахівцями фірми IBM і затверджений урядом США 1977 року) із довжиною ключа, що може змінюватися, та алгоритм ГОСТ 28147-89, який був розроблений та набув широкого застосування в колишньому СРСР і має ключ постійної довжини. Ці алгоритми належать до симетричних алгоритмів шифрування[60].

Алгоритм Потрійний DES був запропонований як альтернатива DES і призначений для триразового шифрування даних трьома різними закритими ключами для підвищення ступеня захисту.

RC2, RC4, RC5 – шифри зі змінною довжиною ключа для дуже швидкого шифрування великих обсягів інформації. Здатні підвищувати ступінь захисту через вибір довшого ключа.

IDEA (International Data Encryption Algoritm) призначений для швидкої роботи в програмній реалізації.

Для приховування інформації можна використовувати деякі асиметричні алгоритми, наприклад, алгоритм RSA. Алгоритм підтримує змінну довжину ключа та змінний розмір блоку тексту, що шифрується[64].

Алгоритм RSA дозволяє виконувати шифрування в різних режимах:

– за допомогою таємного ключа відправника. Тоді всі, хто має його відкритий ключ, можуть розшифрувати це повідомлення;

– за допомогою відкритого ключа отримувача, тоді тільки власник таємного ключа, який є парним до цього відкритого, може розшифрувати таке повідомлення;

– за допомогою таємного ключа відправника і відкритого ключа отримувача повідомлення. Тоді тільки цей отримувач може розшифрувати таке повідомлення.

Але не всі асиметричні алгоритми дозволяють виконувати шифрування даних у таких режимах. Це визначається математичними функціями, які закладені в основу алгоритмів.

Другою метою використання криптографічних методів є захист інформації від модифікації, викривлення або підробки. Цього можна досягнути без шифрування повідомлень, тобто повідомлення залишається відкритим, незашифрованим, але до нього додається інформацію, перевірка якої за допомогою спеціальних алгоритмів може однозначно довести, що ця інформація не була змінена. Для симетричних алгоритмів шифрування така додаткова інформація – це код автентифікації, який

формується за наявності ключа шифрування за допомогою криптографічних алгоритмів [64].

Для асиметричних криптографічних алгоритмів формують додаткову інформацію, яка має назву електронний цифровий підпис. Формуючи електронний цифровий підпис, виконують такі операції:

– за допомогою односторонньої хеш-функції обчислюють прообраз цифрового підпису, аналог контрольної суми повідомлення;

– отримане значення хеш-функції шифрується: таємним або відкритим; таємним і відкритим ключами відправника і отримувача повідомлення –для алгоритму RSA.

– використовуючи значення хеш-функції і таємного ключа, за допомогою спеціального алгоритму обчислюють значення цифрового підпису.

Останнім часом використання електронного цифрового підпису значно поширюється, у тому числі для регулювання доступу до конфіденційної інформації та ресурсів системи, особливо для on-line-систем реального часу[64].

Ефективність захисту систем за допомогою будь-яких криптографічних алгоритмів значною мірою залежить від безпечного розподілу ключів. Тут можна виділити такі основні методи розподілу ключів між учасниками системи.

1) Метод базових/сеансових ключів. Такий метод описаний устандарті ISO 8532 і використовується для розподілу ключів симетричних алгоритмів шифрування. Для розподілу ключів вводиться ієрархія ключів: головний ключ (так званий майстер-ключ, або ключ шифрування ключів) і ключ шифрування даних (тобто сеансовий ключ). Ієрархія може бути і дворівневою: ключ шифрування ключів/ключ шифрування даних. Старший ключ у цій ієрархії треба розповсюджувати неелектронним способом, який виключає можливість його компрометації. Використання такої схеми розподілу ключівв ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» потребує значного часу і значних затрат[69].

2) Метод відкритих ключів. Такий метод описаний у стандарті і може бути використаний для розподілу ключів як для симетричного, так і для асиметричного шифрування. За його допомогою можна також забезпечити надійне функціонування центрів сертифікації ключів для електронного цифрового підпису на базі асиметричних алгоритмів та розподіл сертифікатів відкритих ключів учасників інформаційних систем. Використання методу відкритих ключів дає можливість кожне повідомлення шифрувати окремим ключем симетричного алгоритму та передавати цей ключ із самим повідомленням у зашифрованій асиметричним алгоритмом формі [64].

Вибір того чи іншого методу залежить від структури системи і технології обробки даних. Жоден із цих методів не забезпечує «абсолютного» захисту інформації, але гарантує, що вартість «злому» у кілька разів перевищує вартість зашифрованої інформації.

Щоб використовувати систему криптографії з відкритим ключем, потрібно генерувати відкритий і особистий ключі. Після генерування ключової пари слід розповсюдити відкритий ключ респондентам. Найнадійніший спосіб розповсюдження відкритих ключів – через сертифікаційні центри, що призначені для зберігання цифрових сертифікатів.

Цифровий сертифікат – це електронний ідентифікатор, що підтверджує справжність особи користувача, містить певну інформацію про нього, слугує електронним підтвердженням відкритих ключів.Сертифікаційні центри несуть відповідальність за перевірку особистості користувача, надання цифрових сертифікатів та перевірку їхньої справжності[64].

Отже, в ТОВ «Спільного підприємства «Полтавська газонафтова компанія»»захистити автоматизовані системи без апаратних засобів, лише програмними засобами, неможливо.

3.3 Методи захисту електронної корпоративної інформації в спільному підприємстві «Полтавська газонафтова компанія»

В нинішніх умовах для підприємств дуже важливим є захист електронної корпоративної інформації. Отже, безпека електронної системи – це здатність її протидіяти спробам завдати збитків власникам і користувачам систем у разі появи різних збуджувальних (навмисних і ненавмисних) впливів на неї. Впливи на систему зображено на рисунку 3.1.

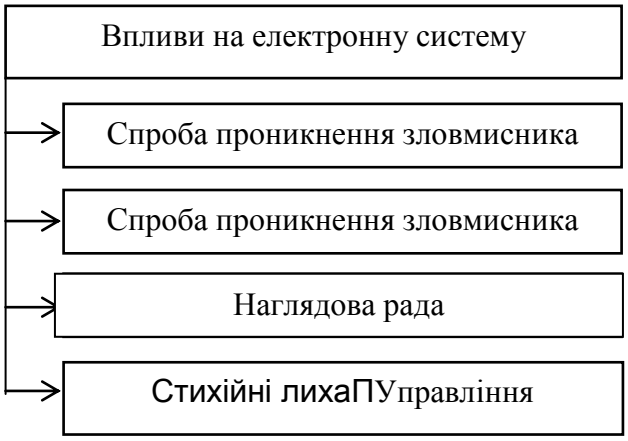

Рисунок 3.1 – Основні види впливів на електронну систему в ТОВ «Спільного підприємства «Полтавська газонафтова компанія»», складено автором за [43]

У ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» розрізняють внутрішню і зовнішню безпеку електронної системи. Внутрішня безпека враховує захист від стихійного лиха, від проникнення зловмисника, отримання доступу до носіїв інформації чи виходу системи з ладу. Предметом внутрішньої безпеки є забезпечення надійної і коректної роботи системи, цілісності її програм і даних. На основі проведеного аналізу, можна стверджувати, що на підприємстві використовують два підходи до гарантування безпеки електронних

систем.

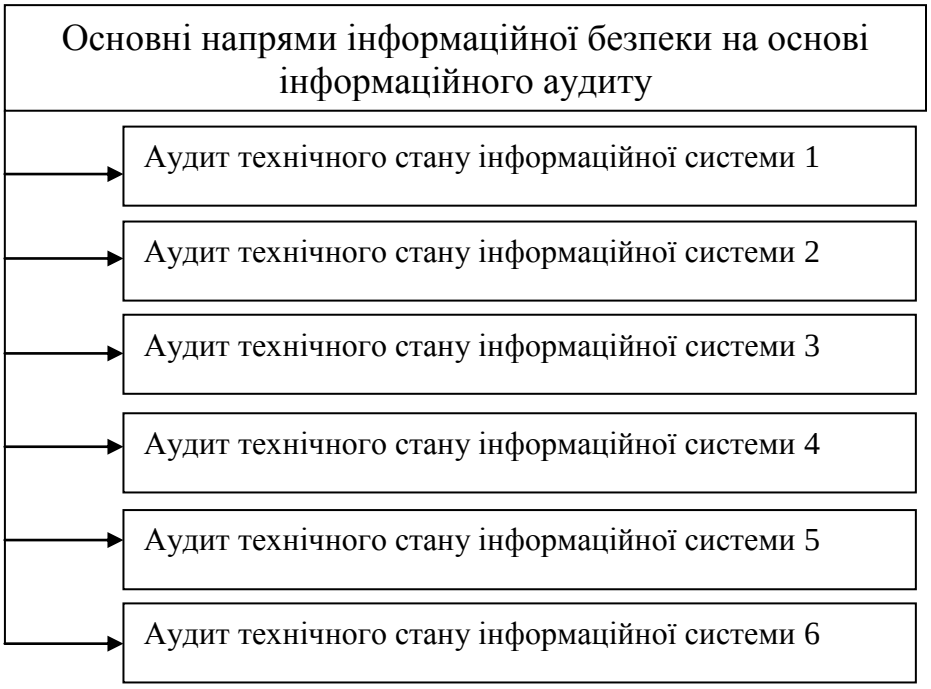

Рисунок 3.2 – Основні підходи до гарантування безпеки електронних систем в ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» [складено автором за (70, с. 207)]

В ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» використовують комплексний підхід, переважно для захисту великих систем, типові програмні засоби яких містять вмонтовані засоби захисту інформації, таких як АС «Мотив», 1С, але цього недостатньо. В цьому разі в ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» потрібно проводити такі заходи:

– організаційні заходи контролю за персоналом, який має високий рівень повноважень щодо дії в системі: за програмістами; за адміністраторами баз даних мережі;

– організаційні й технічні заходи резервування критично важливої інформації;

– організаційні заходи з відновлення працездатності системи у разі виникнення непередбачуваних ситуацій;

– організаційні й технічні заходи управління доступом у приміщеннях, де міститься обчислювальна техніка;

– організаційні й технічні заходи з фізичного захисту приміщень, в яких міститься обчислювальна техніка і носії даних, від стихійних лих тощо.

Аналізуючи ситуацію в світі у сфері стандартизації щодо інформаційної безпеки за роки розвитку індустрії ІБ, можна виділити такі тимчасові періоди, назва яких найбільш чітко характеризує природний розвиток цього процесу: поява стандартів (198 -1995 рр.), випробування практикою (1996-2000) і «виживання сильних»(від 2001і дотепер). Характерним для першого етапу є природний розвиток інформаційних технологій, за яким ледве встигала наука і практика у сфері ІБ. На цьому етапі формувалися понятійний апарат та основні підходи у сфері ІБ, аж до найкращих. Період кінця 80-х і особливо початок 90-х років характеризувався появою величезної кількості різних стандартів у сфері ІБ. Вони з’являлися як в окремих компаніях, або в консорціумах (X-Open, Good Practice тощо), так і в таких авторитетних інститутах, як NIST (National Institute of Standards and Technologies) і комплекс BSI (British Standards Institute) з ISO (International Standards Organisation). Зазначимо, що NIST і BSI нині є основними світовими конкурентами у сфері стандартизації. Природними недоліками стандартів на цьому етапі були: слабке практичне опрацювання, відсутність єдиних підходів та єдиного розуміння інформаційної безпеки[32].

Лише час міг подолати ці недоліки, що й відбулося на другому і третьому етапах – практичне застосування стандартів стимулювало їх природний відбір. Етап випробування практикою в середині 90-х років плавно перейшов в етап природного відбору і «виживання сильних» стандартів. Очевидно, сфера ІБ є досить замкнутою

і обмеженою, через що є зайвою величезна кількість стандартів, які перетинаються один з одним і намагаються різними способами описати одну і ту саму наочну сферу. На практиці вистачає кількох основоположних стандартів, які визнаються фахівцями й використовуються бізнесом на практиці. Таким чином, у цій битві стандартів виживали й вижили сильніші, зокрема стандарт ISO 15408[39], що регламентує вимоги до захищеності програмного забезпечення, або стандарт управління ISO 27001/17799 [59]. Ці стандарти нині дістали статус міжнародних. Щоправда, є одне «але». Світ розділився на дві географічно незалежні з огляду на стандартизацію зони: Європа й Азія визнають стандарти ISO, а США вважає за краще використовувати стандарти NIST. Зазначимо маловідомий факт: найбільш відомі стандарти ISO грунтуються на BSI: ISO 9001[20]. У 1985 році Національний центр комп'ютерної безпеки Міністерства оборони США опублікував «Помаранчеву книгу» («Критерії оцінки достовірності обчислювальних систем Міністерства оборони»). В ній наведено основні положення, за якими американське відомство оборони визначало ступінь захищеності інформаційно-обчислювальних систем; систематизовано основні поняття, рекомендації та класифікацію за видами загроз безпеці інформаційних систем, методи захисту від них, які далі перетворилися на зведення науково обґрунтованих норм і правил, що описують системний підхід до гарантування безпеки інформаційних систем та їх елементів. Запропонована в «Помаранчевій книзі» методологія стала загальноприйнятою та увійшла в національні стандарти.Поняття «політика безпеки» було також введене «Помаранчевою книгою»[45].

Політика безпеки – це сукупність норм, правил і методик, наоснові яких в подальшому будується діяльність інформаційної системи в галузі опрацювання, зберігання і розподілу критичної інформації[43, с. 202].

Інформаційна система – це не лише апаратно-програмний комплекс, а й обслуговуючий персонал. Політика безпеки формується на основі аналізу

поточного стану і перспективи розвитку інформаційної системи, можливих загроз і визначає:

- мету, завдання і пріоритети системи безпеки;
- галузь дії окремих підсистем;
- гарантований мінімальний рівень захисту;
- обов’язки персоналу щодо забезпечення захисту;
- санкції за порушення захисту.

Якщо політика безпеки проводиться не повною мірою або непослідовно, то ймовірність порушення захисту інформації різко зростає. Визначення політики безпеки неможливе без аналізу ризику, який підвищує рівень поінформованості про слабкі й сильні сторони захисту, створює базу для підготовки та прийняття рішень, оптимізує розмір витрат на захист, оскільки більшість ресурсів спрямовується на блокування загроз, що можуть завдати найбільшої шкоди[43, с. 203].

Аналіз ризику завершують прийняттям політики безпеки і складанням плану захисту,що має такі розділи:

1. Поточний стан. Опис статусу системи безпеки в момент підготовки плану.

2. Рекомендації. Вибір основних засобів захисту, що реалізують політику безпеки.

3. Відповідальність. Список відповідальних працівників і зон відповідальності.

4. Розклад. Визначення порядку роботи механізмів захисту, в тому числі і засобів контролю.

5. Перегляд положень плану, які потрібно періодично переглядати. У загальній системі гарантування безпеки захист інформації відіграє значну роль.

Виділяють такі підходи до організації захисту інформації:

- фізичні;
- законодавчі;

- управління доступом;
- криптографічне закриття.

Фізичні способи передбачають застосування фізичних перешкод для зловмисника, які закривають шлях до захищеної інформації (надійна система допуску на територію чи вприміщення з апаратурою або носіями інформації). Ці способи захищають лише від зовнішніх зловмисників і не захищають інформацію від осіб, які володіють правом входу в приміщення. Практика свідчить, що 75% порушень здійснюють працівники організації. До законодавчих способів захисту належать законодавчі акти, які регламентують правила використання й опрацювання інформації з обмеженим доступом і встановлюють міру відповідальності за порушення цих правил. Сюди належать також внутрішньо-організаційні методи роботи і правила поведінки[43, с. 204].

Управління доступом – захист інформації з регулюванням доступу до ресурсів системи: технічних, програмних та елементів баз даних. Регламентується порядок роботи користувачів і персоналу, право доступу до окремих файлів в базах даних. Відповідно до встановленої класифікації даних, користувачів, апаратури, приміщень відповідальні за безпеку розробляють багаторівневу підсистему управління доступом. Для захисту від несанкціонованого під’єднання до системи здебільшого використовують перевірку паролів, засоби антивірусного захисту і контролю цілісності, контролю та управління захисними механізмами, програми відновлення й резервного збереження інформації.

На концептуальному рівні служби безпеки в ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» специфікують напрями нейтралізації загроз. Усі напрями організації захисту інформації (фізичні, законодавчі, управління доступом, криптографічне закриття) реалізуються механізмами безпеки[43, с. 205].

В межах ідеології «відкритих систем» служби й механізми безпеки потрібно використовувати на будь-якому рівні еталонної моделі: фізичному; канальному;

мережевому; транспортному; сеансному; представницькому; прикладному. Протоколи інформаційного обміну поділяють на дві групи: віртуального з'єднання, дейтаграмні. Відповідно до зазначених протоколів мережі поділяють на віртуальні й дейтаграмні. У віртуальних мережах інформація між абонентами передається віртуальним каналом і проходить три етапи (фази):

- створення (встановлення) віртуального каналу;
- передача віртуального каналу;
- знищення віртуального каналу (роз’єднання).

При цьому повідомлення розбивається на блоки (пакети), які передаються в порядку їх розташування в повідомленні.

У дейтаграмних мережах блоки повідомлень передаються від відправника до адресата незалежно один від одного та різними маршрутами, тому порядок доставки блоків може не відповідати порядку їх розміщення у повідомленні.

Отже, віртуальна мережа в концептуальному плані відповідає принципу організації телефонного зв’язку,а дейтаграмна – поштовому. Ці два підходи визначають деякі розбіжності у складі та особливостях служб безпеки[43, с. 206].

Практичною рекомендацією щодо захисту електронної корпоративної інформації в ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» буде криптографічне закриття інформації у комп’ютерних системах, оскількице є найефективнішим способом захисту інформації із властивим йому високим рівнем захисту. В основі цього способу лежать програми криптографічного перетворення (шифрування) та програми захисту юридичної вагомості документів (цифровий підпис). Шифрування забезпечує засекречування інформації і використовується низкою інших сервісних служб. При цьому наявність чи знання загальнодоступного ключа не дає змоги визначити секретний ключ. Для використання механізмів криптографічного закриття інформації в локальній обчислювальній мережі потрібна налагоджена організація спеціальної служби

генерації ключів та їх розподіл між її абонентами[71].

Метод DEC (Data Encryption Standard) розроблений фірмою IBM і рекомендований для використання Агентством національної безпеки США, де він є федеральним стандартом. Алгоритм криптографічного захисту відомий і опублікований. Вважається, що нині апаратури, здатної виконувати обчислення, передбачені цим алгоритмом, немає.Російський стандарт шифрування даних ГОСТ 28147-89 – єдиний алгоритм криптографічного перетворення даних для великих інформаційних систем. Не накладає обмежень на ступінь секретності інформації. Має переваги алгоритму DEC і водночас позбавлений його недоліків, метод з відкритим ключем (RSA). Шифрування проводиться першим відкритим ключем, розшифрування – іншим секретним ключем[60].

Спеціалісти з криптографії вважають, що системи з відкритим ключем зручніше застосовувати для шифрування даних, що передаються, ніж при збереженні інформації. Існує ще одна галузь використання цього алгоритму – цифрові підписи, що підтверджують справжність документів і повідомлень, які передаються. Проте і він не є досконалим. Його недоліком є не до кінця вивчений алгоритм[71].

Отже, захист інформації в ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» здійснюють:

- комплексним застосуванням різних засобів і методів;
- створенням структури захисту й охорони з кількома рівнями;
- постійним їх удосконаленням.

Успіх справи залежить від збалансованої й налагодженої взаємодії захисту операційних систем і гарантування безпеки баз даних. У межах цієї програми розрізняють такі пасивні об’єкти захисту: файли, прикладні програми, термінали; ділянки оперативної пам’яті[71].

Активними є суб’єкти (процеси) захисту, котрі можуть виконувати над об’єктами визначені операції. Захист об’єктів здійснюється операційною системою

засобів контролю за виконанням суб'єктами захисту сукупності правил, що регламентують ці операції.

Статус захисту – це сукупність правил, які регламентують захист об'єктів. Під час свого функціонування суб'єкти генерують запити на виконання операцій над захищеними об'єктами.

Права (атрибути) доступу – це операції, які виконуються над захищеними об'єктами, а права доступу суб'єкта стосовно конкретного об'єкта є можливостями. Для формальної моделі статусу захисту в операційній системі використовують переважно матрицю доступу. Вона містить m рядків (за кількістю суб'єктів) і nстовпців (за кількістю об'єктів)[71].

Слід пам'ятати, що числа m і n на практиці здебільшого великі, а число множини можливостей елементів матриці доступу мале. Досить простим уреалізації засобом розмежування доступу до захищених об'єктів є механізм кола безпеки. Коло безпеки характеризується своїм унікальним номером. Нумерація здійснюється «із середини – назовні», і внутрішні кільця є привілегійованими щодо зовнішніх.

Доступ до ресурсів операційної системи може обмежуватися засобами захисту за паролями, який може бути використаний також як ключ для шифрування-дешифрування інформації в користувальних файлах. Самі паролі також зберігаються у зашифрованому вигляді, що утруднює їх виявлення і використання зловмисниками[14, с. 241].

Пароль може бути змінений користувачем, адміністратором системи або самою системою після встановленого інтервалу часу.

Відповідно до вище розглянутого в третьому роділі можна стверджувати, якщо в політика безпеки проводиться не повною мірою або непослідовно, то ймовірність порушення захисту інформації різко зростає. Визначення політики безпеки в ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» неможливе без аналізу ризику, який підвищує рівень поінформованості про слабкі й сильні

сторони захисту, створює базу для підготовки та прийняття рішень, оптимізує розмір витрат на захист, оскільки більшість ресурсів спрямовується на блокування загроз, що можуть завдати найбільшої шкоди.

ВИСНОВКИ

У дипломній роботі здійснені теоретичні узагальнення та запропоновано нове вирішення наукового завдання щодо забезпечення інформаційної безпеки підприємства, зокрема в ТОВ «Спільного підприємства «Полтавська газонафтова компанія», що сприятиме підвищенню ефективності захисту інформації та інформаційного продукту, а за результатами дослідження можна зробити такі висновки теоретико-методичного змісту та науково-практичного спрямування.

У першому розділі було визначено, що:

– поняття системи інформаційної безпеки для підприємстваполягає у діях щодо вияву, усунення та нейтралізації негативних джерел, причин і умов впливу на інформацію, але при цьому поняття «інформаційна безпека» характеризує стан інформаційного захисту господарюючого суб’єкта, в умовах якого можлива дія загроз;

– основними видами загроз є компрометація даних, розголошення конфіденційної інформації, помилкове використання інформаційних ресурсів, відмова в обслуговуванні, несанкціонований обмін інформації, відмова від інформації та несанкціоноване використання ресурсів локальної мережі. Знання можливих загроз інформаційній безпеці та вразливих місць системи захисту, необхідне для того, щоб обрати найбільш економічні і ефективні засоби забезпечення безпеки;

– на основіаналізу актуальних способів та методів несанкціонованого доступу в сучасних інформаційних системах та мережахстворено діаграму відсоткового співвідношення причин, через які відбувається порушення захисту інформації та виокремлено три основні шляхи несанкціонованого доступу до інформації, що полягають в: застосуванні технічних та програмних засобів; використанні недоліків мови програмування та недоліків у операційній системі, крадіжки носіїв

інформації; отриманні захищених даних за допомогою запитів дозволу, реквізитів розмежування доступу, таємних паролей.

У другому розділі було зроблено:

– аналіз діяльності Публічного акціонерного товариства «Спільного підприємства «Полтавська газонафтова компанія»», який показав, що результат роботи поширюється на всі сфери життя Полтавщини, впливає на розвиток економіки, а також стосується інтересів кожного мешканця регіону. Діловодство займає провідне місце у роботі апарату, оскільки впорядковує роботу з документами, носіями інформації на підприємстві, забезпечуючи економію ресурсів управлінської ланки;

– дослідження основних принципів та методів забезпечення інформаційної безпеки в ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» можна зробити висновки, що в ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» є достатня кількість захисних засобів забезпечення інформаційної безпеки. До основних можна віднести засоби: ідентифікації та аутентифікації користувачів, шифрування інформації, антивірусного захисту, контентної фільтрації;

– оцінено стан забезпечення інформаційної безпекив ТОВ «Спільного підприємства «Полтавська газонафтова компанія»»з використанням можливостей програми «Гриф», можна узагальнити, що рівень інформаційної безпеки знаходиться на достатньому рівні захисту, оскільки загальний рейтинг інформаційної безпеки становить 7,9. Недоліками в системі захисту інформації ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» є недостатня захищеність програмного забезпечення від хакерських атак, оскільки підприємство використовує застарілі версії програм захисту інформації.

У третьому розділі з’ясовано, що:

– в АС «Мотив» захист від НСД до документів здійснюється адміністратором системи захисту інформації за допомогою чіткого розмежування доступу користувачів до системи;

– для захисту інформації можна використовувавти комбінацію апаратних і програмних механізмів криптографічного захисту, використовуючи програмну реалізацію криптоалгоритмів з апаратним зберіганням ключів. Такий спосіб криптозахисту є досить надійним і не надто дорогим. Але, обираючи апаратн ізасоби для зберігання криптографічних ключів, необхідно пам’ятати про забезпечення захисту від перехоплення ключів під час їх зчитування з носія та використання в програмі;

– в ТОВ «Спільного підприємства «Полтавська газонафтова компанія»» існує два основних підходи до гарантування безпеки електронних систем на підприємстві: фрагментарний і комплексний. Підприємство здебільшого використовує комплексний підхід, переважно для захисту великих систем, типові програмні засоби яких містять вмонтовані засоби захисту інформації, таких як АС «Мотив», 1С, але це є недостатнім для повноцінного захисту, а отже необхідним буде проведення додаткових організаційних заходів з контролю за персоналом, зокрема за програмістами, адміністраторами баз даних мережі; заходів з резервування критично важливої інформації; заходів з відновлення працездатності системи у разі виникнення непередбачуваних ситуацій.

РЕКОМЕНДАЦІЇ

Захист інформації – є практичною реалізацією комплексної програми (концепції) інформаційної безпеки установи і являє собою жорстко регламентований і динамічний технологічний процес, що попереджає порушення доступності, цілісності, достовірності та конфіденційності цінних інформаційних ресурсів і в кінцевому рахунку забезпечує досить надійну безпеку інформації в процесі управлінської та виробничої діяльності установи. В даному випадку безпека розцінюється як реального результат, досягнутий за рахунок функціонування обраної системи захисту інформації.

Система захисту інформації – раціональна сукупність напрямків, методів, засобів і заходів, що знижують уразливість інформації та перешкоджають несанкціонованому доступу до інформації, її розголошенню чи витоку.

У сучасних підприємствах, установах, організаціях практично кожен основний співробітник стає носієм цінних відомостей, які становлять інтерес для конкурентів і кримінальних структур. Тому варто пам’ятати, що в основі системи захисту інформації лежить людський фактор, який передбачає відданість персоналу інтересам установи, і усвідомлене дотримання ним встановлених правил захисту інформації. І ніяка СЗІ не може забезпечити необхідного рівня безпеки інформації без належної підготовки користувачів і дотримання ними всіх встановлених правил, спрямованих на її захист.

Рекомендуємо:

– посилити аналітичну роботу по захисту інформації, так як результати цієї роботи показують ступінь безпеки інтелектуальної власності, умов функціонування установ і є основою побудови і вдосконалення системи захисту традиційних і електронних ІР, формування рубежів охорони території, будівлі, приміщень, обладнання і персоналу установи;

– постійно вести аналіз загроз, який полягає у виявленні та класифікації максимального складу джерел загрози конфіденційної інформації; обліку і вивченні кожного окремого суб'єктивного внутрішнього і зовнішнього джерела, ступеня його небезпеки (аналіз ризику) при реалізації загрози; розробці превентивних заходів щодо локалізації і ліквідації об’єктивних загроз;

– проводити періодичні і разові напрямки аналітичної роботи, які проводяться через певні проміжки часу з метою контролю ефективності і можливості внесення покращень в діючу в установі систему захисту інформації;

– періодично проводити аналіз порушень режиму конфіденційності;

– застосовувати оцінку інформації (метод ранжування джерел інформації, самої інформації та способів її отримання);

– інструктувати і навчати працівників практичним діям із захисту інформації;

– складати та регулярно оновлювати склад (перелік, список, матрицю) захищеної інформації, складати та вести перелік (опис) захищених паперових, машиночитаних та електронних документів установи;

– періодично інструктувати персонал щодо його дій в екстремальних ситуаціях.

СПИСОК ІНФОРМАЦІЙНИХ ДЖЕРЕЛ

1. Про інформацію [Електронний ресурс] : Закон України № 2657-XII (2657-12) від 2.10.1992 р. – Режим доступу : http://zakon2.rada.gov.ua/laws/show. – Назва з екрана. – Дата звернення: 15.11.19.

2. Про Національну програму інформатизації [Електронний ресурс] : Закон України № 74/98-ВР від 4.02.1998 р. – Режим доступу : http://zakon2.rada.gov.ua/laws/show. – Назва з екрана. – Дата звернення: 05.11.19.

3. Про електронні документи та електронний документообіг: Закон України : прийнятий ВРУ 22.05.2003 р. № 851–IV // Відомості Верховної Ради України. - 2003 р. - №44. – С.1175-1176.

4. Інформація та документація. Базові поняття. Терміни та визначення: ДСТУ 2398–94. / [Чинний від 1995–02–01]. – К. : Держспоживстандарт України, 1995. – I, 45 с. – (Національний стандарт України).

5. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки: Закон України: прийнятий ВРУ 09.01.2007 р. № 537–V // Відомості Верховної Ради України. - 2007 р. - №125. – С.1120-1124.

6. Інформація і документація. Словник термінів (ISO 5127:2001, IDT): ДСТУ ISO 5127:2007 / [Чинний від 2007–14–12]. – К. : Держспоживстандарт України, 2007. – III, 389 с. – (Національний стандарт України).

7. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України: прийнятий ВРУ 05.07.1994 р. № 81/94-ВР // Відомості Верховної Ради України. - 1994 р. - №31. – С.1115-1158.

8. Про захист персональних даних: Закон України: прийнятий ВРУ 01.06.2014 р. № 2297-VI // Відомості Верховної Ради України. - 2010 р. - №34. – С.1105-1150.

9. Про електронні документи та електронний документообіг: Закон України : прийнятий ВРУ 22.05.2003 р. № 851–IV // Відомості Верховної Ради України. - 2003 р. - №44. – С.1175-1176.

10. Про Національну програму інформатизації: Закон України: прийнятий ВРУ 4.02.1998 р. № 74/98 // Відомості Верховної Ради України. – 1998. – №32. – С.1480-1490.

11. Про основи національної безпеки України: : [Електронний ресурс] : Закон України : № 964-IV від 19.06.2003 р. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/964-15. – Назва з екрана. – Дата звернення: 14.11.19.

12. Комплектування фонду документів. Бібліографування. Каталогізація. Терміни і визначення: ГОСТ 7.76 – 96. / [Чинний від 1998– 01–01]. – Минск.: Изд–во стандартов, 1997. – 52 с. – (Система стандартів з інформації, бібліотечної та видавничої справи).

13. Про місцеві державні адміністрації: [Електронний ресурс] : Закон України: № 586-XIV від 09.04.1999 р. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/586-14. – Назва з екрана. – Дата звернення: 09.11.19.

14. Про захист інформації в автоматизованих системах [Електронний ресурс] : Закон України № 80/94-ВР від 05.07.1994 р. – Режим доступу : http://zakon2.rada.gov.ua/laws/show. – Назва з екрана. – Дата звернення: 25.11.19.

15. Уніфіковані системи документації. Основні положення: ГОСТ 6.10.1–88/ [Чинний від 1995–18–03]. – К. : Держспоживстандарт України, 1995. – III, 360 с. – (Національний стандарт України).

16. Про інформацію [Електронний ресурс] : Закон України № 2657-XII (2657-12) від 2.10.1992 р. – Режим доступу : http://zakon2.rada.gov.ua/laws/show. – Назва з екрана. – Дата звернення: 15.11.19.

17. Алексенцев А. И. Понятие и назначение комплексной системы защиты информации / А. И. Алексенцев // Вопросы защиты информации. – 2000. – № 2. – С. 2-3.

18. Андрєєва В. І. Діловодство: практичний посібник / В.І. Андрєєва. – М.: ТОВ «Управління персоналом», 2005. – 234 с.

19. Андрианов В. В. Обеспечение информационной безопасности бизнеса / В. В. Андрианов, С. Л. Зефиров, В. Б. Голованов, Н. А. Голдуев. – М.: Альпина Паблишерз, 2011. – 338 с.

20. Анин Б. Ю. Защита компьютерной информации / Б. Ю. Анин. – Санкт-Петербург.: БХВ-Петербург, 2000. – 384 с.

21. Баранов О. А. Інформаційний суверенітет або інформаційна безпека? / О. А. Баранов // Національна безпека та оборона. – 2001. – № 1. – С. 70-76.

22. Барсуков В. С. Безпека: технології, засоби, послуги / В. С. Борсуков. – М.: 2001 – 496 с.

23. Батюк А. Є. Інформаційні системи в менеджменті / А. Є. Батюк, З. П. Двуліт, К. М. Обельовська та ін. – Львів: Інтелект-Захід, 2004. – С. 343–384.

24. Белов Е. Б. Основы информационной безопасности [Електронний ресурс] / Е. Б.Белов, В. П. Лось. – Електронні дані. – Режим доступу: http://www.proklondike.com/books/defence/defence_belov_los_osnovi_security.html. – Назва з екрана. – Дата звернення: 15.11.19.

25. Блинов А. М. Информационная безопасность / А. М. Блинов. – Санкт-Петербург: ГУЭФ, 2011. – Ч. 1. – 96 с.

26. Бурячок В. Л. Метод визначення найбільш значимих загроз із «генеральної сукупності» загроз інформаційним ресурсам на підставі їх якісних та кількісних показників / В. Л. Бурячок, Я. В. Невойт // Сучасний захист інформації. – 2014. – № 3. – С. 18-21.

27. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. – К.: ДУТ, 2015.– 288 с.

28. Власова Л. А. Защита информации / Л. А. Власова. – Хабаровск: РИЦ ХГАЭП, 2007. – 84 с.

29. Галицкий А. В. Защита информации в сети – анализ технологий и синтез решений / А. В. Галицкий. М.: ДМК Пресс, 2005. – 616 с.

30. Грибунин В. Г. Комплексная система защиты информации на предприятии / В. Г. Грибунин, В. В. Чудовский. – М.: Академия, 2009. – 416 с.

31. Для чего нужна автоматизация делопроизводства: [Електронний ресурс]. – Електронні дані. – Режим доступу: http://www.mdi.ru/library/analit/avtom.html. – Назва з екрана. – Дата звернення: 15.11.19.

32. Замкова Т. В. Проблемы защиты информации в современных информационных системах [Електронний ресурс] / Т.В. Замков. – Електронні дані. – Режим доступу: http://www.rae.ru/snt/?section =content&op=show_article&arti. – Назва з екрана. – Дата звернення: 15.11.19.

33. Зубок М. І. Інформаційна безпека / М. І. Зубок – К.: КНТЕУ, 2005. – 93 с.

34. Зубок М. І. Правове регулювання безпеки підприємницької діяльності / М. І. Зубок. – К.: КНТЕУ, 2005. – 76 с.

35. Иванов О. В. Информационная составляющая современных войн / О.В. Иванов // Вестник Московского университета. Сер. 18: Социология и политология. – 2004. – № 4. – С. 64-70.

36. Информационная технология. Методы защиты. Практическое руководство для менеджмента информационной безопасности: ISO 9001[Електронний ресурс]. – Електронні дані. – Режим доступу: http://www.klubok.net/Downloads-index-req-viewdownloaddetails-lid-362.html. – Назва з екрана. – Дата звернення: 15.11.19.

37. Інформаційне законодавство: збірник законодавчих актів / Ред. Ю. С. Шемшученко, К. С. Чиж. – Т. 5: Міжнародно-правові акти в інформаційній сфері. – К.: Юридична думка, 2005. – 328 с.

38. Карпенко О. О. Сучасне діловодство : навч. посіб. / О. О. Карпенко, М. М. Матліна. – Х. : Нац. аерокосм. ун-т «Харк. авіац. ін-т», 2009. – 75 с.

39. Коваленко Ю. О. Забезпечення інформаційної безпеки на підприємстві [Електронний ресурс] / Ю. О. Коваленко. – Електронні дані. – Режим доступу: http://www.econindustry.org/arhiv/html/2010/st_51_18.pdf . – Назва з екрана. – Дата звернення: 13.02.2017.

40. Коваленко Ю. О. Організація систем інформаційної безпеки підприємств [Електронний ресурс] / Ю. О. Коваленко. – Електронні дані. – Режим доступу: http://fullref.ru/job_05dc6b4cd1d240ca816e0bf9a1e0c2d4.html. – Назва з екрана. – Дата звернення: 15.11.19.

41. Конеев И. Р. Информационная безопасность предприятия / И. Р. Конеев, А. В. Беляев. – Санкт-Петербург: БХВ-Петербург, 2003. – 752 с.

42. Користін О. Є. Економічна безпека: навч. посібник / О. Є. Користін, О. І. Барановський, Л. В. Герасименко. – К.: Центр навчальної літератури, 2010. – 368 с.

43. Кормич Б. А. Організаційно-правові основи політики інформаційної безпеки України: автореф. дис. ... д-ра юрид. наук / Б. А. Кормич. – Харків, 2004. – 44 с.

44. Кримінальний Кодекс України [Електронний ресурс]. – Електронні дані. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/2341-14. – Назва з екрана. – Дата звернення: 15.11.19.

45. Кузнецов С. Л. Выбор и опытное внедрение системы электронного документооборота / С. Л. Кузнецов // Секретарское дело – 2001. – № 3. – С.17–22.

46. Кузьменко Б. В. Захист інформації. Організаційно-правові засоби забезпечення інформаційної безпеки: навч. посібник / Б. В. Кузьменко, О. А. Чайковська. – К.: Ліра, 2009. – Ч.1. – 83 с.

47. Кушнаренко Н. Н. Документоведенье [Електронний ресурс]: навч. посібник / Н. Н. Кушнаренко. – Електронні дані. – Режим доступу: http://vk.com/doc-64916839_263602110?hash=b6961d38bac833ae6a&dl=425727e28b9667dd45 – Дата звернення 15.11.19.

48. Литвинюк А. А. Основи інформаційної безпеки. Комплексна система захисту інформації: структура, встановлення та підтримка функціонування [Електронний ресурс] / А. А. Литвинюк. – Електронні дані. – Режим доступу: http://www.cvk.gov.ua /visnyk/pdf/2008_4/visnik_st_08.pdf. – Назва з екрана. – Дата звернення: 15.11.19.

49. Лукацкий А. В. Обнаружение атак / А. В. Лукацкий. – Санкт-Петербург: БХВ-Петербург, 2001. – 624 с.

50. Малюк А. А . Информационная безопасность: концептуальные и методологические основы защиты информации: учеб. пособие / А. А. Малюк. – М.: Горячая линия – Телеком, 2004. – 280 с.

51. Матвієнко О. В. Основи організації електронного документообігу: навч. посібник для студ. ВНЗ / О. В. Матвієнко, М. Н. Цивін. – К.: Центр навчальної літератури, 2008. – 112 с.

52. Матиев Д. Ш. Средства защиты информации: проблема выбора и соответствия [Електронний ресурс] / Д. Ш. Матиев. – Електронні дані. – Режим доступу: http://bankir.ru/publikacii/s/sredstva-zaschiti-informacii-problema-vibora-i-sootvetstviya-5386161. – Назва з екрана. – Дата звернення: 15.11.19.

53. Мотив [Електронний ресурс]. – Електронні дані. – Режим доступу: http://www.motiw.ru/. – Назва з екрана. – Дата звернення: 15.11.19.

54. Низенко Е. І. Забезпечення інформаційної безпеки підприємництва: навч. посібик / Е. І. Низенко, В. П. Каленяк. – К.: МАУП, 2006. – 154 с.

55. Общие критерии оценки безопасности информационных технологи: ISO 15408 [Електронний ресурс]. – Електронні дані. – Режим доступу:

http://iso27000.ru/standarty/iso-15408-obschie-kriterii-ocenki-bezopasnosti-informacionnyh-tehnologii . – Назва з екрана. – Дата звернення: 15.11.19.

56. Ортинський В. Л. Економічна безпека підприємств, організацій та установ [Електронний ресурс] / В. Л. Ортинський. – Електронні дані. – Режим доступу: http://westudents.com.ua/glavy/16615-64-metodi-sposobi-zahistu-nformats.html. – Назва з екрана. – Дата звернення: 15.11.19.

57. Охріменко Г. В. Основні принципи та проблеми впровадження електронного документообігу в організації / Г. В. Охріменко // Наукові записки Національного університету «Острозька академія». Серія «Культура і соціальні комунікації». – Острог, 2009. – Ч. 1. – С. 300-307.

58. Палеха Ю. І. Загальне документознавство: навч. посібник / Ю. І. Палеха, Н. О. Леміш. – 3-тє вид., К.: Ліра-К, 2012. – 432 с.

59. Петренко С. А. Политикf безопасности компании при работе в интернет / С. А. Петренко, В. А. Курбатов. – М.: ДМК Пресс, 2011. – 396 с.

60. Помаранчева книга. Критерії оцінки достовірності обчислювальних систем Міністерства оборони [Електронний ресурс]. – Електронні дані. – Режим доступу: http://www.securitylab.ru/informer/240650.php. – Назва з екрана. – Дата звернення: 05.04.2016.

61. Про акціонерні товариства: [Закон України: прийнятий ВРУ 17 вересня 2008 р. № 514-17] // Відомості Верховної Ради України. – 2008. № 59-51. – 384с.

62. Про електронний цифровий підпис: [Закон України: прийнятий ВРУ 22 травня 2003 р.]// Відомості Верховної Ради України. – 2003. – № 36. – 276 с.

63. Про електронні документи та електронний документообіг [Закон України: прийнятий ВРУ 22 травня 2003 р. № 851-15] // Відомості Верховної Ради України. – 2003. – № 36. – 275 с.

64. Про концепцію національної програми інформатизації: [Закон України: прийнятий ВРУ 04 лютого 1998 р. № 75/98-ВР] // Відомості Верховної Ради України. – 1998. – № 27-28. – С. 182.

65. Про національну програму інформатизації: [Закон України: прийнятий ВРУ 04 лютого 1998 року № 74/98-ВР] // Відомості Верховної Ради України. – 1998. – № 27-28. – С. 181.

66. Про основи національної безпеки України: [Закон України: прийнятий ВРУ 19 червня 2003 р. № 964-IV] // Відомості Верховної Ради України. – 2003. – № 39. – С. 351.

67. Про Стратегію національної безпеки України: [Указ Президента України: затв. ВРУ 12 лютого 2007 р. № 105/200] // Офіційний вісник України. – 2007. – № 11. – 389 с.

68. Рекомендації парламентських слухань з питань розвитку інформаційного суспільства в Україні: [Постанова Верховної Ради України 01 грудня 2005 р.] // Відомості Верховної Ради України. – 2006. – № 15. – 131 с.

69. Роговец В. С. Информационные войны в современном мире: причины, механизмы, последствия / В. С. Роговец // Персонал. – 2013. – № 5. – С. 34-40.

70. Рощин С. К. Психологическая безопасность: новый подход к безопасности человека, общества и государства [Електронний ресурс] / С. К. Рощин, В. А. Соснин. – Режим доступу: http://www.bookap.by.ru/psywar/grachev/ gl6.shtm. – Назва з екрана. – Дата звернення: 15.11.19.

71. Сельченкова С. В. Автоматизированные системы управления документами / С. В. Сельченкова // Секретарь-референт. – 2005. – № 01 (26). – С. 12-15.

72. Системы менеджмента информационной безопасности: ISO 27001/17799 [Електронний ресурс]. – Електронні дані. – Режим доступу: http://17799.standardsdirect.org/ISO 27001. – Назва з екрана. – Дата звернення: 15.11.19.

73. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования: ГОСТ 28147-89 [Електронний ресурс]. – Електронні дані. – Режим доступу: http://www.gosthelp.ru/gost/gost11287.html. – Назва з екрана. – Дата звернення: 15.11.19.

74. Степанов Е. І. Информационная безопасность и защита информации / Е. І. Степанов, І. С. Корнеев. – М.: Инфра – М.: 2001. – 333 с.

75. Столингс В. Основы защиты сетей. Приложения и стандарты / В. Столингс. – М.: Издательский дом «Вильямс», 2002. – 432 с.

76. Страхарчук В. П. Інформаційні системи та технології в банках [Електронний ресурс] / В. П. Страхарчук. – Електронні дані. – Режим доступу: http://pidruchniki.com/15070412/bankivska_sprava/kriptografichniy_zahist_informatsiyi_sistemi_rozpodilu_klyuchiv. – Назва з екрана. – Дата звернення: 15.11.19.

77. Хоменко М. Ф. Посібник з діловодства: навч. посібник / М. Ф. Хоменко, О. В. Грабарь. – 2-е вид., випр. і доп.. – К.: Генеза, 2003. – 103 с.

78. Система електронного документообігу органу виконавчої влади. Технічні умови ТУ У 30.0-33240054-001:2005 [Електрон.ресурс]. – Режим доступу : http://www.stc.gov.ua. – Дата звернення 17.11.19

79. Скібіцька Л. І. Діловодство : Навч.посібник / Укладач Л. І.Скібіцька. – Київ : Центр навчальної літератури, 2006. – 224 с.

80. Филенко Е. Н. Появление персональных компьютеров и начало формирования новой «компьютерной» технологии / Е. Н. Филенко // Делопроизводство. – 2008. – №1. – С. 47–44.

81. Філіпова Л. Я. Системи управління електронним документообігом: загальні поняття термінології, організації, технології (зарубіжний досвід) / Л. Я. Філіпова // Вісник Книжкової палати. – 2001. – № 4. – С. 15–18.

82. Хандадашева Л. Н. Комп'ютер й інша оргтехніка для секретаря-референта / Л.Н. Хандадашева. – Ростов на Дону, 2003. – 384 с.

83. Черноскутова А. І. Інформатика / А. І.Черноскутова. – СПб. 2005.– 272 с.

84. Ценные бумаги. Формат для передачи номеров заголовков и сертификатов: ISO 8532:1986 [Електронний ресурс]. – Електронні дані. – Режим доступу: http://www.gosthelp.ru/gost/gost11287.html. – Назва з екрана. – Дата звернення: 05.11.2019.

85. Юдін О. К. Захист інформації в мережах передачі даних: підручник / О. К. Юдін, О. Г. Корченко, Г. Ф. Конахович. – К.: Інтерсервіс, 2009. – 716 с.