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:

«Організація та управління службою інформаційної безпеки підприємства»
(за матеріалами ГПУ "Полтавагазвидобування")

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

Виконавець роботи Козирєва Аліна Вікторівна

_____
(підпис, дата)

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

_____
(підпис, дата)

Рецензент

Полтава 2019

ЗМІСТ

ВСТУП

В процесі діяльності будь–яке підприємство оперує інформацією як специфічним товаром високої цінності. Володіння інформацією, її оптимальне використання забезпечує ефективне функціонування суб'єкта господарювання як цілісного комплексу. Тому проблема забезпечення інформаційної безпеки є надзвичайно актуальною на сучасному етапі розвитку інформаційних технологій, який супроводжується введенням інформаційних систем у всі сфери діяльності людини, постійною взаємодією підприємств на теренах саме інформаційного простору.

Інформаційна безпека підприємства характеризується конфіденційністю, цілісністю, доступністю та може розглядатися як сукупність таких елементів: безпечні умови функціонування інформаційних технологій, побудова ефективної інфраструктури інформаційного простору, цілісного ринку інформації, створення оптимальних умов для проходження інформаційних процесів.

Метою інформаційної безпеки є збереження цілісності, повноти та точності інформації, мінімізація ризику несанкціонованих змін у інформаційних системах.

Забезпечення незмінності існуючого порядку функціонування інформаційних систем має відбуватися на трьох рівнях: адміністративному – за допомогою політики безпеки організації, локальному - шляхом формування специфічних правил та рекомендаційних норм для персоналу, об'єктному – використання сертифікованих, легальних засобів програмного та апаратного забезпечення.

Суб'єкти впливу на інформаційну систему підприємства поділяються на 2 групи: зовнішні (злочинці, хакери, їх об'єднання тощо) та внутрішні (персонал, який має доступ до інформаційних систем та технічних засобів підприємства).

Аніловська Г.Я. одним із методів забезпечення інформаційної безпеки підприємства називає стандартизацію інформаційної структури інформаційної

системи, елементами якої є форми існування і подання інформації у цілому, а зв'язками – операції перетворення інформації в системі. Стандартизація цього типу полягає у запровадженні єдиних правил введення, зберігання, аналізу, оброблення інформації.

Одним з найбільш ефективних методів оптимізації рівня інформаційної безпеки є конкретна програма державної політики у цій сфері, яка повинна формуватися відповідно до норм чинного законодавства.

Варто зазначити, що на стан інформаційних систем можуть вплинути так звані "природні" фактори, тобто фактори, не зумовлені несанкціонованими діями суб'єктів.

Всі методи забезпечення інформаційної безпеки підприємства можна об'єднати у три групи: правові, організаційні та програмно-технічні.

Правові методи включають сукупність нормативно–правових актів, які регулюють відносини, пов'язані з використанням інформації в діяльності підприємства. Програмно-технічні методи реалізуються за допомогою засобів програмного та апаратного забезпечення. Організаційні методи полягають в забезпеченні збереження конфіденційної інформації підприємства шляхом формування корпоративної системи захисту.

Незважаючи на використання вищезазначених методів, забезпечення інформаційної безпеки підприємства на належному рівні можливе лише тоді, коли інформаційна складова економічної безпеки розглядатиметься як невід'ємний елемент процесу управління підприємством.

Таким чином, використання інформаційних технологій в підприємницькій діяльності значно підвищує ефективність процесів, зменшує затрати на їх проведення, проте в той же час зумовлює виникнення нових загроз для функціонування підприємства. Отже, інформаційна безпека фактично відображається у ступені захищеності важливої для підприємства інформації від впливу дій випадкового або навмисного характеру, які можуть завдати збитків підприємству. Оптимальним варіантом забезпечення інформаційної безпеки є дотримання систематичного поєднання правових, організаційних та

програмно-технічних методів у процесі управління підприємством.

Мета дипломної роботи полягає у вивченні основних напрямків, принципів та методів організації і управління службою інформаційної безпеки на підприємстві.

Завдання дипломної роботи обумовлені її метою:

- розкрити сутність докуметних потоків на підприємстві;

- розглянути основні напрями забезпечення інформаційної безпеки документів;

- проаналізувати законодавчу базу підприємства і нормативно-правові аспекти інформаційної безпеки;

- навести загальну характеристику фінансово-господарської діяльності ГПУ "Полтавагазвидобування";

- провести оцінку стану забезпечення інформаційної безпеки на ГПУ "Полтавагазвидобування";

- розглянути основні принципи та методи забезпечення інформаційної безпеки на ГПУ "Полтавагазвидобування";

- дослідити організаційне забезпечення ефективності системи інформаційної безпеки ГПУ "Полтавагазвидобування";

- розглянути порядок формування директив контролю інформаційної безпеки на основі інформаційного аудиту ГПУ "Полтавагазвидобування";

- проаналізувати ресурсне забезпечення ефективності системи інформаційної безпеки ГПУ "Полтавагазвидобування".

Об’єктом дослідження для даної дипломної роботи є ГПУ "Полтавагазвидобування".

Предметом дослідження є основні напрямки, принципи та методи забезпечення інформаційної безпеки на ГПУ "Полтавагазвидобування".

Методи дослідження: обумовлені об’єктом і предметом дипломної роботи.

Для розв’язання визначених завдань, досягнення мети застосовано комплекс взаємодоповнюючих методів дослідження: методи системного аналізу, методи причинно-наслідкового аналізу, методи прямого структурного аналізу. При

опрацюванні вихідної інформації були використані загальнонаукові методи аналізу, синтезу, абстрагування та узагальнення.

Результатит дослідження були апробовані на студентській конференції і опублікована стаття за результатами конференції

Практичне значення роботи полягає в розробці рекомендацій щодо вдосконалення організації і управління службою інформаційної безпеки підприємства, а саме ГПУ "Полтавагазвидобування".

Наукова новизна отриманих результатів дослідження полягає в наступному: удосконалено:

− підхід до раціональної організації управління службою інформаційної безпеки підприємства, а саме ГПУ "Полтавагазвидобування".

Отримало подальший розвиток:

− раціональний підхід до організації та управління службою інформаційної безпеки підприємства ГПУ "Полтавагазвидобування".

За матеріалами дослідження опублікована стаття: Бурдун А. В. Організація та управління службою інформаційної безпеки підприємства А.В. Бурдун, Л.М.Колєчкіна// Збірник наукових статей магістрів. Інституту економіки, управління та інформаційних технологій. – Полтава : ПУЕТ, 2019. – Ч. 1. – С. 231-236.

Робота складається зі вступу, трьох розділів, висновків; містить 105 сторінок тексту, 8 рисунків, 5 таблиць, 3 додатків. Список джерел включає 85 найменувань літератури, 8 електронних публікацій.

РОЗДІЛ 1
ТЕОРЕТИЧНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

1.1 Сутність теорії захисту інформації

На сьогодні 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 угроз безпеки інформації, і насамперед несанкціонованого доступу до неї зловмисника [11]. Захисту підлягає будь документована інформація, неправомірне поводження з якою може завдати шкоди її власнику, власнику, користувачеві або іншій особі. Захисту потребує не тільки конфіденційний докомент. 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.

Багато авторів по-різному трактують поняття «інформаційна безпека». Порівняння поняття подано у таблиці 1.1.

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 патогенних 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. Напрямки захисту інформації на підприємстві

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 перебуває інформація:

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

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

- соціотехнічне (людино-машинне).

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.

Багато авторів по-різному трактують поняття «інформаційна безпека». Порівняння поняття подано у таблиці 1.1.

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.

Таблиця 1.1 – Визначення та порівняння поняття «інформаційна безпека» [розроблено автором]

Автор	Визначення
О.Г. Додонов	Визначає інформаційну безпеку як стан захищеності інформаційного простору, що забезпечує формування та розвиток цього простору в інтересах особистості, суспільства та держави.
Б.М Кормич	Інформаційна безпека – це захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечу-

	ють гарантовані Конституцією умови існування і розвитку людини, всього суспільства і держави.
І.М.Панарін	На його думку, інформаційна безпека – стан інформаційного середовища суспільства і політичної еліти, який забезпечує її формування і розвиток в інтересах керівництва країни, громадян і суспільства.
Ю.А. Фісун	Характеризує інформаційну безпеку як «стан захищеності інформаційного середовища, який відповідає інтересам держави, за якого забезпечується формування, використання і можливості розвитку незалежно від впливу внутрішніх та зовнішніх інформаційних загроз».
В.К.Гасеський, В.А.Авраменко	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.
А.А. Тер-Акопов	Під інформаційною безпекою він розуміє «стан захищеності інформації, яка забезпечує життєво важливі інтереси людини».
В.І. Ярочкін	визначає безпеку як «стан захищеності особи, суспільства і держави від зовнішніх та внутрішніх небезпек і загроз, який базується на діяльності людей, суспільства, держави, світового співтовариства з виявлення (вивчення), попередження, послаблення, ліквідації і відбиття небезпек і загроз, здатних загубити їх, лишити фундаментальних матеріальних і духовних цінностей, завдати неприйнятної шкоди, закрити шлях для прогресивного розвитку»
Р.Л. Калюжний	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, розповсюдженням, зберіганням та використанням інформації.
О.В.Соснин	Інформаційна безпека – це «стан захищеності національних інтересів у інформаційній сфері, які визначаються сукупністю збалансованих інтересів особистості, суспільства і держави».

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.

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.)

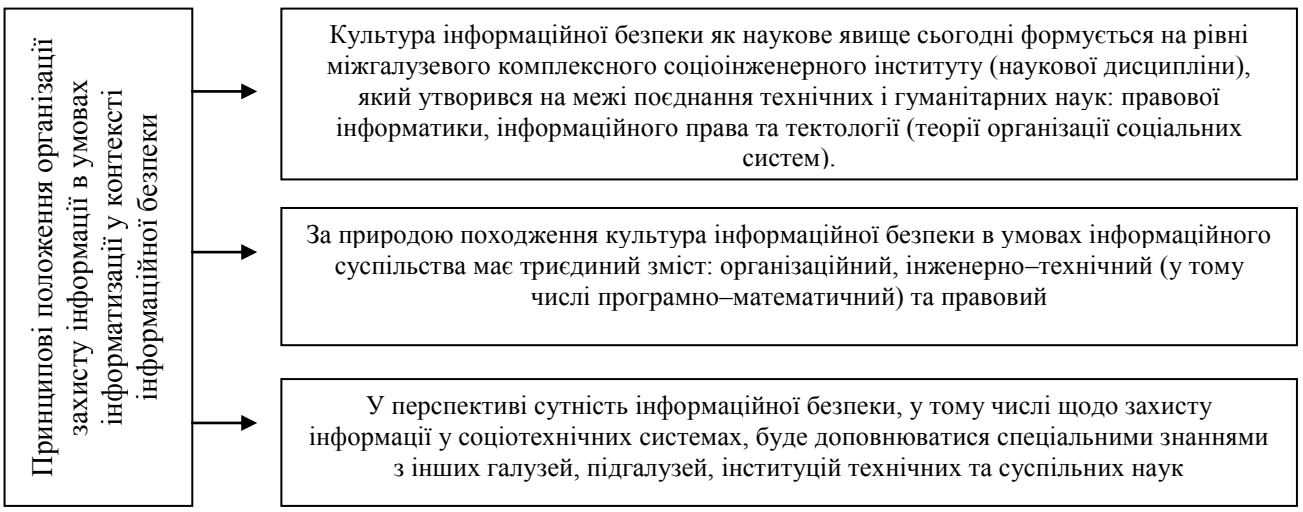

Рисунок 1.4 Принципові положення організації захисту інформації в умовах інформатизації у контексті інформаційної безпеки

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-правова база організації інформаційної безпеки 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 СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ГПУ "ПОЛТАВАГАЗВИДОБУВАННЯ"

2.1. Загальна характеристика діяльності ГПУ "Полтавагазвидобування"

Об'єктом дослідження нашої роботи є ГПУ "Полтавагазвидобування", які знаходиться за адресою: м. Полтава, вул. Фрунзе, 173.

Підприємство є юридичною особою, має самостійний баланс, банківські рахунки, печатку та штамп встановленого зразку, фірмові бланки, емблеми, товарний знак та іншу атрибутику.

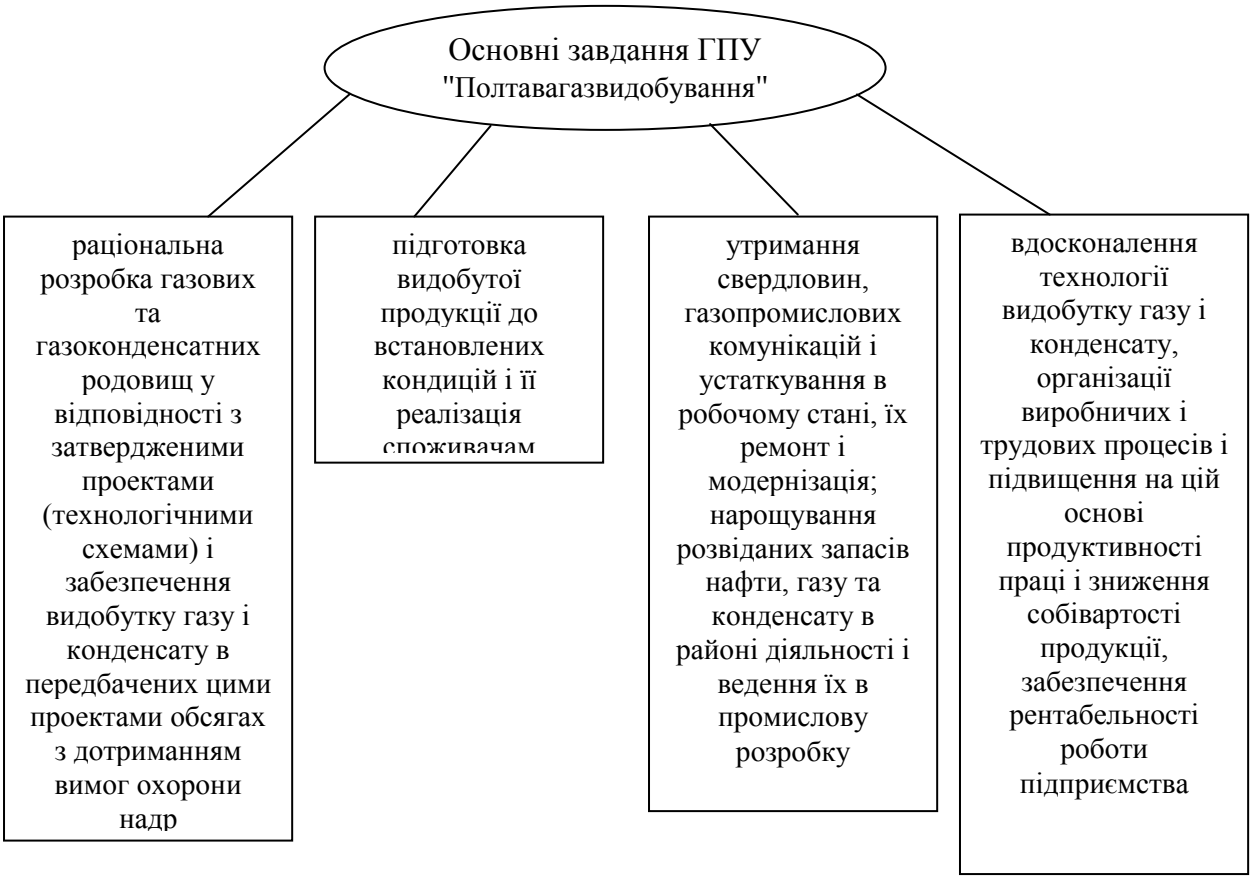

Рисунок 2.5 – Основні завдання ГПУ «Полтавагазвидобування

Над виконанням цих завдань і працюють всі підрозділи ГПУ "Полтавагазвидобування".

Газовидобувне управління очолює директор. У відповідності з головними завданнями ГПУ "Полтавагазвидобування" на нього покладені такі функції:

- керівництво виробничо-господарською діяльністю підприємства і окремих його підрозділів;

- організація всієї роботи апарату управління і ГПУ "Полтавагазвидобування" в цілому та контроль за роботою апарату і виробничих підрозділів;

- спрямування діяльності колективу на забезпечення раціональної розробки родовищ газу і конденсату, видобутку встановлених обсягів газу і конденсату та їх реалізації;

- підвищення ефективності виробництва і продуктивності праці, зниження собівартості продукції.

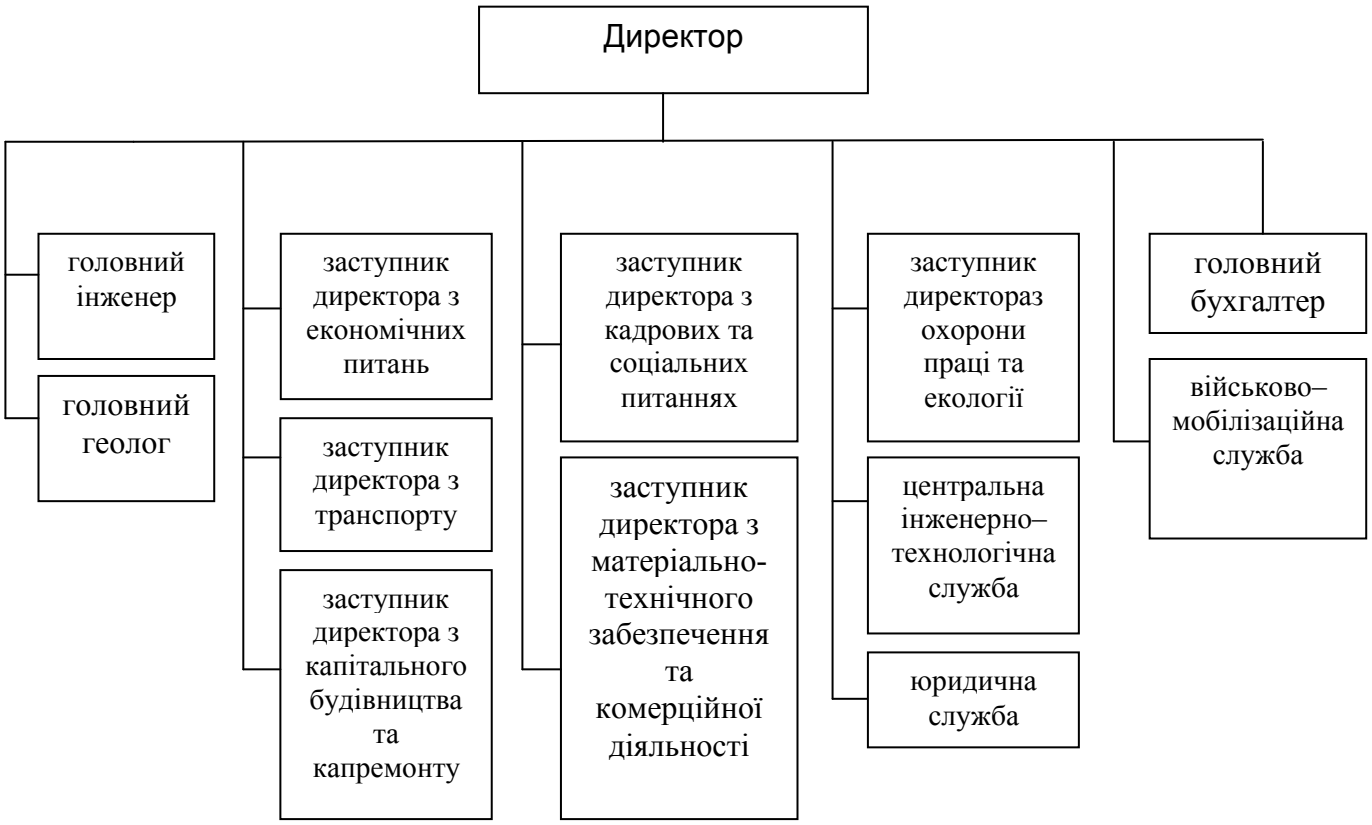

Рисунок 2.6 – Підпорядкованість директору ГПУ«Полтавагазвидобування

Головному інженеру підпорядковані: виробничо–технічний відділ, механо–енергетичний відділ, служба з технічного нагляду, відділ газопереробки, програмно–інформаційний відділ. Він організовує діяльність підлеглих відділів для інженерно–технічного забезпечення планів виробництва, поточних і перспективних планів впровадження нової техніки і передової

технології.

Виробничо-технічний відділ розробляють заходи з вдосконалення процесу виробництва і покращенню використання обладнання, аналізують виконання встановлених режимів і технічних норм роботи обладнання, оформляють необхідну технічну документацію, організовують технічний облік роботи обладнання.

Механічно–енергетичний відділ керує механічно–ремонтною службою ГПУ "Полтавагазвидобування" з метою забезпечення раціональної експлуатації і продовження тривалості роботи обладнання. На нього покладається контроль за правильною експлуатацією механічного обладнання та здійснює забезпечення безперебійного енергопостачання виробничих об'єктів, контроль за експлуатацією енергетичного обладнання, ремонтом і своєчасним вводом в експлуатацію об'єктів енергопостачання [24].

Головним завданням служби з технічного нагляду є забезпечення утримування парових та водогрійних котлів, посудин, що працюють під тиском, вантажопідіймальних механізмів, трубопроводів пари і гарячої води у справному стані і безпечних умов їх роботи.

Головною задачею програмно–інформаційного відділу є програмне забезпечення апарату управління і структурних підрозділів та підтримка в робочому стані і нагляд за правильною експлуатацією:

- обладнання телефонного і радіозв'язку;

- обладнання комп'ютерної мережі.

Головним завданням відділу газопереробки являється організація виконання виробничих завдань переробки газу, оптимальної експлуатації технологічних установок і споруд газопереробного виробництва та газового виробництва ГПУ "Полтавагазвидобування", впровадження нових більш ефективних та удосконалення існуючих технологій газопереробки та постійний технічний нагляд, технічне обслуговування і проведення планово–попереджувальних та поточних ремонтів об'єктів газового господарства ГПУ "Полтавагазвидобування" [34].

Заступнику директора з охорони праці та екології підпорядковані: відділ охорони праці, відділ охорони навколишнього середовища та радіаційної безпеки.

Головним завдання відділу охорони праці і техніки безпеки є організація роботи по створенню безпечних і здорових умов праці, здійснення контролю за роботою виробничих підрозділів і служб ГПУ "Полтавагазвидобування" по покращенню умов праці, розробка санітарно–гігієнічних заходів по попередженню виробничого травматизму і профзахворювань.

Головним завданням служби охорони навколишнього середовища та радіаційної безпеки є організація, координація, аналіз і контроль за виконанням та додержанням норм і правил охорони навколишнього природного середовища та радіаційної безпеки.

На головного геолога покладена організація розробки планів геолого–технічних заходів на експлуатаційних об'єктах, контроль і оцінка їх виконання; визначення основних завдань, керівництво, контроль і координація діяльності підрозділів геологічної служби, затвердження планів роботи цих підрозділів, оцінка результатів їх виконання; систематичний аналіз стану запасів нафти, газу та конденсату на розроблюваних родовищах; оцінка підготовленості родовищ до розробки.

Головному геологу підпорядковані: група з інтенсифікації газовидобутку та дослідження свердловин, відділ геології, відділ розробки родовищ. Головним завданням відділу геології являється уточнення геологічної побудови газових і газоконденсатних родовищ, параметрів продуктивних пластів в період розбурювання і розробки, облік руху запасів газу і конденсату, приросту запасів і переводу їх у вищі категорії, керівництво розробкою перспективних і поточних планів видобутку газу , об'ємів закачки робочих агентів для ППТ і нових методів підвищення газовіддачі, забезпечення їх ефективності, облік і звітність по розробці родовищ, планування комплексу геофізичних досліджень, контроль за виконанням і обліком вказаних робіт, за охороною надр, оформленням договорів, матеріалів на ввід родовищ в розробку, перевід

свердловин на інші горизонти, видачу гірничих відводів, завдань на проектування, здійснення контролю за бурінням свердловин, раціональним використанням коштів на буріння.

Головним завданням групи інтенсифікації газовидобутку та дослідження свердловин є пошуки шляхів інтенсифікації газовидобутку, вибір свердловин і складання планів обробки привибійних зон, проведення цих обробок, визначення їх ефективності виконання гідродинамічних досліджень свердловин, обробка матеріалів досліджень [56].

Головною задачею відділу розробки родовищ являється впровадження затверджених схем і проектів розробки родовищ, постійне вдосконалення діючих систем розробки на родовищах, які експлуатуються, досягнення проектних рівнів видобутку газу і конденсату, вишукування шляхів подальшої інтенсифікації розробки і забезпечення проектної газоовіддачі пластів.

Заступник директора з економічних питань здійснює організацію систематичного комплексного аналізу виробничо–господарської діяльності ГПУ "Полтавагазвидобування" і його підрозділів; розробляє заходи по підвищенню ефективності виробництва, продуктивності праці, покращенню використання основних і оборотних фондів, трудових і матеріальних ресурсів. Безпосередньо заступнику начальника з економічних питань підпорядковані:

- планово–економічний відділ;

- відділ організації праці та зарплати.

Головним завданням ПЕВ є організація планово–економічної роботи управління: розробка планів виробництва, аналіз і узагальнення результатів роботи, виявлення невикористаних резервів і підвищення ефективності виробництва.

Відділ організації праці та зарплати займається вдосконаленням організації праці, технічного нормування, впровадженням прогресивних форм і систем оплати праці і матеріального стимулювання.

Заступнику директора з кадрових та соціальних питань підпорядковані: відділ кадрів, фельдшерсько–оздоровчий пункт, соціально–господарський

відділ.

Відділ кадрів веде підбір робітників потрібної кваліфікації, вивчення ділових якостей працівників, перевірку розміщення і раціональності їх використання у відповідності зі спеціальністю, рівнем підготовки і досвідом роботи.

На соціально–господарський відділ покладено визначення потреби і своєчасне оформлення заявок на інвентар, оргтехніку, канцелярське приладдя, забезпечення ними працівників ГПУ "Полтавагазвидобування", контроль за станом робочих приміщень та їх своєчасний ремонт, забезпечення чистоти і порядку та ін.

Головному бухгалтеру підпорядковані: бухгалтерія, фінансова група. Бухгалтерія і фінансова група веде бухгалтерський облік господарської діяльності підприємства, здійснює контроль за витратою матеріальних цінностей і грошових коштів, складає бухгалтерські звіти і баланси, проводить розрахунки з робітниками і службовцями.

Заступник директора з капітального будівництва та капремонту здійснює керівництво над: відділом організації капітального будівництва та капремонту, проектно-кошторисним бюро, топографо–геодезичною групою. Відповідно відділ капітального будівництва керує капітальним будівництвом і капітальним ремонтом виробничих і житлових об'єктів [54].

Головним завданням проектно–кошторисного бюро являється виконання проектних та кошторисних робіт згідно затверджених завдань або дефектних актів в зазначений термін і в необхідному об'ємі.

Головним завданням топографо–геодезичної групи являється проведення топографо–геодезичних робіт та забезпечення топографічними матеріалами для вирішення питань: пошуків і розвідки родовищ газу і конденсату, складання проектної документації на розробку родовищ, проектування і будівництва об'єктів збору, підготовки і транспорту газу і конденсату, проектування і будівництво будівель і споруд в межах гірничих відводів родовищ, що знаходяться в промисловій розробці.

Заступник директора з матеріально–технічного забезпечення та комерційної діяльності здійснює керівництво над: договірною службою, відділом матеріально–технічного забезпечення та комерційної діяльності. Відділ матеріально–технічного забезпечення та комерційної діяльності постачає підрозділи ГПУ "Полтавагазвидобування" всіма видами матеріалів, інструменту, запасних частин і обладнання, необхідних для виконання плану виробництва [67].

Головним завданням договірної служби є упорядкування роботи щодо розробки, підготовки та укладання договорів, контрактів та угод, контроль за їх виконанням, ведення обліку договорів, що відображається в журналах реєстрації договорів.

Заступнику директора з транспорту підпорядковані: відділ безпеки руху, відділ транспорту і спецтехніки.

Головним завданням служби безпеки руху є забезпечення безаварійної роботи транспортних засобів та підвищення ефективності їх використання. Головним завданням відділу транспорту і спецтехніки є організація виробництва по технічному обслуговуванню і ремонту рухомого складу автотракторної техніки і підтриманню об'єктів, що експлуатуються в технічно справному стані.

В якості підрозділів основного виробництва ГПУ "Полтавагазвидобування" виступають цехи по видобутку газу і конденсату, координацію роботи яких здійснює центральна інженерно–технологічна служба (ЦІТС).

ЦІТС здійснює:

- оперативне керівництво роботою основних цехів по видобутку газу;

- цілодобовий контроль і координацію діяльності всіх виробничих підрозділів ГПУ при виконанні робіт на об'єктах основного виробництва;

- оперативне керівництво виконання плану організаційно–технічних заходів по забезпеченню планових завдань по видобутку газу, введенню в дію нових газових і газоконденсатних свердловин, проведенню підземного

поточного і капітального ремонту свердловин, введенню свердловин в дію із простою, виконання заходів по інтенсифікації видобутку газу і конденсату.

Одна з найважливіших характеристик фінансового стану підприємства – забезпечення стабільності його діяльності з позиції довгострокової перспективи. Вона пов'язана із загальною структурою балансу підприємства, його залежністю від кредиторів та інвесторів.

Фінансова стійкість підприємства характеризується насамперед співвідношенням між власним капіталом і зобов'язаннями. Чим більшу питому вагу в структурі пасивів займає позиковий капітал, тим вищий ризик кредиторів, нижча ймовірність повернення боргів.

Якщо підприємство фінансово стійке, то воно в стані "витримати" несподівані зміни ринкової кон'юнктури, і не виявитися на краю банкрутства.

Фінансове стійким можна вважати таке підприємство, яке за рахунок власних оборотних коштів спроможне забезпечувати формування запасів, не допускає невиправданої кредиторської заборгованості, своєчасно розраховується зі своїми зобов'язаннями.

Визначення типу фінансової стійкості підприємства проведено за даними табл. 2.1

Таблиця 2.1

Показники порогу рентабельності та запасу фінансової стійкості ГПУ "Полтавагазвидобування" за 2015–2017 рр.

№ з/п	Показник	2015 р.	2016 р.	2017 р.	Відхилення 2017 р. від 2015 р., (+,-)	
					абсолютне	відносне
1.	Операційний доход, тис. грн.	15572,0	16027,0	16182,0	610,0	103,92
2.	Операційні витрати, тис. грн. у тому числі:	15914,0	16206,0	24747,0	8833,0	155,5
	а) змінні витрати	10093,0	9285,0	16759,0	6666,0	166,05
	б) постійні витрати	5821,0	6921,0	7988,0	2167,0	137,23
3.	Прибуток (збиток) від операційної діяльності, тис. грн.	-114,0	-1,0	-686,0	-572,0	В 6 разів
4.	Маржинальний доход, тис. грн.	-342,0	-179,0	-8565,0	-8223,0	В 25 разів
5.	Частка (коефіцієнт)	0,022	0,011	0,529	0,51	В 24

	маржинального доходу в операційному доході					рази
6.	Поріг рентабельності, тис. грн.	264590,9	629181,8	15100,2	-249490,7	5,71
7.	Частка порогу рентабельності в операційному доході, %	1699,1	3925,7	93,3	-1605,8	X
8.	Зона фінансової стійкості, тис. грн.	15545,4	16272,7	16190,9	645,5	104,15
9.	Запас фінансової стійкості, %	99,8	101,5	100,1	0,3	X

Як свідчать дані табл. 8.1.2, протягом 2015–2017 рр. на ГПУ "Полтавагазвидобування" поріг рентабельності зменшується на 249490,7 тис. грн. або на 94,29%, зона фінансової стійкості збільшується на 645,5 тис. грн. або на 4,15%, запас фінансової стійкості збільшується на 0,3 пункти. Такі зміни являються негативними, оскільки характеризують зменшення маржинального доходу на 8223 тис. грн. або в 25 разів.

Отже, ліквідність балансу ГПУ "Полтавагазвидобування" не абсолютна, значить, в разі потреби підприємство не зможе оплати свої зобов’язання, але нестача високоліквідних активів протягом аналізованого періоду, 2015–2017 рр. має тенденцію до зменшення. Нестача високоліквідних активів протягом 2016–2017 рр. збільшується на 443 тис. грн., важколіквідних активів – на 550 тис. грн. Тобто з роками ситуація покращується.

Зміни рівня показників ліквідності та платоспроможності ГПУ "Полтавагазвидобування" протягом 2017–2019 рр. свідчать про погіршення фінансового стану підприємства, незадовільний стан ліквідності та платоспроможності, недостатність власних оборотних коштів для формування запасів..

Сума власних оборотних коштів протягом 2017–2019 рр. збільшується на 4689 тис. грн., в той час як загальна величина джерел формування запасів збільшується на 3516 тис. грн., що являється негативним моментом і свідчить про зменшення участі довгострокових зобов’язань та короткострокових кредитів у формуванні цих джерел, які зменшилися на 610 тис. грн. та 563 тис. грн. відповідно.

Коефіцієнт забезпеченості запасів відповідними джерелами формування менше одиниці, що свідчить про нестачу останніх, хоча протягом 2015–2017 рр. вона зменшується на 0,18 пунктів.

2.2. Оцінка стану захисту інформації на ГПУ "Полтавагазвидобування"

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

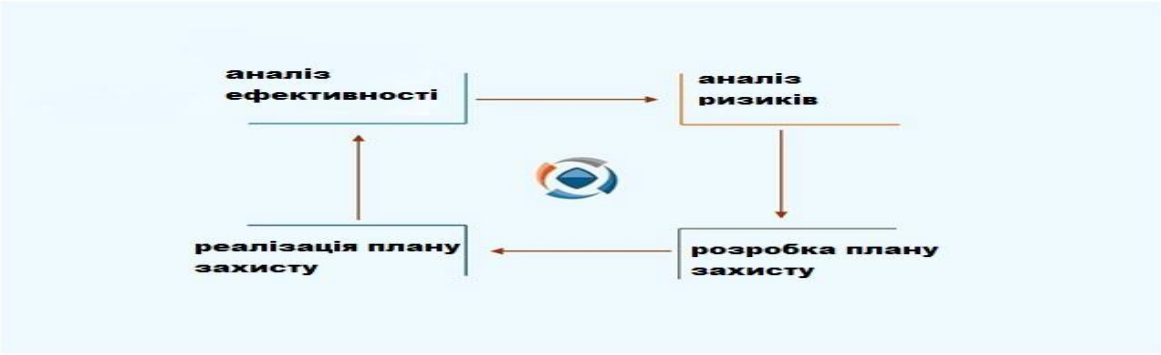

Рисунок 2.7 - Забезпечення ІБ системи «Гриф»

Основне завдання системи "Гриф" - дати можливість IT-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.

На рис.2.8 представлений можливий збиток по загрозам конфіденційності, цілісності та доступності, він повинен бути менше або дорівнює вартості інформації.

Рисунок 2.8 Можливі збитки по загрозам системи «Гриф»

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.

Дана методика оцінки ризиків основана на методі "Гриф", дозволяє змінювати основні характеристики інформаційних ресурсів і підбирати відповідні адекватні засоби захисту з урахуванням специфіки підприємства, не потребує спеціалістів і великих затрат.

Таблиця 2.10

Оцінка стану забезпечення інформаційної безпеки на ГПУ "Полтавагазвидобування"

Показники безпеки	балів
Рівень ефективності функціонування інформаційних систем	9
Рівень ефективності функціонування іншого основного та додаткового програмного забезпечення	8
Рівень захисту від вірусних атак	7
Рівень захисту від хакерських атак	5
Визначення переліку відомостей, що становлять комерційну таємницю, а також кола осіб, які в силу займаного службового положення на підприємстві мають до них доступ	8
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	9
Формування вимог до системи захисту в процесі створення і участь у проектуванні системи захисту, її випробування і приймання в експлуатацію	7
Планування, організація та забезпечення функціонування системи захисту інформації	8
Розподіл між користувачами необхідних реквізитів захисту, включаючи установку (періодичну зміну) паролів, управління засобами захисту комунікацій і крипто захист зраджувати, збережених і оброблюваних даних	9
Координація дій з аудиторською службою, спільне проведення аудиторських перевірок, контроль функціонування системи захисту і її елементів, тестування системи захисту	9
Організація навчання співробітників СІБ відповідно до їх функціональних обов'язків; навчання користувачів АС правилам безпечної обробки інформації	9
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	8
Вжиття заходів реагування на спроби несанкціонованого доступу до інформації та порушенням правил функціонування системи захисту	7
Виконання відновлювальних процедур після фактів порушення безпеки	8
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	8
Спільна робота з представниками інших організацій з питань безпеки - безпосередній контакт або консультації з партнерами або клієнтами	9
Постійна перевірка відповідності прийнятих в організації правил безпечної обробки інформації існуючим правовим нормам, контроль за дотриманням цієї відповідності	7
Загальний рейтинг стану інформаційної безпеки	7,9

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 ГПУ "Полтавагазвидобування" є недостатня захищеність програмного забезпечення від хакерських атак, оскільки підприємство використовує застарілі версії програм захисту своєї інформації [34].

Інформаційно-аналітична робота на ГПУ "Полтавагазвидобування" - це одна із основних внутрішньовиробничих функціональні складових безпеки підприємства.

Інформаційна складова полягає у здійсненні ефективного інформаційно-аналітичного забезпечення господарської діяльності ГПУ "Полтавагазвидобування".

Належні служби ГПУ "Полтавагазвидобування" виконують певні функції, які в сукупності характеризують процес створення та захисту інформаційної складової безпеки підприємства. До таких належать на ГПУ "Полтавагазвидобування":

- 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 економічної безпеки.

На ГПУ "Полтавагазвидобування" 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.

Оперативна реалізація заходів з розробки та охорони інформаційної складової економічної безпеки на ГПУ "Полтавагазвидобування" 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.

Основне завдання на ГПУ "Полтавагазвидобування" - 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 дезинформації конкурентів:

- через засоби масової інформації;

- через інформаційно-телекомунікаційні канали;

- через постачальників, суміжників, партнерів, клієнтів;

- шляхом організації псевдопросочування конфіденційної інформації;

- розробка програм захисту конфіденційної інформації [43].

Першою і найважливішою операцією на ГПУ "Полтавагазвидобування" 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, на ГПУ "Полтавагазвидобування" 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 на ГПУ "Полтавагазвидобування". ГПУ "Полтавагазвидобування" 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.

Для того, щоб розробити раціональну структуру служби інформаційної безпеки на ГПУ "Полтавагазвидобування", 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.

До завдань служби безпеки ГПУ "Полтавагазвидобування" 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;

- 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.

Додатково до обов'язків співробітників СІБ на ГПУ "Полтавагазвидобування" 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 [54].

Склад і розмір групи безпеки (СІБ) на ГПУ "Полтавагазвидобування" 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 ГПУ "Полтавагазвидобування":

- загроза - зовнішнє, відносно системи, джерело порушення властивості захищеність;

- об'єкт атаки - частина системи, на яку діє загроза;

- канал дії - середовище перенесення зловмисної дії.

Інтегральною характеристикою, яка об'єднує всі ці компоненти, є політика безпеки (ПБ) - 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, КС, операційної системи (ОС), 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.

ПБ інформації в КС є частиною загальної ПБ ГПУ "Полтавагазвидобування" 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 ОС, фізичного середовища та багатьох інших чинників.

Частина ПБ, яка регламентує правила доступу користувачів і процесів до ресурсів комп'ютерної системи (КС), становить правила розмежування доступу ГПУ "Полтавагазвидобування".

Розробка і підтримка ПБ ГПУ "Полтавагазвидобування" 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.

Водночас, вибір ПБ для ГПУ "Полтавагазвидобування" - 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 ГПУ "Полтавагазвидобування" 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 ГПУ "Полтавагазвидобування", 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 правильнее застосування ПБ є надзвичайно актуальною проблемою сучасних СЗІ.

Побудова ПБ на ГПУ "Полтавагазвидобування" - це зазвичай такі кроки:

- в інформацію вноситься структура цінностей і проводиться аналіз ризику;

- визначаються правила для будь-якого процесу користування певним видом доступу до елементів інформації, які мають певну оцінку цінностей.

Однак реалізація цих кроків є дуже складним завданням. Результатом помилкового або бездумного визначення правил ПБ здебільшого є руйнування цінності інформації без порушення ПБ. Тобто при незадовільній ПБ навіть надійна СЗІ може бути прозорою для зловмисника.

ПБ може бути викладена як на описовому рівні, так і за допомогою певної формальної мови. Вона є необхідною (а іноді й достатньою) умовою безпеки системи.

Формальний вираз політики безпеки на ГПУ "Полтавагазвидобування" 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.

ПБ на ГПУ "Полтавагазвидобування" 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.

ГПУ "Полтавагазвидобування" використовує дискреційну модель політики безпеки. Основою дискреційної політики безпеки (ДПБ) 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.

Назва пункту є дослівним перекладом з англійської терміна Discretionary policy, 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'єкту.

З практичної точки зору політику безпеки на ГПУ "Полтавагазвидобування" 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.

На політику верхнього рівня на ГПУ "Полтавагазвидобування" 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.

Сфера політики верхнього рівня на ГПУ "Полтавагазвидобування" повинна бути чітко окреслена. Можливо, це будуть комп'ютерні системи самої організації, а, можливо, і деякі аспекти використання домашніх комп'ютерів у співробітників цієї організації. Вироблення програми інформаційної безпеки верхнього рівня і її здійснення – це завдання певних посадових осіб, за виконання якої вони повинні регулярно звітувати.

Нарешті, політика інформаційної безпеки верхнього рівня на ГПУ "Полтавагазвидобування", 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.

Політика середнього рівня на ГПУ "Полтавагазвидобування" по кожному подібному аспекту передбачає вироблення відповідного документованого управлінського рішення, в якому зазвичай є:

- опис аспекта. Наприклад, якщо взяти застосування користувачами неофіційного програмного забезпечення, то про нього обов'язково має бути сказано, що це таке забезпечення, яке не було схвалено і / або закуплено на рівні організації;

- вказівка на область її застосування (розповсюдження тієї чи іншої 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. Наприклад, якщо для використання працівником неофіційного програмного забезпечення потрібно офіційний дозвіл, то має бути відомо, у кого і як його слід отримувати. Якщо повинні перевірятися диски, принесені з інших комп'ютерів, необхідно описати процедуру перевірки. Якщо неофіційне програмне забезпечення використовувати не можна, слід знати, хто стежить за виконанням цього правила;

- механізм забезпечення "законослухняності". Політика має містити загальний опис заборонених дій і покарання за них.

Політика безпеки нижнього рівня на ГПУ "Полтавагазвидобування" 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. Ось лише кілька прикладів-запитань, на які слід дати відповідь при розробці політики безпеки нижнього рівня:

- хто має право доступу до об'єктів, що підтримуються сервісом?
- за яких умов можна читати і модифікувати дані?
- як організований вилучений доступ до сервісу?

При формулюванні цілей, політика нижнього рівня на ГПУ "Полтавагазвидобування" може виходити з міркувань цілісності, доступності та конфіденційності, але вона не повинна на цьому зупинятися. Її цілі мають бути конкретнішими. Наприклад, якщо мова йде про систему розрахунку зарплати, можна поставити мету, щоб тільки працівникам відділу кадрів і бухгалтерії дозволялося вводити і змінювати інформацію. У більш загальному випадку цілі повинні пов'язувати між собою об'єкти сервісу та логічні з точки зору інформаційної безпеки, осмислені, дії з ними. З цілей зазвичай виводяться правила безпеки, що описують, хто, що і за яких умов може робити. Чим детальніше правила, чим більш формально вони викладені, тим простіше підтримувати їх виконання програмно-технічними заходами. З іншого боку, занадто жорсткі правила можуть заважати роботі користувачів на ГПУ "Полтавагазвидобування", і, ймовірно, їх доведеться часто переглядати.

Керівництву ГПУ "Полтавагазвидобування" необхідно знайти розумний компроміс, коли за прийнятну ціну буде забезпечений прийнятний рівень безпеки, а працівники не виявляться надмірно сковані.

2.3. Основні принципи та методи забезпечення захисту інформації на ГПУ "Полтавагазвидобування"

Незважаючи на те, що обов'язки та відповідальність співробітників служби інформаційної безпеки на ГПУ "Полтавагазвидобування" варіюються від організації до організації, можна виділити декілька основних положень, яким повинні відповідати функціональні обов'язки в усіх установах.

Організаційно групи СІБ на ГПУ "Полтавагазвидобування" 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 на ГПУ "Полтавагазвидобування" надається адміністративна підтримка, яка полягає у відображенні основних положень прийнятої політики безпеки у відповідних інструкцій і розпоряджень. У них в першу чергу на ГПУ "Полтавагазвидобування" 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 на ГПУ "Полтавагазвидобування" визначені права і обов'язки Служби, а також правила її взаємодії з іншими підрозділами з питань захисту інформації на об'єкті.

Організаційно-правовий статус СІБ на ГПУ "Полтавагазвидобування" визначається таким чином:

- чисельність служби повинна бути достатньою для виконання всіх перерахованих вище функцій;

- штатний склад служби не повинен мати інших обов'язків, пов'язаних з функціонуванням АС;

- співробітники служби повинні мати право доступу до всіх приміщень, де встановлена апаратура АС і право припиняти автоматизовану обробку інформації при наявності безпосередньої загрози для захищається інформації;

- керівнику служби має бути надано право забороняти включення в число діючих нові елементи АС, якщо вони не відповідають вимогам захисту інформації;

- службі інформаційної безпеки повинні бути забезпечені всі умови, необхідні для виконання своїх функцій.

Існують різні варіанти детально розробленого штатного розкладу груп, що включають перелік функціональних обов'язків, необхідних знань і навичок, розподіл часу і зусиль. При організації захисту існування детально розроблених обов'язків співробітників СІБ абсолютно необхідні.

Ключовий (а іноді і єдиною) фігурою в службі інформаційної безпеки є адміністратор безпеки (АБ).

Адміністратор безпеки - особа у своєму роді виняткове. Він повинен бути представницьким, комунікабельним, мати можливість по взаємодії з будь-якими підрозділами і посадовими особами організації для більш ефективного виконання своїх обов'язків.

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

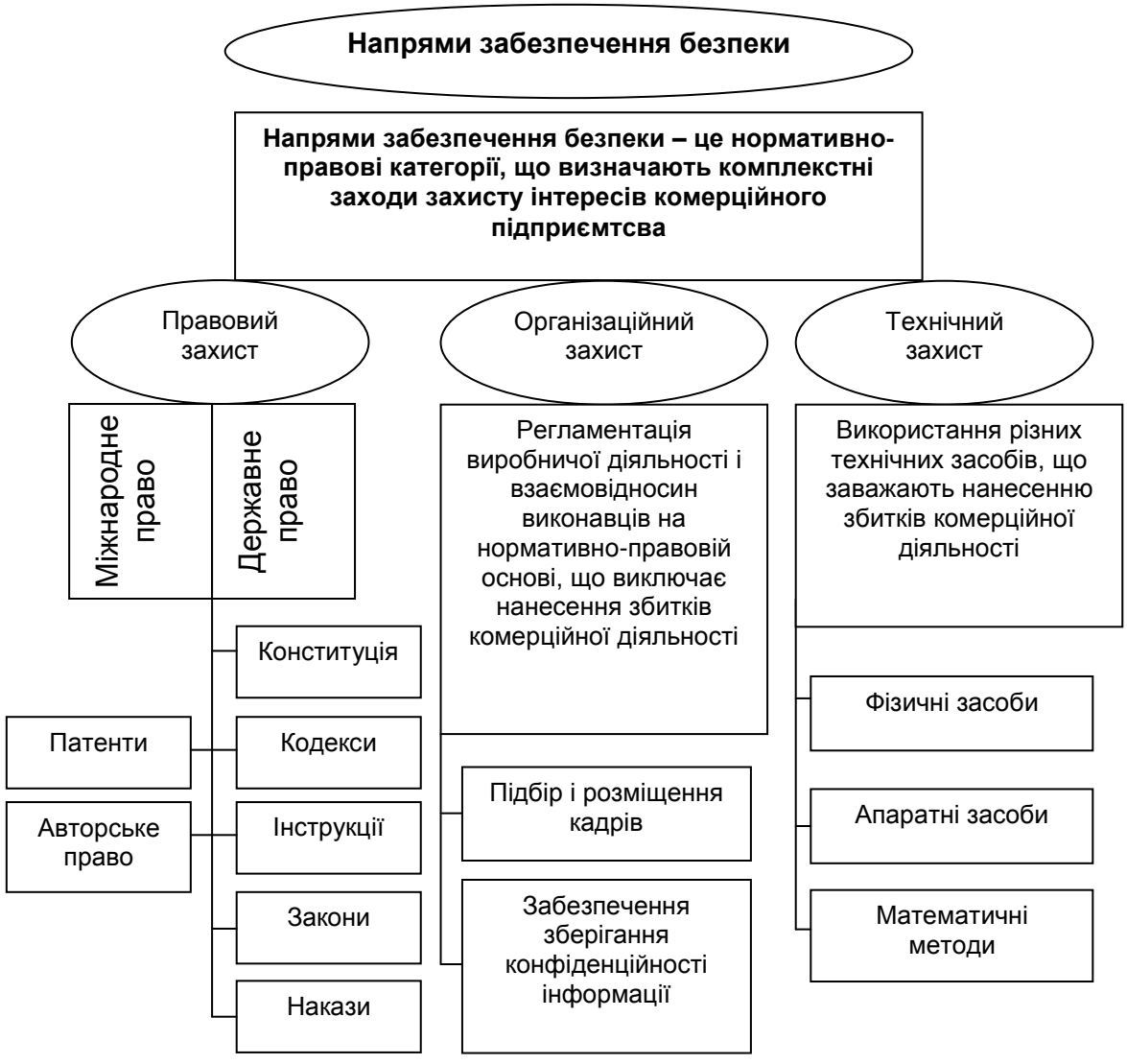

Рисунок 2.9 - Основні принципи та методи забезпечення інформаційної безпеки ГПУ "Полтавагазвидобування"

Служба безпеки ГПУ "Полтавагазвидобування" - це самостійний структурний підрозділ. Вона вирішує завдання безпосереднього забезпечення захисту життєво важливих інтересів підприємства в умовах комерційного і підприємницького ризику, конкурентної боротьби. На всіх великих і середніх підприємствах (в організаціях) звичайно створюються автономні служби безпеки, а безпеку функціонування невеликих фірм можуть гарантувати територіальні (районні або міські) служби за договорами найму одного чи кількох охоронців. Такі служби охорони зазвичай створюються при місцевих органах внутрішніх справ або при державній службі безпеки.

ГПУ "Полтавагазвидобування" як система має певні структурні ланки:

- дирекцію - керівництво підприємства;
- бухгалтерію;
- відділи - функціональні ланки підприємства;
- допоміжні служби;
- службу безпеки (СБ).

Система діяльності ГПУ "Полтавагазвидобування" організаційно складається з таких частин, як:

- організаційно-управлінська діяльність;
- фінансова;
- комерційна або інша основна діяльність підприємства;
- кадрова;
- із гарантування власної безпеки.

Кожна структурна ланка на ГПУ "Полтавагазвидобування" 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.

Служба безпеки як відділ ГПУ "Полтавагазвидобування" вирішує завдання:

- організації захисту економічних інтересів на підприємстві;

- гарантування безпеки спеціальними засобами і методами. Виконуючи організаційну функцію, служба безпеки працює у взаємодії з дирекцією і відділами (функціональними ланками) підприємства.

Служба безпеки ГПУ "Полтавагазвидобування" спільно з дирекцією забезпечує:

- ухвалення правильних управлінських рішень (забезпечує керівництво інформацією, веде аналітичну роботу);

- управління системою безпеки (консультує керівництво з питань захисту економічних інтересів);

- створення режиму збереження комерційної таємниці (розробляє правила, що забезпечують його дотримання);

- надання допомоги і здійснення контролю за діяльністю всіх функціональних ланок підприємства [34].

Служба безпеки ГПУ "Полтавагазвидобування" спільно з відділами забезпечує:

- здійснення комерційних операцій (бере участь у підготовці контрактів, перевіряє надійність партнерів, відстежує виконання взятих ними зобов'язань);

- підбір, перевірку і підготовку персоналу;

- навчання персоналу прийомів поведінки і правил спілкування, формування загальної і особистої зацікавленості, створення на підприємстві обстановки пильності.

Служба безпеки ГПУ "Полтавагазвидобування" самостійно працює спеціальними засобами і методами:

- у середовищі працівників підприємства;

- у середовищі партнерів і конкурентів підприємства.

Отже, в діяльності ГПУ "Полтавагазвидобування" гарантування безпеки - цілісне явище, що має свою чітку структуру й систему. Перед нею стоїть конкретна мета, якої досягають вирішенням управлінських і специфічних завдань.

Діяльність із гарантування безпеки на ГПУ "Полтавагазвидобування" спрямована на конкретні об'єкти і здійснюється особливими засобами і методами. Вона тісно пов'язана з діяльністю всіх функціональних ланок підприємства і має здійснюватися комплексно. Будучи підсистемою організації, ця діяльність має здійснюватися з позицій сучасного менеджменту - науки, практики і мистецтва управління виробництвом, послугами, збутом, персоналом відповідно до умов ринкової економіки, демократичних і економічних свобод.

ГПУ "Полтавагазвидобування" як самокерована система, з одного боку, є елементом загального ринкового організму, з другого - самостійною спільністю із специфічним внутрішнім середовищем, здатним в умовах конкуренції до ефективної діяльності і розвитку. Тому системний підхід тут особливо важливий. Саме система здатна швидко реагувати на зміни, їх відпрацювання, аналіз, вибір альтернативних рішень щодо виниклих нестандартних ситуативних проблем або завдань.

Основною метою підсистеми безпеки ГПУ "Полтавагазвидобування" є запобігання: збитку в її діяльності за рахунок розголошення, просочування інформації та несанкціонованого доступу до джерел конфіденційної інформації; розкраданню фінансових і матеріально-технічних коштів, знищенню майна і цінностей; порушенню роботи технічних засобів забезпечення виробничої діяльності, зокрема засобів інформатизації, а також запобігання збитку персоналу організації. Завданнями підсистеми безпеки підприємства є:

- своєчасне виявлення й усунення загроз персоналу і ресурсам; причин і умов виникнення фінансового, матеріального і морального збитку інтересам підприємства, порушення її нормального функціонування і розвитку;

- віднесення інформації до категорії обмеженого доступу (службової і

комерційної таємниць, іншої конфіденційної інформації, належного захисту від неправомірного використання), а інших ресурсів - до різних рівнів уразливості (небезпеки) і до категорії тих, що підлягають збереженню;

- створення механізму і умов оперативного реагування на загрози безпеки і прояви негативних тенденцій у функціонуванні підприємства;

- ефективне припинення посягань на ресурси і загроз персоналу на основі комплексного підходу до безпеки;

- створення умов для максимально можливого відшкодування й локалізації збитку, завданого неправомірними діями фізичних і юридичних осіб, для ослаблення негативного впливу наслідків порушення безпеки на досягнення стратегічної мети [56].

У своїй діяльності служба безпеки на ГПУ "Полтавагазвидобування" керується:

- інструкцією з організації режиму і охорони;

- інструкцією щодо захисту комерційної таємниці;

- переліком відомостей, що становлять комерційну таємницю;

- інструкцією щодо роботи з конфіденційною інформацією для керівників, фахівців і технічного персоналу;

- інструкцією щодо організації зберігання справ, що містять конфіденційну інформацію, в архіві;

- інструкцією щодо інженерно-технічного захисту інформації;

- інструкцією про порядок роботи з іноземними представниками і представництвами та ін.

Служба безпеки ГПУ "Полтавагазвидобування" постійно виконує певний комплекс завдань. Головними з них для є такі:

- гарантування безпеки виробничо-господарської діяльності та захисту відомостей, що вважаються комерційною таємницею підприємства (підприємства, організації);

- організація роботи з правового та інженерно-технічного захисту комерційної таємниці підприємства;

- запобігання необґрунтованому допуску й доступу до відомостей та робіт, які становлять комерційну таємницю;

- організація спеціального діловодства, яке унеможливлює несанкціоноване одержання відомостей, віднесених до комерційної таємниці відповідної підприємства;

- виявлення і локалізація можливих каналів витоку конфіденційної інформації в процесі звичайної діяльності та в екстремальних ситуаціях;

- забезпечення режиму безпеки за здійснення всіх видів діяльності, зокрема зустрічі, переговори й наради у рамках ділової співпраці підприємства з іншими партнерами;

- забезпечення охорони приміщень, устаткування, офісів, продукції і технічних засобів, необхідних для виробничої або іншої діяльності;

- забезпечення особистої безпеки керівництва та провідних менеджерів і спеціалістів підприємства;

- оцінка маркетингових ситуацій та неправомірних дій конкурентів і зловмисників.

Зрозуміло, що перелік конкретних завдань щодо гарантування безпеки ГПУ "Полтавагазвидобування" залежно від специфіки її діяльності може бути більшим або меншим, але завжди достатнім та обґрунтованим.

Сукупність конкретних завдань, що стоять перед службою безпеки ГПУ "Полтавагазвидобування", зумовлює певний набір виконуваних нею функцій.

Система захисту інформації (СЗІ) на ГПУ "Полтавагазвидобування" представляє собою комплекс організаційних, технічних і технологічних засобів, методів і мір, які перешкоджають несанкціонованому (незаконному) доступу до інформації.

Система захисту інформації на ГПУ "Полтавагазвидобування" повинна бути багаторівневою з ієрархічним доступом до інформації, гранично конкретизованою і прив'язаною до специфіки підприємства по структурі методів та засобів захисту, що використовуються, відкритою для регулярного оновлення, надійної як в звичайних, так і в екстремальних ситуаціях. Вона не

повинна створювати співробітникам підприємства серйозні незручності в роботі. Комплексність системи захисту досягається її формуванням з різних елементів - правових, організаційних, технічних та програмно-математичних.

Співвідношення елементів та їх зміст забезпечують індивідуальність системи захисту інформації ГПУ "Полтавагазвидобування" і гарантують її неповторність та трудність подолання. Конкретну систему захисту можна уявити у вигляді цегляної стіни, як складається з безлічі різноманітних елементів (цегли). Співвідношення елементів системи, їх склад та взаємозв'язок відображають, визначають не тільки її індивідуальність, але й конкретний заданий рівень захисту з врахуванням цінності інформації та вартості подібної системи [34].

Елемент правового захисту інформації на ГПУ "Полтавагазвидобування" 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.

Елемент організаційного захисту інформації на ГПУ "Полтавагазвидобування" містить міри управлінського та обмежувального характеру, які спонукають персонал дотримуватися правил захисту конфіденційної інформації івключає 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 безпаперового 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 [64].

Елемент організаційного захисту на ГПУ "Полтавагазвидобування" є стержнем, який зв'язує в одну систему всі інші елементи. Центральною проблемою при розробці методів організаційного захисту інформації є формування дозвільної (обмежувальної) систем і доступу персоналу до конфіденційних відомостей, документів і баз даних.

Важливо чітко і однозначно встановити: хто, кого, до яких, відомостей, коли, на який період і як допускає. Дозвільна система доступу вирішує наступні задачі: забезпечення співробітників всіма необхідними для роботи документами і інформацією; обмеження кола осіб, які допускаються до конфіденційних документів; виключення несанкціонованого ознайомлення з документу Ієрархічна послідовність доступу реалізується по принципу "чим вища цінність конфіденційних відомостей, тим менша чисельність співробітників можуть їх знати". У відповідності з цією послідовністю визначається необхідний ступінь посилення захисних мір, структура рубежів (ешелонів) захисту інформації. Доступ співробітника до конфіденційних відомостей, який здійснюється у відповідності з дозвільною системою, називається санкціонованим [33].

Дозвіл (санкція) на доступ до цих відомостей на ГПУ "Полтавагазвидобування" завжди є строго персоніфікованим і видається керівником в письмовому вигляді: наказом, що затверджує схему посадового чи іменного доступу до інформації, резолюцією на документі, списком-дозволом в карточці видачі справи або на обложці справи ознайомлення з документом. Організаційні міри захисту відображаються в нормативно-методичних документах служби безпеки підприємства. У зв'язку з цим часто використовується єдина назва двох розглянутих вище елементів системи захисту - елемент організаційно-правового захисту інформації.

Елемент технічного захисту на ГПУ "Полтавагазвидобування" включає: засоби захисту технічних каналів витоку інформації, що виникають під час роботи ЕОМ, 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 і т.д.).

Елемент програмно-математичного захисту інформації на ГПУ "Полтавагазвидобування" 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 ЕОМ та мережах, криптографування (шифрування) тексту під час передачі їх по каналам звичайного та факсимільного зв'язку, під час пересилки поштою. В кожному елементі захисту можуть бути реалізовані на практиці тільки окремі складові частини.

Наприклад, в організаційному захисті можна регламентувати тільки прийоми обробки конфіденційних документів і систему доступу до них персоналу. Методи і засоби захисту інформації в рамках системи захисту на ГПУ "Полтавагазвидобування" регулярно змінюються з метою попередження їх розкриття зловмисником. Конкретна система захисту інформації ГПУ "Полтавагазвидобування" є строго конфіденційною.

Спеціалісти, які розробляли цю систему, ніколи не повинні бути її користувачами. Отже, система захисту конфіденційної інформації, яка використовується фірмою, є індивідуалізованою сукупністю необхідних елементів захисту, кожний з яких окремо вирішує свої специфічні для даної підприємства задачі і володіє конкретизованим відносно цих задач змістом. В комплексі ці елементи формують багатограничний захист секретів підприємства і дають відносну гарантію безпеки підприємницької діяльності підприємства.

Сутність загроз інформаційної безпеки на ГПУ "Полтавагазвидобування" зводиться, як правило, до нанесення того чи іншого збитку підприємству (організації).

Прояви можливого збитку ГПУ "Полтавагазвидобування" можуть бути найрізноманітнішими:

- моральна і матеріальна шкода діловій репутації організації;
- моральний, фізичний чи матеріальний збиток, пов'язаний з

розголошенням персональних даних окремих осіб;

- матеріальний (фінансовий) збиток від розголошення конфіденційної інформації;

- матеріал (фінансовий) збиток від необхідності відновлення порушених інформаційних ресурсів, які захищаються;

- матеріальні збитки (втрати) від неможливості виконання взятих на себе зобов'язань перед третьою стороною;

- моральний і матеріальний збиток від дезорганізації в роботі всього підприємства.

Джерела зовнішніх загроз ГПУ "Полтавагазвидобування" 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. 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 інформації ГПУ "Полтавагазвидобування", 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, 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 компанії.

- "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 і т.д.

Таким чином, у сучасних умовах наявність розвиненої системи інформаційної безпеки ГПУ "Полтавагазвидобування" стає однією з найважливіших умов конкурентоспроможності і навіть життєздатності будь-якої компанії.

На сьогоднішній день існує великий арсенал методів забезпечення інформаційної безпеки ГПУ "Полтавагазвидобування":

- засоби ідентифікації і аутентифікації користувачів (так званий комплекс ЗА);

- 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 [67].

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.

"Комплекс ЗА" на ГПУ "Полтавагазвидобування" включає аутентифікацію (або ідентифікацію), авторизацію і адміністрування. Ідентифікація та авторизація - це ключові елементи інформаційної безпеки. При спробі доступу до інформаційних активів функція ідентифікації дає відповідь на питання: чи ви є авторизованим користувачем мережі. Функція авторизації відповідає за те, до яких ресурсів конкретний користувач має доступ. Функція адміністрування полягає у наділенні користувача певними ідентифікаційними особливостями в рамках даної мережі і визначенні обсягу допустимих для нього дій.

Системи шифрування на ГПУ "Полтавагазвидобування" дозволяють мінімізувати втрати у випадку несанкціонованого доступу до даних, що зберігаються на жорсткому диску або іншому носії, а також перехоплення інформації при її пересилання по електронній пошті або передачу з мережних

протоколах. Завдання даного засобу захисту - забезпечення конфіденційності. Основні вимоги, що пред'являються до систем шифрування - високий рівень криптостійкості та легальність використання на території держави.

Міжмережевий екран являє собою систему або комбінацію систем, що утворить між двома чи більш мережами захисний бар'єр, що оберігає від несанкціонованого потрапляння в мережу або виходу з неї пакетів даних.

Основний принцип дії міжмережевих екранів на ГПУ "Полтавагазвидобування" - перевірка кожного пакету даних на відповідність вхідної та вихідної IP адреси базі дозволених адрес. Таким чином, міжмережеві екрани значно розширюють можливості сегментації інформаційних мереж та контролю за циркулюванням даних.

Говорячи про криптографію і міжмережеві екрані, слід згадати про захищені віртуальні приватні мережі (Virtual Private Network - VPN). Їх використання дозволяє вирішити проблеми конфіденційності і цілісності даних при їх передачі по відкритим комунікаційних каналам. Використання VPN можна звести до вирішення трьох основних завдань:

- захист інформаційних потоків між різними офісами компанії (шифрування інформації проводиться тільки на виході у зовнішню мережу);

- захищений доступ віддалених користувачів мережі до інформаційних ресурсів компанії, як правило, здійснюваний через Internet;

- захист інформаційних потоків між окремими додатками всередині корпоративних мереж (цей аспект також дуже важливий, оскільки більшість атак здійснюється з внутрішніх мереж).

Ефективний засіб захисту від втрати конфіденційної інформації на ГПУ "Полтавагазвидобування" - 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 на ГПУ "Полтавагазвидобування" 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 ГПУ "Полтавагазвидобування" можуть бути відслідковані адміністратором мережі або іншим авторизованим користувачем завдяки технології перевірки цілісності вмісту жорсткого диска (integrity checking). Це дозволяє виявляти будь-які дії з файлами (зміна, видалення або ж просто відкриття) і ідентифікувати активність вірусів, несанкціонований доступ або крадіжку даних авторизованими користувачами. Контроль здійснюється на основі аналізу контрольних сум файлів (CRC сум) [56].

Сучасні антивірусні технології, які використовує ГПУ "Полтавагазвидобування" 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. Виявлені об'єкти можуть піддаватися лікуванню, ізолюватися (міститися в карантин) або видалятися. Захист від вірусів може бути встановлено на робочі станції, файлові і поштові сервера, міжмережеві екрани, що працюють під практично будь-якою з поширених операційних систем (Windows, Unix-і Linux-системи, Novell) на процесорах різних типів.

Для протидії природним загрозам інформаційної безпеки на ГПУ "Полтавагазвидобування" 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 і т.д.

Основними принципами інформаційної безпеки на ГПУ "Полтавагазвидобування" 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.

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.

Отже, етапи проведення робіт із забезпечення інформаційної безпеки на ГПУ "Полтавагазвидобування" 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.

Метою комплексної інформаційної безпеки на ГПУ

"Полтавагазвидобування" є збереження інформаційної системи підприємства, захист і гарантування повноти і точності виданої нею інформації, мінімізація руйнувань і модифікація інформації, якщо такі трапляються.

Інформаційні технології все більш наполегливо проникають в усі сфери людської діяльності, вірніше, людство все більш сміливо інтегрується з інформаційними технологіями. Тому, особливо актуальною є проблема забезпечення інформаційної безпеки (ІБ).

Проте сама по собі інформаційна безпека є достатньо абстрактним поняттям. Має бути деякий додаток 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.

РОЗДІЛ 3
НАПРЯМКИ УДОСКОНАЛЕННЯ ОРГАНІЗАЦІЇ ТА УПРАВЛІННЯ СЛУЖБОЮ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ ГПУ "ПОЛТАВАГАЗВИДОБУВАННЯ"

3.1. Організаційне забезпечення ефективності системи захисту інформації безпеки ГПУ "Полтавагазвидобування"

Інформаційно-аналітична робота на ГПУ "Полтавагазвидобування" - це одна із основних внутрішньовиробничих функціональні складових безпеки підприємства.

Інформаційна складова полягає у здійсненні ефективного інформаційно-аналітичного забезпечення господарської діяльності підприємства.

Належні служби на ГПУ "Полтавагазвидобування" виконують певні функції, які в сукупності характеризують процес створення та захисту інформаційної складової безпеки підприємства. До таких належать:

- 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 економічної безпеки.

На ГПУ "Полтавагазвидобування" 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.

Оперативна реалізація заходів з розробки та охорони інформаційної складової економічної безпеки на ГПУ "Полтавагазвидобування" здійснюється послідовним виконанням певного комплексу робіт, ми виділяємо 5 напрямків:

- 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.

Першою і найважливішою операцією на ГПУ "Полтавагазвидобування" 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, повинна бути виключена 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.

Допускається два критерії, по яких можна судити про точність інформації, надійність джерела і самої інформації. Головним критерієм правдоподібності є пошук підтвердження за іншими джерелами, якщо можливо - за незалежним.

Інформація може бути важливою і точною і в той же час даремною, оскільки вона недостатня для розуміння і дії. Розвідка в бізнесі відноситься до даних про навколишнє середовище і конкурентів, аналізованим з метою використовувати їх в конкретній ситуації. Ні окрема особа, ні організація не можуть ефективно діяти в умовах конкуренції без глибокого розуміння цього середовища або не маючи в своєму розпорядженні новітньої інформації про те, що в ній відбувається.

Вид потрібної інформації залежить від виду компанії (підприємства, її конкурентного середовища і багатьох інших характеристик самої підприємства і її оточення. Сьогодні практично весь український бізнес в тому або іншому ступені має тіньові сторони: ухилення від податків, подвійна бухгалтерія, заниження і подальша підміна інвойсів, захована дійсного об'єму постачань, безготівкові операції через підприємства-однодніввки і ін. У такій ситуації фірма може стати заручником кримінальної структури, яка бере фірму під свій контроль (так званий "дах") і може використовувати її для відмивання власних нелегально отриманих коштів. Крім того, як "дах" можуть виступати і різні силові структури. Отже, необхідно постійно володіти інформацією про співвідношення сил і розділення сфер впливу в місті або регіоні, в яких знаходиться фірма, в ніші ринку, яку займає фірма.

Потреба в інформації варіюється залежно від здійснюваної або планованої діяльності. ГПУ "Полтавагазвидобування" 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.

До завдань служби безпеки ГПУ "Полтавагазвидобування" 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;

- 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.

Додатково до обов'язків співробітників СІБ на ГПУ "Полтавагазвидобування" 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 [54].

На ГПУ "Полтавагазвидобування" буде доцільним наступний штатний розклад такої служби:

- заступник директора з безпеки і захисту інформації;

- адміністратор безпеки АС – штатний співробітник відділу захисту інформації;

- адміністратор системи - штатний співробітник відділу автоматизації;

- адміністратори груп – штатні співробітники підрозділів, що експлуатують АС;

- менеджери безпеки;

- оператори

Організаційно групи СІБ на ГПУ "Полтавагазвидобування" повинні бути 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 на ГПУ "Полтавагазвидобування" необхідна відповідна адміністративна підтримка, яка полягає у відображенні основних положень прийнятої політики безпеки у відповідних інструкцій і розпоряджень. У них в першу чергу повинні бути 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 на ГПУ "Полтавагазвидобування" необхідно визначити права і обов'язки Служби, а також правила її взаємодії з іншими підрозділами з питань захисту інформації на об'єкті.

Організаційно-правовий статус СІБ на ГПУ "Полтавагазвидобування" визначається таким чином:

- чисельність служби повинна бути достатньою для виконання всіх перерахованих вище функцій;

- служба повинна підкорятися тій особі, яка в даній установі несе персональну відповідальність за дотримання правил поводження з захищається інформацією;

- штатний склад служби не повинен мати інших обов'язків, пов'язаних з функціонуванням АС;

- співробітники служби повинні мати право доступу до всіх приміщень, де встановлена апаратура АС і право припиняти автоматизовану обробку інформації при наявності безпосередньої загрози для захищається інформації;

- керівнику служби має бути надано право забороняти включення в число діючих нові елементи АС, якщо вони не відповідають вимогам захисту

інформації;

- службі інформаційної безпеки повинні бути забезпечені всі умови, необхідні для виконання своїх функцій.

Існують різні варіанти детально розробленого штатного розкладу груп, що включають перелік функціональних обов'язків, необхідних знань і навичок, розподіл часу і зусиль. При організації захисту існування детально розроблених обов'язків співробітників СІБ абсолютно необхідні.

Адміністратор безпеки - особа у своєму роді виняткове. Він повинен бути представницьким, комунікабельним, мати можливість по взаємодії з будь–якими підрозділами і посадовими особами організації для більш ефективного виконання своїх обов'язків.

Завдання гарантування інформаційної безпеки ГПУ "Полтавагазвидобування" є одним із основних, пріоритетних завдань, що стоять перед усіма структурними ланками і всіма працівниками підприємства, так само як і завдання збільшення прибутку, підвищення власного добробуту. Ефективний захист економічних інтересів підприємства може бути забезпечений лише у разі об'єднання зусиль її персоналу: адміністрації, інженерно-технічних працівників, службовців, робітників.

Кожна структурна ланка 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 [67].

Служба безпеки як відділ на ГПУ "Полтавагазвидобування" вирішує завдання:

- організації захисту економічних інтересів на підприємстві;

- гарантування безпеки спеціальними засобами і методами. Виконуючи організаційну функцію, служба безпеки працює у взаємодії з дирекцією і відділами (функціональними ланками) підприємства.

Служба безпеки на ГПУ "Полтавагазвидобування" спільно з дирекцією

забезпечує:

- ухвалення правильних управлінських рішень (забезпечує керівництво інформацією, веде аналітичну роботу);

- управління системою безпеки (консультує керівництво з питань захисту економічних інтересів);

- створення режиму збереження комерційної таємниці (розробляє правила, що забезпечують його дотримання);

- надання допомоги і здійснення контролю за діяльністю всіх функціональних ланок підприємства.

Служба безпеки спільно з відділами на ГПУ "Полтавагазвидобування" забезпечує:

- здійснення комерційних операцій (бере участь у підготовці контрактів, перевіряє надійність партнерів, відстежує виконання взятих ними зобов'язань);

- підбір, перевірку і підготовку персоналу;

- навчання персоналу прийомів поведінки і правил спілкування, формування загальної і особистої зацікавленості, створення на підприємстві обстановки пильності.

Служба безпеки на ГПУ "Полтавагазвидобування" самостійно працює спеціальними засобами і методами:

- у середовищі працівників підприємства;

- у середовищі партнерів і конкурентів підприємства.

Отже, в підприємницькій діяльності гарантування безпеки - цілісне явище, що має свою чітку структуру й систему. Перед нею стоїть конкретна мета, якої досягають вирішенням управлінських і специфічних завдань.

Діяльність із гарантування безпеки на ГПУ "Полтавагазвидобування" спрямована на конкретні об'єкти і здійснюється особливими засобами і методами. Вона тісно пов'язана з діяльністю всіх функціональних ланок підприємства і має здійснюватися комплексно. Будучи підсистемою організації, ця діяльність має здійснюватися з позицій сучасного менеджменту - науки, практики і мистецтва управління виробництвом, послугами, збутом,

персоналом відповідно до умов ринкової економіки, демократичних і економічних свобод.

3.2. Удосконалення управління службою інформаційної безпеки на ГПУ "Полтавагазвидобування"

Контроль інформації забезпечує у багатьох випадках "живучість" підприємства. Достовірність даних - це, в кінцевому рахунку, доходи і втрати. Виходячи з цього, система управління вибудовує сукупність процедур контролю та перевірки точності даних.

Автоматичний контроль інформації виконується на всіх етапах її отримання та переробки. Для цієї мети використовують систему логічних умов і спеціальних обчислювальних процедур. До них на ГПУ "Полтавагазвидобування" відносяться: перевірка на логічність появи; відповідність макету структури даних; збереження обсягу відомостей та ін.

При зберіганні і переробці даних основними способами контролю ГПУ "Полтавагазвидобування" повинні служити:

- дублювання (повторення процедур запису та алгоритмів обчислень, після чого проходить зіставлення результатів);

- відстеження контрольних сум (за окремими записами та масиву даних у цілому обчислюється контрольна арифметична сума всіх реквізитів, яка перевіряється після кожного етапу перезапису);

- перевірка макета даних (за окремими реквізитами уточнюється необхідне число знаків, інтервал припустимого значення).

В умовах ринкової економіки для керівництва ГПУ "Полтавагазвидобування" та його контрагентів із прямим та непрямим фінансовим інтересом надзвичайно важливе значення має якісна, повна та достовірна інформація про результати його діяльності. Одним із методів отримання такої інформації є проведення незалежних документальних перевірок - аудиту. За результатами аудиторської перевірки формується

обґрунтована, неупереджена, документально підтверджена думка кваліфікованого фахівця, яка на заключному етапі перевірки узагальнюється в аудиторському висновку. Такий контроль вірогідності інформації, відображеної в бухгалтерській і податковій звітності, є необхідним для зацікавлених користувачів з метою ухвалення ефективних управлінських рішень. Розвиток автоматизованих інформаційних систем сприяє проведенню аудиторського контролю за допомогою комп'ютерної техніки.

Поширення автоматизованих інформаційних технологій на облікові процеси та зміна об'єкту перевірки визначили появу "комп'ютерного аудиту". Сутністю цього терміну є проведення аудиту за умови застосування досліджуваним підприємством комп'ютерів будь-якого розміру та типу для обробки фінансової інформації, суттєвої для аудиторської перевірки, незалежно від того, використовується цей комп'ютер самим підприємством чи третьою особою.

На сьогодні комп'ютерні технології використовуються на всіх стадіях аудиторського процесу. При цьому мета і завдання аудиторської перевірки залишаються незмінними. Застосування ГПУ "Полтавагазвидобування" комп'ютерних інформаційних мереж та різних видів обчислювальної техніки у процесі збору й узагальнення інформації вимагає зміни підходу до системи контролю за результатами їх діяльності.

Застосування ГПУ "Полтавагазвидобування" інформаційних технологій у бізнесі змінили середовище, в якому проводиться перевірка. Переважно підприємства передбачають у обліковій політиці ведення бухгалтерського обліку за комп'ютерною формою. За таких умов методичні прийоми аудиторських перевірок зазнають змін. Комп'ютерні інформаційні технології стають інструментом аудитора і одночасно об'єктом його дослідження.

Комп'ютерний аудит - це застосування інформаційних технологій як методу і інструменту аудитора в процесі перевірки та проведення ревізії інформації, сформованої в середовищі комп'ютерної інформаційної системи клієнта, на базі оцінки ризиків притаманних такому середовищу.

Використання ГПУ "Полтавагазвидобування" автоматизованих облікових систем викликає необхідність контролю заефективністю їх функціонування в умовах конкретного підприємства.Для перевірки безпечності інформаційної системи використовують комп'ютерний аудит.

Виділяють різні напрями комп'ютерного аудиту інформаційної системи ГПУ "Полтавагазвидобування". Основні напрями комп'ютерного аудиту інформаційної системи ГПУ "Полтавагазвидобування" представлено на рис. 3.1.

Аудит технічного стану інформаційної системи ГПУ "Полтавагазвидобування" як напрям комп'ютерного аудиту інформаційної системи спрямований на зменшення втрат, які відбулися внаслідок певних системних збоїв;

З метою проведення оцінки сукупної вартості володіння інформаційною системою, оцінки повернення коштів, вкладених у цю інформаційну систему та розробки оптимальної схеми вкладень, а також порівняння показників досліджуваної інформаційної системи з лідером у цій галузі проводиться аудит ефективності інформаційної системи ГПУ "Полтавагазвидобування".

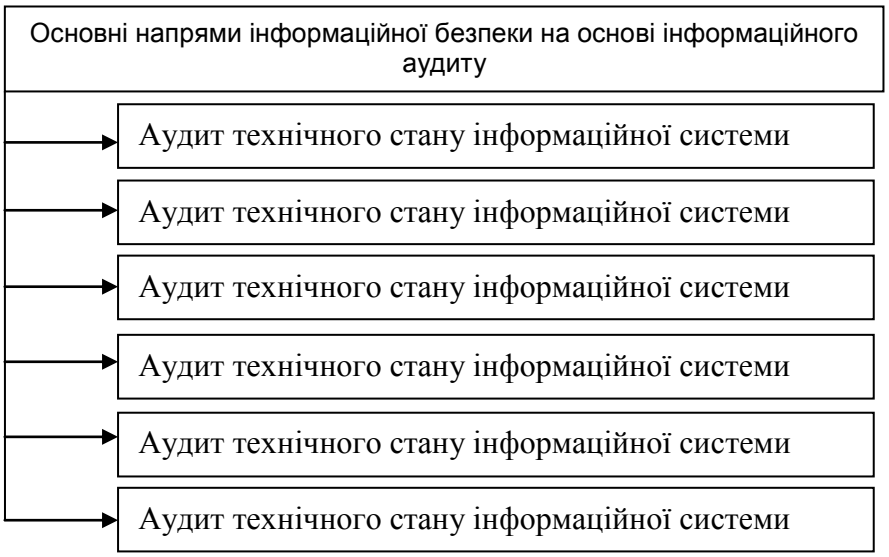

Рисунок.3.10 – Основні напрями комп'ютерного аудиту ІС [34]

Для побудови ефективної корпоративної системи захисту інформації, адекватної завданням і меті бізнесу проводиться аудит інформаційної безпеки

на ГПУ "Полтавагазвидобування".

У випадку, якщо різного роду державні органи, а також партнери ГПУ "Полтавагазвидобування" можуть зажадати сертифікації інформаційної системи підприємства з метою відповідності послуг необхідному рівню якості проводиться оціночний аудит інформаційної системи. Такий напрям комп'ютерного аудиту інформаційної системи сприяє виявленню відхилень інформаційної системи від наявних стандартів і забезпечує формуванню певних висновків та рекомендацій щодо усунення певних відхилень.

Аудит проектів впровадження та реінжинірингу на ГПУ "Полтавагазвидобування" дає змогу оцінити ризики впровадження реінжинірингу інформаційної системи, строки та плановані ресурси на розробку та впровадження рішень, правильність вибору методів технології, а також виявляє помилки та дає рекомендації щодо підвищення ефективності проекту;

Оціночний аудит програмного забезпечення ГПУ "Полтавагазвидобування" визначає економічну ефективність від впровадження і експлуатації певного виду програм або комплексу програмних ресурсів.

Надійність зберігання інформації, її захист є актуальним питанням та постійно знаходиться в полі зору. Робота із контролю за надійністю зберігання інформації ГПУ "Полтавагазвидобування" може передбачати наступні дії:

- стандартизація, сертифікація і аудиторський контроль інформаційно-телекомунікаційних систем на предмет їх безпеки;

- вивчення і запобігання інформаційно-технологічних катастроф;

- захист інформаційних систем від протиправних посягань та досягання незаконної мети;

- кадрове забезпечення інформаційної системи та ін.

Захист інформації можна забезпечити за допомогою розробки чіткого планування роботи системи внутрішнього захисту та контролю на ГПУ "Полтавагазвидобування", що передбачатиме персональну відповідальність кожного працівника, починаючи з технічного персоналу і закінчуючи

керівництвом підприємства.

Аудит безпеки - це процес збору і аналізу інформації про автоматизовані системи, необхідної для подальшого проведення якісної або кількісної оцінки рівня захисту від атак зловмисників.

Для забезпечення захисту інформації ГПУ "Полтавагазвидобування" доцільно здійснювати контроль захисту інформаційної системи. Одним із різновидів такого контролю може бути незалежний аудит. Аудит безпекиінформаційної системи дає змогу керівництву підприємства бути впевненим у тому, що їхня внутрішньогосподарська інформація буде надійно захищена від несанкціонованого використання її конкурентами та іншими зовнішніми користувачами.

Виділяють наступні види аудиту інформаційної безпеки ГПУ "Полтавагазвидобування":

- експертний аудит безпеки, в процесі якого виявляються недоліки в системі засобів захисту інформації на основі наявного досвіду експертів, що беруть участь у процедурі обстеження;

- інструментальний аналіз захищеності автоматизованої системи, спрямований на виявлення і усунення проблем програмно-апаратного забезпечення програми;

- оцінка відповідності рекомендаціям Міжнародного стандарту ISO 17799, а також керівних документів;

- комплексний аудит, що включає всі вищеперелічені форми проведення перевірки.

Отже, комп'ютерний аудит може виступати засобом оцінки інформаційної системи та захисту інформації на ГПУ "Полтавагазвидобування". Його проведення відіграє важливе значення у системі контролю інформації сформованої в середовищі комп'ютерної інформаційної системи клієнта та гарантуванні її безпеки. Здебільшого, проведення комп'ютерного аудиту інформаційних систем використовується, якщо автоматизована система призначена для обробки конфіденційної чи секретної інформації підприємства.

За умов використання підприємством автоматизованої системи збору і обробки інформації потрібно використовувати найкращі засоби захисту інформації, які може запропонувати аудиторська фірма після проведення аудиту.

Організація і методика аудиту визначається, передусім, належним інформаційним забезпеченням аудитора про суб'єкт господарської діяльності. Зростання обсягів інформації потребує від аудитора певної її систематизації і класифікації, оскільки без такого підходу важко зібрати необхідні аудиторські докази, правильно оцінити господарські явища, факти, процеси виробництва.

Аудиторський контроль на ГПУ "Полтавагазвидобування" базується не тільки на використанні інформації, а й сам бере безпосередню участь у формуванні інформаційного забезпечення системи управління суб'єктів перевірки. Інформацією аудиту цікавляться не тільки внутрішні споживачі (менеджери, акціонери), а й зовнішні (банки, страхові компанії, торговельні партнери, інвестори).

Під інформаційним забезпеченням аудиту розуміють певним чином упорядковану сукупність інформації, яку формують і використовують на різних стадіях процесу аудиту. Основою інформаційного забезпечення аудиту є економічна інформація, що характеризує виробничу і фінансово-господарську діяльність суб'єктів контролю.

Найпотрібнішу інформацію про фінансово-господарську діяльність аудитор отримує з даних бухгалтерського обліку, внутрішньогосподарського контролю, бухгалтерської і статистичної звітності. В аудиторському контролі використовують також інформація зовнішніх джерел: банків, страхових компаній, торговельних партнерів, аудиторських і юридичних фірм. Важливе місце у формуванні інформаційної бази аудиту займає законодавча, планово-нормативна та довідкова інформація. В аудиторському контролі використовують матеріали попереднього зовнішнього та внутрішнього аудиту, акти перевірки податкових органів, контрольно-ревізійних служб, позабюджетних фондів та ін.

Для об'єктивної оцінки фінансового стану підприємства, визначення

ефективності використання матеріальних, трудових і фінансових ресурсів на виробництві аудиторові часто доводиться вивчати особливості організації і технології виробництва суб'єктів перевірки, використовувати матеріали контрольних обмірів, лабораторних аналізів тощо.

Отже, для аудитора важливо не тільки мати знання про інформаційне забезпечення аудиторського контролю, а й про процес формування інформації щодо суб'єктів господарської діяльності та використання її у практичній роботі. Для цього неабияке значення має наукова класифікація економічної інформації, яку використовують в аудиті.

За основу класифікації інформаційного забезпечення фінансовогосподарського контролю й аудиту взято ознаки: професійно-інформаційна комунікація, пізнавальність інформації, зміст інформаційного забезпечення [34].

Професійна інформаційна комунікація грунтується на контактах працівників контролю на ГПУ "Полтавагазвидобування". Одночасно дає визначення інформаційно-прямої, інформаційно-непрямої і опосередкованої інформації, як вивчення, відповідно до даних про стан пізнавальних об'єктів, нормативно-правових актів та про виробничо-фінансово-господарську діяльність підприємств однієї галузі та зіставлення їх із даними підконтрольного підприємства, спеціальної літератури тощо. В даному випадку при поділі інформації на пряму, непряму і опосередковану більше підходить ознака - об'єкт контролю.

Нова інформація відображає, новизну запропонованого рішення або обгрунтовує причину недоліків виявлених у процесі аудиту, а релевантна - це та, що раніше була в аналогах, тобто в прототипі.

Основним джерело законодавчої інформації є закони і постанови, які прийняла Верховна Рада України, Укази Президента України, постанови уряду та інші законодавчі акти, що регулюють питання господарської діяльності суб'єктів аудиторського контролю. До джерел законодавчого інформаційного забезпечення відносять також законодавчі акти з цивільного, трудового й

адміністративного права.

Планову інформацію аудитор черпає з перспективних і поточних планів, які розробляють безпосередньо на ГПУ "Полтавагазвидобування". Сюди можна також віднести бюджети реалізації і витрат, прибутків та ін. Що стосується нормативно-довідкової інформації, то її варто виділити в окрему групу, а не змішувати з плановою інформацією.

Технологічна інформація на ГПУ "Полтавагазвидобування" включає відомості про технологію виробництва, технічні й технологічні умови експлуатації обладнання і технологічних ліній, технічні умови якості та ін. Основними джерелами технологічної інформації є технічна і проектно-технологічна документація, паспорти та інші документи, які використовуються на суб'єкті господарської діяльності.

Джерелами організаційно-управлінської інформації є установчі документи ГПУ "Полтавагазвидобування", накази і розпорядження керівника, посадові інструкції та ін. Організаційно-управлінська інформація залежить від типу та структури підприємства, організації і стилю управління ГПУ "Полтавагазвидобування".

Фактографічна інформація характеризує об'єкти аудиту на основі даних, що відображені у первинних документах, облікових регістрах, бухгалтерській і статистичній звітності.

Інформація оперативного обліку не завжди зафіксована в документах. Проте аудитор може сам її отримати в оперативному порядку по телефону, факсу. Найдоказовішою інформацією щодо об'єктів контролю є, звичайно, дані бухгалтерського обліку (фінансового, управлінського) і звітності.

Важливим джерелом отримання інформації щодо об'єктів аудиту є матеріали перевірки зовнішнього контролю. Такий вид контролю здебільшого здійснюють органами податкової служби, контрольно-ревізійного управління, Пенсійного фонду та ін.

3.3. Ресурсне забезпечення ефективності системи захисту інформації ГПУ "Полтавагазвидобування"

Виходячи з результатів аналізу інформаційних загроз та засобів інформаційного захисту ГПУ "Полтавагазвидобування", встановлено їх суттєву невідповідність, яка приводить до неефективності системи інформаційної безпеки ГПУ "Полтавагазвидобування". У зв'язку з цим,, виникає необхідність у визначенні заходів, які б дозволили забезпечити ефективність системи інформаційної безпеки ГПУ "Полтавагазвидобування".

У застосуванні до системи інформаційної безпеки ГПУ "Полтавагазвидобування", ефективність - це співвідношення приросту рівня інформаційної безпеки до приросту витрат ресурсів на формування та функціонування системи інформаційної безпеки.

Виходячи з наданого визначення ефективності, існує два основних напрямки її забезпечення:

- підвищення рівня інформаційної безпеки ГПУ "Полтавагазвидобування";

- скорочення витрат ресурсів на формування та функціонування системи інформаційної безпеки.

Комплексна регламентація системи інформаційної безпеки ГПУ "Полтавагазвидобування" передбачає розробку набору інструктивних документів з організації інформаційного захисту, які повинні затверджуватисянаказом керівництва ГПУ "Полтавагазвидобування" та регулювати наступні питання: визначення основних термінів з інформаційної безпеки; структура та функції підрозділу інформаційної безпеки підприємства; права та обов'язки персоналу у сфері інформаційного захисту; відповідальність за порушення правил інформаційного захисту; регламентація режиму інформаційного захисту; встановлення профілів інформаційного захисту; порядок управління доступом; порядок управління інцидентами; порядок зовнішніх інформаційних зносин.

Іншим важливим питанням організаційного характеру є визначення необхідності створення підпрозділу інформаційної безпеки підприємства (служби інформаційної безпеки) та її кадрового, матеріально-технічного та фінансового забезпечення. Відповідь на це питання потребує диференційованого підходу, оскільки ГПУ "Полтавагазвидобування" незважаючи на загальну галузеву належність має особливі риси (табл. 3.11).

Таблиця 3.11

Фактори формування служби інформаційної безпеки (СІБ)

ГПУ "Полтавагазвидобування"

Відношення інформаційних збитків до власного капіталу		
>0,6	=0,5	<0,2
Багатопрофільна внутрішня ОБ з розширеними повноваженями та залучення зовнішніх спеціалістів	Багатопрофільна внутрішня СІБ з розширеними повноваженями	Багатопрофільна внутрішня СІБ

Для запровадження системи навчання та контролю персоналу ГПУ "Полтавагазвидобування" необхідно, перш за все, визначити питання, які підлягають вивченню, орієнтуючись на вимоги наказу з інформаційної політики та статистики інцидентів. Крім того, важливими питаннями є періодичність та форми навчання, які визначають виходячи з розмірів підприємства.

При розробці програми навчання особливу увагу на ГПУ "Полтавагазвидобування" слід приділити тим питанням інформаційної безпеки, які пов'язані з виникненням на підприємстві найбільших збитків та шкоди. Також, слід врахувати перспективні напрямки розвитку підприємства та зміни зовнішнього середовища підприємства, які можуть призвести до суттєвої зміни стратегічних пріоритетів та вимог до системи інформаційної безпеки підприємства.

Обов'язковим елементом системи навчання та контролю персоналу на ГПУ "Полтавагазвидобування" є не тільки контроль знань, вмінь та навичок співробітників, але й контроль у процесі виконання службових обов'язків. Результати такого контролю необхідно використовувати для двох основних

функцій:

- виявлення порушень та винних у їх скоєнні для притягнення їх до відповідальності;

- виявлення співробітників, які сумлінно виконують правила інформаційної безпеки та їх заохочення.

Тобто, контроль персоналу повинен виконувати не лише каральну функцію, але й стимулюючу, що дозволить використовувати переваги позитивної мотивації на ГПУ "Полтавагазвидобування".

Ефективність матеріального стимулювання співробітників, які сумлінно виконують правила інформаційної безпеки на ГПУ "Полтавагазвидобування" обумовлена наступними причинами:

- більшість інцидентів інформаційної безпеки трапляється з вини людського фактору;

- майже усі інформаційні процеси на підприємстві здійснюються за участю персоналу;

- основним джерелом доходів більшості українців є зарплата, а її середній по країні розмір не відповідає вимогам нормального існування.

Методика розподілу фонду преміювання персоналу на ГПУ "Полтавагазвидобування" за сумлінне виконання правил інформаційної безпеки включає декілька етапів:

- визначення загального розміру відповідного фонду преміювання;

- вибір критеріїв преміювання з відповідного фонду;

- встановлення пріоритетності критеріїв преміювання;

- регламентація порядку оцінювання за кожним критерієм;

- відбір суб'єктів, що здійснюватимуть оцінку;6) розрахунок інтегральної оцінки кожного співробітника за обраними критеріями з врахуванням їх пріоритету;

- розподіл відповідного фонду преміювання з врахуванням інтегральної оцінки співробітників;

Другим напрямком забезпечення ефективності системи інформаційної

безпеки ГПУ "Полтавагазвидобування", як було визначено вище, є скорочення витрат ресурсів на формування та функціонування системи інформаційної безпеки. Для реалізації цього напрямку ми пропонуємо оптимізувати структуру ресурсозабезпечення системи інформаційної безпеки ГПУ "Полтавагазвидобування" з метою максимізації синергетичного ефекту у формі зниження витрат ресурсів.

Структуру ресурсозабезпечення відобразимо за допомогою ресурсної матриці ГПУ "Полтавагазвидобування" (табл. 3.12).

Таблиця 3.12

Ресурсна матриця системи інформаційної безпеки
ГПУ "Полтавагазвидобування"

Ресурсні потреби	Джерела ресурсів				
	S_1	S_2	S_3	…	Si
C_1	P_{11} R_{11}	P_{12} R_{12}	P_{13} R_{13}	…	Pij Rij
…				…	
C_i	P_{11} R_{11}	P_{12} R_{12}	P_{13} R_{13}	…	Pij Rij

Як видно з табл. 3.12, ресурсна матриця системи інформаційної безпеки ГПУ "Полтавагазвидобування" включає наступні елементи: $C = \{q\}$ - множина ресурсів; $S = \{s_j\}$ - множина джерел ресурсів; $P = \{p_{ij}\}$ - вартість ресурсів і-го виду із j-го джерела ресурсів; $R = \{r_{ij}\}$ - обсяг ресурсів і-го виду, отриманих із j-го джерела ресурсів; $TP = \sum p_{ij} r_{ij}$ - загальна вартість ресурсів.

Реалізація розглянутих пропозицій щодо організаційного та ресурсного забезпечення системи інформаційної безпеки ГПУ "Полтавагазвидобування" дозволить підвищити рівень інформаційної безпеки та знизити витрати на формування та функціонування системи інформаційної безпеки ГПУ "Полтавагазвидобування". У подальших дослідженнях проблеми забезпечення ефективності системи інформаційної безпеки ГПУ "Полтавагазвидобування" необхідно обґрунтувати визначення пріоритетів реалізації внутрішньогосподарських заходів з забезпечення ефективності відповідної системи [34].

Основною метою підсистеми безпеки ГПУ "Полтавагазвидобування" є запобігання: збитку в її діяльності за рахунок розголошення, просочування інформації та несанкціонованого доступу до джерел конфіденційної інформації; розкраданню фінансових і матеріально-технічних коштів, знищенню майна і цінностей; порушенню роботи технічних засобів забезпечення виробничої діяльності, зокрема засобів інформатизації, а також запобігання збитку персоналу організації. Завданнями підсистеми безпеки ГПУ "Полтавагазвидобування" є:

- своєчасне виявлення й усунення загроз персоналу і ресурсам; причин і умов виникнення фінансового, матеріального і морального збитку інтересам підприємства, порушення її нормального функціонування і розвитку;

- віднесення інформації до категорії обмеженого доступу (службової і комерційної таємниць, іншої конфіденційної інформації, належного захисту від неправомірного використання), а інших ресурсів - до різних рівнів уразливості (небезпеки) і до категорії тих, що підлягають збереженню;

- створення механізму і умов оперативного реагування на загрози безпеки і прояви негативних тенденцій у функціонуванні підприємства;

- ефективне припинення посягань на ресурси і загроз персоналу на основі комплексного підходу до безпеки;

- створення умов для максимально можливого відшкодування й локалізації збитку, завданого неправомірними діями фізичних і юридичних осіб, для ослаблення негативного впливу наслідків порушення безпеки на досягнення стратегічної мети.

Сукупність конкретних завдань, що стоять перед службою інформаційної безпеки ГПУ "Полтавагазвидобування", зумовлює певний набір виконуваних нею функцій.

Система захисту інформації (СЗІ) представляє собою комплекс організаційних, технічних і технологічних засобів, методів і мір, які перешкоджають несанкціонованому (незаконному) доступу до інформації.

Власник інформації особисто визначає не тільки склад цінної інформації,

яка належить захисту, але й відповідні способи та засоби захисту. Одночасно ним розробляються міри матеріального і морального стимулювання співробітників, які дотримуються порядку захисту цінної інформації, і міри відповідальності персоналу за розголошення таємниці підприємства.

Система захисту інформації ГПУ "Полтавагазвидобування" повинна бути багаторівневою з ієрархічним доступом до інформації, гранично конкретизованою і прив'язаною до специфіки підприємства по структурі методів та засобів захисту, що використовуються, відкритою для регулярного оновлення, надійної як в звичайних, так і в екстремальних ситуаціях. Вона не повинна створювати співробітникам підприємства серйозні незручності в роботі. Комплексність системи захисту досягається її формуванням з різних елементів - правових, організаційних, технічних та програмно-математичних.

Отже, система захисту конфіденційної інформації, яка використовується ГПУ "Полтавагазвидобування", є індивідуалізованою сукупністю необхідних елементів захисту, кожний з яких окремо вирішує свої специфічні для даної підприємства задачі і володіє конкретизованим відносно цих задач змістом. В комплексі ці елементи формують багатограничний захист секретів ГПУ "Полтавагазвидобування" і дають відносну гарантію безпеки підприємницької діяльності ГПУ "Полтавагазвидобування".

ВИСНОВКИ

Нині неможливо представити сучасний бізнес і процес управління підприємством без підтримки інформаційних технологій.

Забезпечення безпеки інформації і інших об’єктів, що відносяться до інформації - вкрай важливе завдання для будь–якого бізнесу.

На думку експертів в галузі захисту інформації, завдання забезпечення інформаційної безпеки повинні вирішуватися системно. Це означає, що різні засоби захисту апаратні, програмні, фізичні, організаційні і т.д.) повинні застосовуватися одночасно під централізованим управлінням. При цьому компоненти системи повинні "знати" існування один одного, взаємодіяти і забезпечувати захист як від зовнішніх, так і внутрішніх загроз.

Методи забезпечення інформаційної безпеки на ГПУ "Полтавагазвидобування":

- засоби ідентифікації і аутентифікації користувачів;

- засоби шифрування інформації, що зберігається на комп’ютерах і що передається по мережах:

- міжмережеві екрани;

- віртуальні приватні мережі;

- інструменти перевірки цілісності вмісту дисків;

- засоби антивірусного захисту;

- системи виявлення вразливостей мереж і аналізатори мережевих атак.

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

Ідентифікація та авторизація – це ключові елементи інформаційної безпеки на ГПУ "Полтавагазвидобування". При спробі доступу до інформаційних активів функція ідентифікації дає відповідь на питання: чи ви є авторизованим користувачем мережі. Функція авторизації відповідає за те, до

яких ресурсів конкретний користувач має доступ на ГПУ "Полтавагазвидобування". Функція адміністрування полягає у наділенні користувача певними ідентифікаційними особливостями в рамках даної мережі і визначенні обсягу допустимих для нього дій.

Системи шифрування на ГПУ "Полтавагазвидобування" дозволять мінімізувати втрати у випадку несанкціонованого доступу до даних, що зберігаються на жорсткому диску або іншому носії, а також перехоплення інформації при її пересилання по електронній пошті або передачу і мережних протоколах. Завдання даного засобу захисту – забезпечення конфіденційності. Основні вимоги, що пред’являються до систем шифрування – високий рівень криптостійкості та легальність використання на території держави.

РЕКОМЕНДАЦІЇ

Міжмережевий екран являє собою систему або комбінацію систем, що утворює між двома чи більш мережами захисний бар’єр, що оберігає від несанкціонованого потрапляння в мережу або виходу з неї пакетів даних. Основний принцип дії міжмережевих екранів – перевірка кожного пакету даних на відповідність вхідної та вихідної IP адреси базі дозволених адрес. Таким чином, міжмережеві екрани значно розширюють можливості сегментації інформаційних мереж та контролю за циркуляцією даних на ГПУ "Полтавагазвидобування".

Говорячи про криптографію і міжмережеві екрані, слід згадати про захищені віртуальні приватні мережі (Virtual Private Network-VPN). Їх використання дозволяє вирішити проблеми конфіденційності і цілісності даних при їх передачі по відкритим комунікаційних каналам. Використання УРК можна звести до вирішення трьох основних завдань:

- захист інформаційних потоків між різними офісами компанії (шифрування інформації проводиться тільки на виході у зовнішню мережу);

- захищений доступ віддалених користувачів мережі до інформаційних ресурсів компанії, як правило, здійснюваний через Internet;

- захист інформаційних потоків між окремими додатками всередині корпоративних мереж (цей аспект також дуже важливий, оскільки більшість атак здійснюється з внутрішніх мереж).

Ефективний засіб захисту від втрати конфіденційної інформації на ГПУ "Полтавагазвидобування" – 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.

Всі зміни на робочій станції або на сервері можуть бути відстеженні адміністратором мережі ГПУ "Полтавагазвидобування" або іншим авторизованим користувачем завдяки технології перевірки цілісності вмісту

жорсткого диска (integrity checking). Це дозволяє виявляти буд–які дії з файлами (зміна, видалення або ж просто відкриття) і ідентифікувати активність вірусів, несанкціонований доступ або крадіжку даних авторизованими користувачами. Контроль здійснюється на основі аналізу контрольних сум файлів (CRC сум).

Сучасні антивірусні технології дозволяють виявити практично всі вже відомі вірусні програми через порівняння коду підозрілого файлу із зразками, що зберігаються в антивірусної базі. Крім того, розроблені технології моделювання поведінки, що дозволяють виявляти новостворювані вірусні програми. Виявлені об’єкти можуть піддаватися лікуванню, ізолюватися (міститися в карантин) або видалятися.

Захист від вірусів на ГПУ "Полтавагазвидобування" може бути встановлено на робочі станції, файлові і поштові сервера, міжмережеві екрани, що працюють під практично будь-якою і поширених операційних систем (Windows. Unix-I Linux- системи, Novell) на процесорах різних типів. Фільтри спаму значно зменшують невиробничі затрати праці, пов’язані з розглядом спаму. знижують трафік і завантаження серверів, покращують психологічний фон в колективі і зменшують ризик залучення співробітників компанії в шахрайські операції.

Для протидії природним загрозам інформаційної безпеки на ГПУ "Полтавагазвидобування" 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 виникне. Один з основних методів захисту від втрати даних – резервне копіювання з чітким дотриманням встановлених процедур (регулярність, типи носіїв, методи зберігання копій і т.д.

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]. – Київ : 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: 25.11.17.

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: 07.12.17.

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

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

19. 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.

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

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

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

23. 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.

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

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

26. 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.

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

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

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

30. 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.

31. 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: 10.11.2019.

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

33. 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.

34. 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, профессора В. Б. Толубка. – Київ: ДУТ, 2015.– 288 с.

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

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

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

38. Для чего нужна автоматизация делопроизводства: [Електронний ресурс]. – Електронні дані. – Режим доступу: http://www.mdi.ru/library/analit/avtom.html. – Назва з екрана. – Дата звернення: 15.11.2019.

39. 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&article_id =3893. – Назва з екрана. – Дата звернення: 19.02.2019

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

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

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

43. 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: 05.04.2019.

44. 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.

45. 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.

46. 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: 20.10.2019.

47. 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: 20.10.2019.

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

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

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

51. Кримінальний Кодекс України [Електронний ресурс]. – Електронні дані. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/2341-14. – Назва з екрана. – Дата звернення: 20.10.2019.

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

53. 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.

54. Кушнаренко Н. Н. Документоведенье [Електронний ресурс]: навч. посібник / Н. Н. Кушнаренко. – Київ: Знання, 2008. – 459 с.

55. 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: 20.10.2019.

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

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

58. 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.

59. 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: 20.10.2019.

60. Мотив [Електронний ресурс]. – Електронні дані. – Режим доступу: http://www.motiw.ru/. – Назва з екрана. – Дата звернення: 20.10.2019.

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

62. 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: 10.03.2017.

63. 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.

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

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

66. Положення про наглядову раду Публічного акціонерного товариства «Полтаваобленерго» [Копія]. – Затв. Рішенням Заг. зборів акціонерів., протокол № 16 20.04.2011. – Полтава. – 12 с. – Підпис Голови загальних зборів акціонерів А.О. Загорулько. – Копію засвідчено секретарем О.О. Терещук. – Печатка Публічного акціонерного товариства «Полтаваобленерго».

67. 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.

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

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

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

71. 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.

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

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

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

75. 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.

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

77. 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: 20.10.2019.

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

79. Системы менеджмента информационной безопасности: ISO 27001/17799 [Електронний ресурс]. – Електронні дані. – Режим доступу: http://17799.standardsdirect.org/ISO 27001. – Назва з екрана. – Дата звернення: 20.10.2019.

80. 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: 20.10.2019.

81. Степанов Е. І. Информационная безопасность и защита информации / Е. І. Степанов, І. С. Корнеев. – Москва: Инфра – М.: 2011. – 333 с.

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

83. 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: 18.10.2019.

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

85. 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.