

ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ
УНІВЕРСИТЕТ

Економічний факультет

Кафедра “Економіка, менеджмент та комерційна діяльність”

Допущена до захисту:
Завідувач кафедри економіки,
менеджменту та комерційної
діяльності к.е.н., доцент
_____ Тетяна РЯБОВОЛИК
“ 03 ” січня 2024 р.
(протокол засідання кафедри ЕМКД №10
від 03 січня 2024 р.).

Кваліфікаційна робота

за другим (магістерським) рівнем вищої освіти:

на тему: “Управління системою забезпечення інформаційної
безпеки підприємства”

Виконав: здобувач вищої освіти II курсу
магістратури, групи. УФЕБ - 22 М
спеціальності 073 “Менеджмен”
ОПП “Управління фінансово-економічною
безпекою”
Турта Ростислав Анатолійович _____
Керівник: к.юр.н., доцент кафедри ЕМКД
Фомічов Костянтин Сергійович _____
Рецензент: к.е.н., доцент
Коцюрба Ольга Юріївна _____

ЗМІСТ

ВСТУП	4
РОЗДІЛ 1. ТЕОРЕТИЧНІ ТА МЕТОДИЧНІ ОСНОВИ УПРАВЛІННЯ СИСТЕМОЮ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА	7
1.1. Сутність та зміст поняття інформаційної безпека як складової економічної безпеки підприємства	7
1.2. Цінність, класифікація та оцінка інформації як об'єкту інформаційної безпеки	14
1.3 Проблеми інформаційного захисту в контексті автоматизації та інформатизації сучасних підприємств	21
РОЗДІЛ 2. ДОСЛІДЖЕННЯ СТАНУ УПРАВЛІННЯ СИСТЕМОЮ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПРАТ “КІРОВОГРАДОБЛЕНЕРГО”	37
2.1. Оцінка виробничо - господарської діяльності ПрАТ “Кіровоградобленерго”	37
2.2. Аналіз фінансово-економічної діяльності підприємства	48
2.3. Характеристика інформаційних ресурсів та системи інформаційного забезпечення процесу управління на ПрАТ “Кіровоградобленерго”	57
2.4. Оцінка системи забезпечення інформаційної безпеки підприємства ПрАТ “Кіровоградобленерго”	67
РОЗДІЛ 3. НАПРЯМИ ВДОСКОНАЛЕННЯ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА	76
3.1. Формування сучасної системи інформаційної безпеки підприємства	76
3.2. Механізм збереження комерційної таємниці на підприємстві	81
3.3. Впровадження додаткових показників оцінки ефективності управління забезпеченням інформаційної безпеки	88
ВИСНОВКИ	94
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	100
ДОДАТКИ	104

ВСТУП

Глобальний розвиток інформатизації суспільства в останні роки породив нову глобальну проблему - інформаційну безпеку. Багато з найважливіших інтересів компанії сьогодні значною мірою залежать від стану інформаційного середовища, що її оточує. Навмисний або ненавмисний вплив на інформаційну сферу з боку зовнішніх або внутрішніх джерел може завдати серйозної шкоди цим інтересам і створити загрози та ризики для безпеки. Тому інформаційна безпека в сучасних умовах є однією з обов'язкових умов нормального функціонування підприємства.

Стає все більш очевидним, що загальний рівень економічної безпеки підприємства залежить від інформаційної складової. Як свідчить практика, будь-яка ворожа дія проти інтересів юридичної особи починається зі збору інформації. Навіть дрібні крадіжки часто починаються з пошуку можливої протиправної діяльності осіб зі злочинними намірами, а без належного розвідувального супроводу неможливо уявити такі деструктивні показники, як виведення корпоративних активів або захоплення рейдерами.

Не випадково питання інформаційної безпеки вже давно стали одними з найпріоритетніших практично для всіх великих компаній. Сьогодні багато керівників малих і середніх компаній в країні починають усвідомлювати реальну небезпеку ризиків, пов'язаних з інсайдерською інформацією, системами транзакцій і пов'язаними з ними співробітниками.

Фахівці розуміють термін "інформаційна безпека" по-різному і в більшості випадків мають на увазі один з аспектів проблеми. Наприклад, з точки зору керівництва, серйозною загрозою є крадіжка конфіденційних документів, з точки зору розробників антивірусного програмного забезпечення - ризик знищення цінних даних. Кожен з цих аспектів заслуговує на окреме дослідження, але для споживачів важливо забезпечити загальну безпеку, а не тільки з точки зору окремих ризиків.

На наш погляд, інформаційна безпека для компаній складається з

конкретних дій, спрямованих на виявлення, усунення та нейтралізацію джерел, причин та умов, несприятливих для інформації.

Рівень інформаційної складової економічної безпеки визначається використанням неповної, неточної або суперечливої інформації в процесі прийняття управлінських рішень.

Метою даної магістерської роботи є розробка основних заходів щодо забезпечення інформаційної безпеки на підприємствах, запобігання загрозі втрати або знищення інформації.

Завданням магістерської роботи є:

- визначення складових системи управління інформаційною безпекою на підприємстві ПрАТ "Кіровоградобленерго";
- визначити рівень економічної безпеки підприємства та важливість інформаційної безпеки на підприємстві;
- оцінити ефективність збору різних видів інформації, необхідної на підприємстві;
- визначити рівень економічної безпеки підприємства та важливість інформаційної безпеки на підприємстві;
- визначити, як обробляється та організовується інформація;
- оцінити ефективність аналізу цієї інформації;
- визначити стан захищеності інформаційного середовища на підприємстві;
- визначити стан захищеності інформаційного середовища на підприємствах;
- розробити оперативні інструменти забезпечення захисту інформаційних елементів економічної безпеки.

Об'єктом дослідження є господарська діяльність ПрАТ "Кіровоградобленерго", зокрема організаційна структура управління, показники господарської діяльності та організація процесів забезпечення економічної та інформаційної безпеки на підприємстві. Предметом дослідження є організаційний стан забезпечення інформаційної безпеки на

підприємстві.

Магістерська робота складається зі вступу, трьох розділів та висновків, які розкривають теоретичні та практичні аспекти управління системами інформаційної безпеки на підприємстві ПрАТ "Кіровоградобленерго".

Методологічною основою дослідження є метод наукового пізнання, системний підхід та методи фінансового аналізу. У дослідженні використано ретроспективний аналіз, структурний аналіз, порівняльний аналіз та аналіз коефіцієнтів, метод порівняльного R-аналізу.

У якості апробації результатів дослідження нами було опубліковано тези на тему «Характеристика основних заходів щодо забезпечення збереження комерційної таємниці на підприємстві» у збірнику VI Міжнародної науково-практичної конференції «Конкурентоспроможна модель інноваційного розвитку економіки України», 7-8 грудня 2023 року.

Для вивчення цього питання необхідно розібратися в правовому регулюванні: Закон України "Про інформацію" від 2 вересня 92 року; Закон України "Про захист інформації в автоматизованих системах" від 5 липня 94 року; Закон України "Про Національну програму інформатизації" від 4 лютого 98 року; Закон України "Про Концепцію Національної програми інформатизації" від 2 вересня 99 року; Концепція технічного захисту інформації в Україні, № 1126. 1126, а також наукові праці Б. Кормича, А. Баранова, В. Роговця, О. Іванова, С. Рощина, В. Мельникова, В. Герасименка та Л. Я. Гофмана.

В якості джерел інформації для оцінки рівня забезпечення економічної та інформаційної безпеки на підприємствах були використані статут підприємства, форма 1 "Баланс", форма 2 "Звіт про фінансові результати", а також відповідні положення та інструкції підприємства.

РОЗДІЛ 1

ТЕОРЕТИЧНІ ТА МЕТОДИЧНІ ОСНОВИ УПРАВЛІННЯ СИСТЕМОЮ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

1.1. Сутність та зміст поняття інформаційної безпеки як складової економічної безпеки підприємства

Забезпечення безпеки діяльності має важливе значення для всіх підприємств та організацій, від державних установ до невеликих роздрібних магазинів. Різниця полягає лише в засобах, методах і ступені їх захисту.

Перш ніж ми почнемо аналізувати поточний стан питань інформаційної безпеки, давайте розглянемо питання безпеки в цілому. Перш за все, необхідно визначити, що саме потрібно захищати і яких основних принципів необхідно дотримуватися при організації захисту.

Відповідно до сформованої історичної та міжнародної практики забезпечення безпеки, в порядку пріоритетності слід захищати наступне:

- 1) людей;
- 2) інформацію;
- 3) матеріальні активи.

Якщо пріоритетність захисту безпеки людей є очевидною, то пріоритет інформації над матеріальними цінностями слід розглянути більш детально. Це стосується не лише інформації, що становить державну або комерційну таємницю, але й загальнодоступної інформації.

Ринкові відносини та конкуренція як їх невід'ємна частина повинні бути захищені від зовнішніх та внутрішніх впливів. Об'єкти, що захищаються, можуть піддаватися різним атакам і загрозам, більшим або меншим, залежно від цілей зловмисника і конкретних обставин, а також можуть бути поставлені в ситуацію, коли їм загрожує небезпека з об'єктивних причин.

Поняття "безпечна діяльність" будь-якого підприємства чи організації включає в себе:

- 1) фізичну безпеку, захист від загроз життю людей;
- 2) економічну безпеку;
- 3) інформаційну безпеку;
- 4) безпеку фізичних активів від усіх видів загроз, від крадіжок до пожеж та інших стихійних лих.

Не вдаючись у подробиці загроз фізичній та матеріальній безпеці, слід зазначити, що економічна безпека та інформаційна безпека тісно пов'язані між собою.

За даними західних експертів, у 60 з кожних 100 випадків витік 20 відсотків бізнес-інформації призводить до банкрутства компанії. Навіть успішна компанія не може проіснувати більше трьох днів, якщо її інформація, що становить комерційну таємницю, стає відомою. Тому економіка та інформаційна безпека тісно пов'язані між собою.

Будь-яка організація повинна знати про своїх конкурентів, щоб зменшити загрозу для своєї економічної діяльності. Тому природно, що зменшення цієї загрози однією організацією призведе до збільшення загроз для економічної діяльності інших організацій. Це стає можливим завдяки промисловому шпигунству, в тому числі економічному.

Збитки, завдані конкурентами, які використовують тактику шпигунства, становлять 30 відсотків усіх збитків у світі, що обчислюються мільярдами доларів. Як правило, визначити точну суму збитків неможливо, оскільки ні зловмисники, ні жертви не бажають надавати інформацію про свої дії. Перші можуть боятися притягнення до відповідальності, а другі - шкоди для свого іміджу. Цим пояснюється тривалий інкубаційний період правопорушень та відсутність висвітлення у ЗМІ. Як наслідок, громадськість знає про менш ніж 1 відсоток усіх випадків прихованої злочинності.

Аналізуючи структуру економіки та виробництва, можна помітити постійне зростання значення і ролі малого та середнього бізнесу в контексті процесів накопичення знань.

Організація обміну інформацією зробила нові "види бізнесу", тобто нові

форми підприємницької діяльності, більш доступними, полегшивши формування партнерських відносин, пошук торгових партнерів, купівлю та продаж продукції. Інформація загалом тісно пов'язана з бізнесом, і цей зв'язок висуває на перший план питання, які не можна ігнорувати. Однією з таких проблем є забезпечення інформаційної безпеки бізнесу. Таким чином, беручи до уваги різні аспекти людської діяльності, у всіх випадках необхідно вирішувати проблеми безпеки всіх видів. Однак, як бачимо, всі види безпеки тісно пов'язані з інформаційною безпекою і, більше того, не можуть бути забезпечені без інформаційної безпеки. Тому наступною темою, яку ми розглянемо, буде інформаційна безпека.

Тема інформаційної безпеки є відносно добре розробленою в літературі. Необхідно відмітити роботи таких авторів як О. Баранова, К. Белякова, В. Брижка, В. Гавловського, І. Гаврилова, О. Гладківської, М. Гуцалюка М. Жулинського, Л. Задорожньої, О. Зінченка, Г. Лазарева, А. Марущака, А. Новицького, Б. Раціборинського, В. Хахановського, В. Цимбалюка, М. Швеця та ін.

Слід зазначити, що за останні роки з питань інформаційної безпеки виконано низку дисертаційних робіт, більшість з яких пов'язані з питаннями національної інформаційної безпеки та захисту інформаційних систем. Однак питання інформаційної безпеки підприємств ще недостатньо досліджені. Це пов'язано в основному з тим, що автори більше уваги приділяють забезпеченню інформаційної безпеки держави, а у дослідників, які розглядають роль інформації в діяльності підприємств, відсутній підхід до проблеми в цілому. Тому в цьому дослідженні зроблено спробу проаналізувати проблему забезпечення інформаційної безпеки підприємств як об'єкта інформаційного права та інформаційних правовідносин.

Забезпечення інформаційної безпеки організації набуває все більшого значення в системах безпеки. Це пов'язано зі збільшенням обсягу інформаційних потоків та вдосконаленням засобів зберігання, передачі та обробки інформації. Оцифрування значної частини інформації та використання локальних і

глобальних мереж створюють нові загрози для конфіденційної інформації.

Слід зазначити, що в науковій літературі немає єдиного погляду на зміст понять "інформаційна безпека" та "інформаційна безпека організації".

Так, В. Цимбалюк визначає інформаційну безпеку як стан інформації, за якого забезпечується захист визначених політикою безпеки характеристик інформації [5]; В. Глашев стверджує, що інформаційна безпека - це бажана безпечна життєдіяльність особи, суспільства і держави, та розглядає її як різновид суспільно-інформаційних правовідносин щодо створення, підтримання, охорони і захисту середовища [6,]; С. Гутц розглядає інформаційну безпеку як стан, за якого захищені інформаційні потреби особи, суспільства і держави, забезпечується їх існування і прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз О. Литвиненко розглядає інформаційну безпеку як синтез трьох елементів забезпечення захисту інформації, захисту та управління національним інформаційним простором, забезпечення належного рівня інформаційної компетентності; цікавим, але суперечливим є визначення Б. Колміча. Б. Колмич стверджує, що інформаційна безпека - це захищеність встановлених законом правил, за якими здійснюються інформаційні процеси в державі, що забезпечують гарантовані Конституцією умови існування та розвитку особистості, суспільства в цілому і держави [9]; Л.Харченко, В. Ліпкан та О. Логінов визначають інформаційну безпеку як складову національної безпеки, процес управління загрозами і небезпеками державними і недержавними інституціями та окремими громадянами, що гарантує інформаційний суверенітет України [10].

Таким чином, інформаційну безпеку слід розглядати як забезпечення реалізації національних інтересів за допомогою різних інструментів, що є в нашому розпорядженні.

Щодо поняття "інформаційна безпека підприємств", то слід зазначити, що на сучасному етапі розвитку інформаційних технологій з впровадженням інформаційних систем в усі сфери людської діяльності та постійною взаємодією підприємств в інформаційній сфері вона є надзвичайно важливою.

О. Сороківська визначає інформаційну безпеку підприємства як суспільні відносини, пов'язані з побудовою та підтриманням на належному рівні інформаційних систем суб'єкта підприємницької діяльності [11]; М. Танцюра визначає інформаційну безпеку підприємства як захист конфіденційності, цілісності та доступності інформації. Доступність - це властивість бути доступною і використовуваною уповноваженими суб'єктами; цілісність - це властивість підтримувати точність і повноту даних; конфіденційність - це властивість захищати інформацію від несанкціонованого використання окремими особами, організаціями та процесами. Інформаційні активи - це інформація та дані, які мають цінність для організації [12]. Розглядаючи ці визначення, ми погоджуємося з А. Марущаком. "Корпоративна інформаційна безпека - це цілеспрямована діяльність організації та її персоналу з використанням компетентних сил і засобів для забезпечення безпеки інформаційного середовища організації, що гарантує нормальне функціонування і динамічний розвиток організації".

Обговоримо термінологію. Як вже зазначалося, на сьогоднішній день термінологія інформаційної безпеки значною мірою усталилася. Найбільш поширена і необхідна термінологія міститься в Українському стандарті технічного захисту інформації. Тому, звичайно, її будуть дотримуватися і надалі.

Іншими словами, інформаційна безпека - це стан інформації, при якому захищені характеристики інформації, визначені політикою безпеки.

Автоматизована система - це організаційно-технічна система, яка об'єднує комп'ютерні системи, фізичне середовище, персонал і оброблювану інформацію.

Захист інформації в автоматизованих системах (захист інформації, інформаційна безпека, інформаційна безпека, безпека комп'ютерних систем) - діяльність, спрямована на забезпечення безпеки інформації, що обробляється в автоматизованих системах, запобігання або ускладнення можливості реалізації загроз та зменшення розміру потенційного збитку від реалізації загроз.

Комплексна система захисту інформації - це сукупність організаційних та інженерно-технічних заходів, програмних і технічних засобів, які гарантують

захист інформації в автоматизованій системі.

Досвід показує, що боротьба зі злочинністю у сфері поширення інформації на підприємствах вимагає свідомої організації процесів захисту інформаційних ресурсів.

Джерела таких загроз можуть бути внутрішніми (власні працівники), зовнішніми (наприклад, конкуренти) або змішаними (замовники зовнішні, практикуючі власні працівники). Як показує практика, переважна більшість таких правопорушень скоюється власними співробітниками компанії.

Що є безпосередніми об'єктами злочинів у сфері розповсюдження інформації? По-перше, це інформація (дані). Злочинці отримують доступ до захищеної інформації без дозволу власника або з порушенням встановлених процедур доступу. Існують різні способи несанкціонованого доступу до комп'ютерної інформації, наприклад, крадіжка носіїв інформації, порушення інформаційної безпеки, використання чужого імені, зміна кодів або адрес технічних пристроїв, подання фіктивних документів на право доступу до інформації, встановлення записуючих пристроїв, підключених до каналів передачі даних і т.д. Крім того, доступ може бути отриманий з приміщення компанії, де зберігаються носії, з комп'ютера на роботі, з локальної мережі або з глобальної мережі. Усі загрози інформаційній безпеці можна класифікувати на п'ять груп за способом впливу інформаційні, фізичні, організаційно-правові, програмно-математичні та електронні.

Наслідки явно протиправних дій різноманітні:

- копіювання інформації (оригінал захищений);
- копіювання інформації (оригінал захищений); - Копіювання інформації (оригінал захищений); - Копіювання інформації (оригінал захищений);
- блокування інформації - не може бути використано при зберіганні інформації; - Блокування інформації - не може бути використано при зберіганні інформації
- безповоротне знищення інформації;
- знищення комп'ютерів, комп'ютерних систем та мереж.

Правове регулювання поширення інформації на підприємствах та відповідальність за порушення у цій сфері ґрунтується на тому, що відповідно до законодавства України документована інформація, до якої може бути здійснений неправомірний доступ, підлягає захисту, а неправомірний доступ може завдати шкоди її власнику або користувачеві. Захист здійснюється з метою запобігання несанкціонованому знищенню, зміні, перекрученню, копіюванню і блокуванню інформації, а також її витоку, крадіжці, втраті, спотворенню і підробленню, запобігання іншим формам незаконного втручання в роботу інформаційних ресурсів та інформаційних систем, забезпечення правового режиму документованої інформації як власності [15].

Крім того, за вищезазначені протиправні дії передбачена як адміністративна, так і кримінальна відповідальність. Це пов'язано з тим, що загрози інформаційним системам можуть призвести не тільки до значних фінансових втрат, але й до такого незворотного наслідку, як ліквідація самої організації.

Слід також враховувати, що загрози інформаційним системам можуть виходити від наступних осіб:

- співробітники компанії, які використовують своє службове становище (коли законні права цієї посади використовуються для незаконних операцій з інформацією);
- співробітник компанії, який має несанкціонований доступ до конфіденційної інформації, хоча не має на це повноважень в силу свого службового становища;
- особи, які не пов'язані з підприємством трудовим договором (контрактом).

Підсумовуючи вищевикладене, вважаємо за необхідне підкреслити, що найвищим пріоритетом у забезпеченні інформаційної безпеки на підприємстві є захист конфіденційності комерційно важливої інформації для того, щоб підприємство могло успішно конкурувати на ринку виробництва та реалізації товарів і послуг.

1.2. Цінність, класифікація та оцінка інформації як об'єкту інформаційної безпеки

Насправді, суть інформаційної безпеки полягає не в захисті інформації, а в захисті прав власності на інформацію. Щоб зрозуміти це, давайте подивимося на характеристики інформаційної власності.

Історично склалося так, що традиційними об'єктами права власності були матеріальні об'єкти, тобто права власності насправді були правами на віддалені об'єкти.

Знання, з іншого боку, не є матеріальним об'єктом. Знання - це інформація, тобто відображення дійсності у свідомості людини (і не важливо, правдиве воно чи неправдиве, важливо те, що є у свідомості). Лише згодом знання матеріалізується як матеріальний об'єкт у навколишньому світі. Але знання не є матеріальним об'єктом, воно нерозривно пов'язане з людським мозком і матеріальними носіями, які існують окремо від нас, такими як книги, дискети та інші "пам'яті" (пристрої зберігання інформації).

Можливо, з філософської точки зору, можна говорити про інформацію як про якусь абстрактну субстанцію, що існує сама по собі. Однак, з конкретної, матеріальної точки зору, зберігати і передавати інформацію без матеріального носія все одно неможливо.

Отже, можна виділити наступні характеристики знань:

1) інформація як об'єкт права власності може бути скопійована (відтворена) за допомогою матеріального носія. Як відомо, матеріальні об'єкти, що є об'єктами права власності, не можуть бути скопійовані (принаймні поки що). Дійсно, якщо ви подивитеся на два однакових об'єкти (наприклад, одяг або автомобіль), то побачите, що вони зроблені з однієї і тієї ж структури, але все ж таки відрізняються (чим детальніше ви подивитеся, тим більше вони відрізняються). Інформація, з іншого боку, залишається незмінною при копіюванні; це та сама інформація.

2) інформація як об'єкт власності може бути легко передана іншим

об'єктам власності без явного (або принаймні помітного) порушення прав власності на інформацію. Перехід матеріального об'єкта від одного суб'єкта до іншого (без його згоди) обов'язково призводить до втрати права власності на цей об'єкт первісним суб'єктом, тобто до явного порушення його права власності.

3) небезпека копіювання або передачі інформації посилюється тим, що інформація часто відчужується від її власника, тобто зберігається і обробляється в просторі (автоматизовані системи, комп'ютерні мережі тощо), доступному великій кількості суб'єктів, які не є власниками цієї інформації. Вбачається, що інформація як об'єкт права власності нічим не відрізняється від об'єкта традиційного права власності, за винятком вищезазначених характеристик.

Дійсно, відомо, що право власності включає в себе три речові права (право розпорядження, право володіння та право користування), які складають зміст права власності в цілому. Стосовно інформації можна сказати, що суб'єкт інформаційної власності може передати частину своїх прав (право розпорядження) іншому суб'єкту, наприклад, власнику матеріального носія (це володіння або користування) або користувачеві (це користування і, в деяких випадках, володіння), не втрачаючи при цьому своїх прав.

Для інформації право розпорядження означає виключне право визначати, кому (у володіння чи користування) надається ця інформація (нікому, крім власника). Право володіння означає право власності на цю інформацію в її первісному вигляді. Право на використання означає право використовувати цю інформацію у власних інтересах. Таким чином, окрім власника інформації, інші організації, що мають право власності, також можуть мати доступ до інформації, яка є законно дозволеною або (в силу згаданих вище характеристик) не є незаконно дозволеною.

Таким чином, виникає дуже складна система взаємовідносин між різними організаціями, що володіють правами власності. Ці відносини необхідно регулювати та захищати. Тому що будь-яке відхилення від цих відносин тягне за собою порушення права власності на інформацію. Реалізація

права власності на інформацію, як правило, пов'язана зі специфічною інфраструктурою (державною чи приватною).

Для інформації, як і для іншої власності, така інфраструктура складається з ланцюжка законодавча-судова-адміністративна (закон-суд-покарання). Тому, незважаючи на свої численні характеристики, інформація може і повинна розглядатися законом як об'єкт права власності нарівні з матеріальними об'єктами.

Будь-який закон про право власності повинен регулювати відносини між ними шляхом визначення суб'єкта та об'єкта права власності з метою захисту прав власника. Особливості регулювання цих відносин залежать від специфіки об'єкта права власності. У випадку інформаційної власності закон має регулювати відносини між суб'єктом і об'єктом права інформаційної власності, а також відносини між суб'єктом і об'єктом з метою захисту прав власника, законного володільця і користувача інформаційної власності від розголошення, оприлюднення та обробки (відтворення, модифікації та знищення).

В Україні прийнято Закон "Про інформацію" та Закон "Про захист інформації в автоматизованих системах" [8; 9]. Стаття 39 першого закону передбачає, що інформаційна продукція та інформаційні послуги громадян і юридичних осіб, які здійснюють інформаційну діяльність, можуть бути об'єктом товарних відносин, що регулюються Цивільним кодексом та іншим законодавством. Іншими словами, інформація є товаром. Інформаційна продукція (стаття 40) - це уречевлені результати інформаційної діяльності, призначені для задоволення інформаційних потреб громадян, державних органів, підприємств, установ та організацій. Інформаційні послуги (стаття 41) - це інформаційна діяльність у формі інформаційних продуктів, що надаються споживачам з метою задоволення їхніх інформаційних потреб.

Крім її представлення в комп'ютерних системах, цікаво і важливо подивитися на інформацію з інших точок зору. Зокрема, можна побачити, що інформація є товаром, а отже, об'єктом товарних відносин.

В Україні інформаційні відносини регулюються різними законами, в

тому числі Законом "Про інформацію". Зокрема, стаття 18 цього закону регулює класифікацію видів інформації:

- статистична інформація;
- масова інформація;
- інформація про діяльність органів державної влади та органів місцевого самоврядування;

- правова інформація;
- інформація про фізичних осіб;
- довідково-енциклопедична інформація;
- соціологічна інформація.

Інформацію можна купити, продати, імпортувати, підробити або викрасти, а отже, з нею треба поводитися певним чином. Крім того, інформація, якою людина обмінюється з іншою людиною або машиною через машину, є важливою і тому може підлягати захисту. Однак не вся інформація підлягає захисту, а лише та, яка має ціну, тобто цінність. Інформація є цінною, якщо володіння нею забезпечує певну вигоду (моральну, матеріальну, політичну тощо) її фактичному або потенційному власнику.

Оскільки в суспільстві завжди знайдуться люди, які захочуть отримати перевагу над іншими, вони можуть спробувати отримати цінну інформацію незаконним шляхом, і її власникам може знадобитися її захист. Цінність інформації є критерієм для прийняття рішення про необхідність її захисту. Хоча було зроблено багато спроб сформулювати процес оцінки цінності інформації з використанням теорії інформації та аналізу рішень, він залишається дуже суб'єктивним процесом.

У цьому оцінюванні знання потрібно класифікувати не лише за їхньою вартістю, але й за їхньою важливістю.

Залежно від рівня важливості інформацію можна класифікувати наступним чином:

- 1) базова інформація - її наявність необхідна для функціонування системи;

2) критична інформація - інформація, яка може бути змінена або відновлена, але процес відновлення якої є складним і дорогим;

3) корисна інформація - інформація, яку важко відновити, але без якої система функціонуватиме вкрай неефективно;

4) несуттєва інформація - інформація, без якої система може вижити.

Хоча ці категорії можуть здаватися простими у застосуванні, на практиці віднесення інформації до однієї з них може бути дуже складним завданням. Це пов'язано з тим, що одна і та ж інформація може використовуватися багатьма частинами системи, і кожна з них може присвоювати їй різну категорію важливості. Категорії важливості, як і цінність інформації, часто змінюються з часом і залежать від рівня важливості для різних груп споживачів та потенційних порушників.

Власник інформації - організація або особа, яка володіє інформацією; джерело інформації - організація або особа, яка надає інформацію; порушник - організація або особа, яка намагається отримати інформацію незаконним шляхом. Для цих груп одна і та ж інформація може мати різний рівень важливості, зокрема:

- інформація про діяльність компанії (списки замовлень і графіки виробництва на певний тиждень) важлива для власника компанії, але не має ніякої цінності для джерела (замовника) або порушника;

- інформація про перспективи розвитку ринку може бути важливою для порушника, але вже не є важливою для джерела або власника компанії, який завершив аналіз.

Наведена вище класифікація суттєвості повністю узгоджується з існуючим принципом розподілу інформації за рівнями (або категоріями) секретності.

Ступінь секретності - це адміністративний або правовий захід, що відповідає ступеню відповідальності особи, яка розголошує певну інформацію, який регламентується спеціальним документом, з урахуванням національних, військово-стратегічних, комерційних, громадських або особистих інтересів.

Такою інформацією може бути державна, військова, комерційна, службова або особиста таємниця. Ступінь секретності визначається грифом секретності, який присвоюється інформації.

В Україні в державних структурах встановлено такі рівні (грифи) таємності [24]: несекретно, для службового користування, таємно, цілком таємно (Н, ДСК, Т, ЦТ). Аналогічна термінологія існує в більшості країн світу: unclassified, confidential, secret, top secret (U, C, S, TS). Така класифікація дає можливість визначити просту лінійну порядкову шкалу цінності інформації: $H < ДСК < Т < ЦТ$ ($U < C < S < TS$). Цей захід одразу дає зрозуміти, до яких категорій інформації слід застосовувати підвищені вимоги щодо захисту.

Однак слід додати, що, як показує практика, у багатьох випадках конфіденційна інформація - це не єдине, що потребує захисту. Несанкціонований перегляд або модифікація несекретної інформації може призвести до розкриття або втрати відповідної конфіденційної інформації, а також перешкодити автоматизованим системам виконувати свою функцію обробки конфіденційної інформації. Існує також потенційна можливість компрометації чутливої інформації шляхом аналізу набору несекретної інформації. Все це підтверджує тезу про складність класифікації інформації, що підлягає захисту.

Як зазначалося раніше, інформація в останні роки стала найважливішим ресурсом, випередивши навіть сировинні та енергетичні ресурси. Однак для її ефективного використання необхідно вміти оцінювати її важливість для виконання відповідної діяльності, тобто вміти оцінювати інформацію як об'єкт праці.

Для такої оцінки необхідні два типи показників:

- 1) характеристики знань як ресурсу, що забезпечує процес пошуку рішень різних проблем;
- 2) характеристики знання як об'єкта звичайної праці.

Зміст показників першого типу визначається важливістю інформації в процесі вирішення проблем, а також обсягом і складом інформації, що

використовується. Під кількістю інформації тут мається на увазі не абсолютна кількість даних, що використовуються в процесі розв'язання задачі, а їх достатність для інформаційного забезпечення конкретної задачі та адекватність поставленому завданню.

Таким чином, перший тип індикатора виглядає наступним чином:

- важливість - узагальнений показник, що характеризує важливість інформації з точки зору завдання, для якого вона використовується, та організації її обробки. Важливість - це узагальнений показник, що характеризує важливість інформації з точки зору завдань, для яких вона використовується, та організації її обробки. Оцінка тут може здійснюватися за важливістю операцій у відповідній діяльності, ступенем важливості інформації для ефективної реалізації відповідних операцій, рівнем витрат на небажані зміни в інформації та рівнем витрат на відновлення витоку інформації. Зауважимо, що для деяких видів інформації ступінь важливості можна дуже точно оцінити за допомогою так званих коефіцієнтів важливості, які розраховуються на основі математичних, лінгвістичних або неформальних евристичних моделей;

- повнота - показник достатності знань для вирішення поставленого завдання. Для вимірювання цього показника також існують формальні та неформальні моделі розрахунку коефіцієнтів повноти;

- релевантність - це ступінь відповідності знань реальній ситуації предмета, який вони відображають. Актуальність залежить від об'єктивності, з якою отримано знання про предмет, та від часу, що пройшов між моментом їх отримання та моментом оцінювання компетентності. Зауважимо, що існують також формальні та неформальні підходи до оцінювання компетентності, які дозволяють здійснювати кількісну оцінку;

- релевантність - міра відповідності знань потребам розв'язуваної задачі. Відомий коефіцієнт релевантності - це відношення кількості релевантної інформації до загального обсягу інформації. Існують також моделі для його розрахунку;

- толерантність - це міра легкості розпізнавання і використання інформації в процесі розв'язання задачі. Це поняття настільки широке, розпливчате і суб'єктивне, що формального методу оцінки не існує.

Нагадаємо, що всі етапи обробки інформації повинні відповідати показникам першого типу. Зрозуміло, що найважливішим тут є форма і подання інформації, а також її кількість. Таким чином, до другого типу індикаторів відносяться:

- 1) метод або система, за допомогою якої інформація кодується, тобто ефективність кодування;
- 2) обсяг коду, що відображає цю інформацію.

Слід зазначити, що методи визначення цих показників добре розроблені в теорії інформації. Тому необхідний рівень захисту інформації повинен визначатися з урахуванням значень усіх вищезазначених показників, а також грифу конфіденційності.

Насамкінець слід звернути увагу на описану вище різницю між конфіденційністю та інформаційною безпекою [8].

Отже, інформаційна безпека - це захищеність інформації від несприятливих впливів на неї і пов'язана з технічними процедурами, що забезпечують її захист. Конфіденційність інформації - це стан інформації, який фіксується відповідно до її важливості та потребує певного рівня захисту. Таким чином, це поняття стосується особи або осіб, які несуть відповідальність за інформацію і вирішують, яку інформацію слід оприлюднити, а яку приховати від інших.

1.3. Проблеми інформаційного захисту в контексті автоматизації та інформатизації сучасних підприємств

Сучасне суспільство не могло б існувати без постійного використання інформаційних технологій. Комп'ютери підтримують банківські системи, контролюють роботу ядерних реакторів, розподіляють енергію, стежать за

розкладом руху поїздів і літаків, керують космічними апаратами. Комп'ютерні системи і телекомунікації визначають надійність і силу національних систем оборони і безпеки. Комп'ютери роблять інформаційні технології можливими, дозволяючи зберігати, обробляти і надавати інформацію споживачам.

Однак метою сучасного суспільства є найвищий ступінь автоматизації, який залежить від ступеня безпеки інформаційних технологій, що стосується добробуту і навіть життя багатьох людей. Технічний прогрес має деякі неприємні особливості. У кожному досягненні завжди є щось, що обмежує його розвиток і на певному етапі обертає успіх на шкоду, а не на користь людству.

У випадку інформаційних технологій це означає, що широке використання популярних, дешевих, масових комп'ютерних систем робить їх надзвичайно вразливими до деструктивних впливів. Приклади, що підтверджують поширеність цього явища, можна знайти на сторінках багатьох видань, а в Інтернеті їх набагато більше. Фактів настільки багато, що для їх перерахування знадобиться багато часу. Наприклад, у 2018 році повідомлялося, що в середньому кожні 20 секунд у США скоюється злочин, пов'язаний з програмним забезпеченням (а зараз, мабуть, частіше). Понад 80 відсотків комп'ютерних злочинів скоюється через Інтернет. Оцінки збитків коливаються від десятків мільйонів до мільярдів доларів. Точні підрахунки неможливі з ряду причин. Багато організацій не знають про те, що сталося порушення, а це означає, що інформація може бути викрадена без їхнього відома. Тому інформація стала таким важливим і цінним товаром, оскільки вона пов'язана з можливістю матеріальної, економічної та моральної шкоди.

Як показує аналіз історичних фактів і сучасний досвід, постійно винаходяться нові види і форми обробки інформації і, паралельно, нові види і форми її захисту. Однак повністю захистити інформацію неможливо і, мабуть, ніколи не вдасться. Іншими словами, можна говорити про своєрідну кризову ситуацію в сфері безпеки інформаційних технологій.

Які передумови сьогоденної кризи? Не зупиняючись на соціальних,

правових та економічних аспектах проблеми, систематизуємо науково-технічні передумови кризової ситуації у сфері безпеки інформаційних технологій [9].

Збільшення обсягів інформації, що накопичується, зберігається та обробляється за допомогою комп'ютерів та інших засобів інформаційно-обчислювальної техніки (ІКТ). При цьому йдеться не тільки про стрімке і реальне збільшення обсягів інформації, а й про розширення арсеналу методів, засобів і можливостей її концентрації та зберігання, наприклад, коли інформація різного призначення і зв'язків може бути зібрана в єдиній базі даних. Дійсно, якщо потрапити в досить потужну базу даних, то можна буквально дізнатися про все на світі. Такі можливості розширилися, особливо з появою глобальної мережі Інтернет.

Сучасні комп'ютери за останні роки набули величезної обчислювальної потужності, але (як це не парадоксально) вони також стали набагато простішими у використанні. Це означає, що в результаті "персоналізації" ПК більшість користувачів тепер володіють власними робочими станціями і керують ними, вони стали простішими у використанні, і все більше нових користувачів мають доступ до комп'ютерів.

Підтримувати високий рівень безпеки системи на регулярній основі для більшості користувачів не є можливим, оскільки це вимагає відповідних знань, навичок, часу та грошей. Поширення мережевих технологій дозволило об'єднати окремі комп'ютери в локальну мережу, де вони мають спільні ресурси, а використання технології клієнт-сервер перетворило такі мережі на розподілені обчислювальні середовища. Сьогодні безпека мережі залежить від безпеки всіх її компонентів, і зловмиснику достатньо порушити роботу одного з них, щоб скомпрометувати всю мережу.

Сучасні телекомунікаційні технології інтегрували локальні мережі в глобальні. В результаті виникло унікальне явище: Розвиток Інтернету призвів до підвищеного інтересу до питань безпеки і, принаймні частково, викликав необхідність перегляду базових правил. Насправді, на додаток до всіх переваг

його використання, Інтернет пропонує широкі можливості для компрометації безпеки комп'ютерних систем по всьому світу. Поки комп'ютер підключений до Інтернету, для злочинців не має значення, чи знаходиться він у сусідній кімнаті, чи на іншому кінці світу.

Розвиток апаратного забезпечення супроводжується ще більш стрімким розвитком програмного забезпечення. Як показує практика, більшість сучасного програмного забезпечення, яке широко використовується (особливо операційні системи), не відповідає навіть мінімальним вимогам безпеки, незважаючи на значні зусилля розробників. В основному це пов'язано з неправильним налаштуванням функцій безпеки та різними "недокументованими" можливостями. Після виявлення багато недоліків усуваються за допомогою оновлення версії або додаткових інструментів, але частота, з якою виявляються нові недоліки, викликає занепокоєння. Коротше кажучи, більшість систем надають зловмисникам широкий спектр можливостей для здійснення порушень.

Завдяки появі та широкому розповсюдженню віртуальних машин та різноманітних інтерпретаторів, різниця між даними та виконуваними програмами майже зникає на наших очах. Сьогодні всілякі складні програми, від текстових процесорів до браузерів, не лише обробляють дані, але й інтерпретують інструкції інтегрованих в них спеціалізованих мов програмування. Це значно розширює можливості зловмисників у створенні засобів для проникнення в чужі системи та ускладнює захист через необхідність контролювати взаємодію на іншому рівні - рівні віртуальних машин та інтерпретаторів.

Існує значний розрив між теоретичними моделями безпеки, які працюють з абстрактними поняттями, такими як об'єкти та суб'єкти, та сучасними інформаційними технологіями. Це призводить до невідповідності між моделлю безпеки та її застосуванням у засобах обробки інформації. Крім того, багато заходів безпеки, таких як заходи проти комп'ютерних вірусів і системи брандмауерів, не мають систематичного наукового обґрунтування. Це пов'язано

з відсутністю загальної теорії інформаційної безпеки, відсутністю комплексної моделі комп'ютерної безпеки, що описує механізми дії зловмисних атак на реальні системи, і відсутністю системи, яка може ефективно перевіряти конкретні рішення з безпеки. Така ситуація склалася. Як наслідок, майже всі системи безпеки базуються на аналізі результатів успішних атак і відстають від реальної ситуації. Прикладом цього є поширена практика закриття вразливостей, які "раптово" виявляються. На додаток до вищесказаного, в цій галузі (особливо в нашій країні) не існує навіть загальноприйнятої термінології. Теорія і практика часто знаходяться в різних площинах.

В сучасних умовах дуже важливо створити нормативну базу, яка б встановлювала вимоги до безпеки і не ускладнювала завдання розробника, а навпаки, встановлювала базовий рівень безпеки. Існує низка міжнародних стандартів, які намагаються вирішити це питання, але до недавнього часу не можна було сказати, що вони є керівництвом до дії або навіть закладають основи для майбутніх безпечних інформаційних технологій.

Різні країни, в тому числі й Україна, розробили документи, які лише частково імітують іноземні стандарти десятирічної давнини. Оскільки найважливіші галузі економіки та державні органи значною мірою оснащені інформатизацією та комп'ютеризацією, наша країна потребує нових рішень у цій сфері.

Ситуація у сфері інформаційних технологій в Україні є надзвичайно складною. Хоча Україна має один з найвищих рівнів індексу освіти у світі (98%) і великий потенціал з населенням близько 36 мільйонів осіб, промисловість знаходиться на низькому рівні, а інфраструктура недостатньо розвинена.

Сьогодні здійснення державного планування втратило свою інтелектуальну складову і зводиться переважно до реалізації інформаційно-транспортної системи, тобто системи зв'язку. Такі важливі завдання, як формування стратегії розвитку України, підготовка державного бюджету та інші питання державного будівництва є складовими інтелектуального кібернетичного питання. Однак цієї специфічної складової національної інформаційної політики не існує.

Нарешті, глобальна безпека. Останніми роками спостерігається зростання питань, пов'язаних з безпекою людей в усьому світі. Внаслідок політичної та економічної нестабільності відбувається постійний потік негативних подій - від локальних війн до міжнародного тероризму. Тому проблема забезпечення економічної, матеріальної і навіть фізичної безпеки стала більш складною. З широким розповсюдженням інформаційних технологій практично у всіх сферах людської діяльності забезпечення такої безпеки стало безпосередньо пов'язане з інформаційною безпекою.

В результаті сукупного впливу цих факторів перед розробниками сучасних інформаційних систем, призначених для обробки критично важливої інформації, постають наступні виклики, які потребують нагального та ефективного вирішення:

1. Захист нових типів джерел інформації. Оскільки комп'ютерні системи сьогодні безпосередньо інтегровані в інформаційну структуру сучасного суспільства, засоби захисту повинні враховувати сучасні форми представлення інформації (наприклад, гіпертекст, мультимедіа). Це означає, що системи безпеки повинні забезпечувати безпеку на рівні інформаційних ресурсів, а не на рівні окремих документів, файлів або повідомлень.

2. Організація довіреної взаємодії (взаємна ідентифікація/автентифікація) між сторонами в інформаційній сфері. Розвиток локальних мереж та Інтернету вимагає ефективного захисту віддаленого доступу до інформації та взаємодії з користувачами через мережі загального користування. Причому це завдання необхідно вирішувати в глобальному масштабі, незважаючи на те, що зацікавлені сторони знаходяться в різних частинах світу і працюють на різних апаратних платформах і під управлінням різних операційних систем.

3. Захист від автоматизованих засобів атаки. Це здатність забезпечити безпеку за умови будь-якої взаємодії з такими засобами, включаючи появу всередині програм деструктивних програм, таких як комп'ютерні віруси, автоматизовані засоби злому та атакуючі агенти. На перший погляд може здатися, що цю проблему можна вирішити за допомогою контролю доступу, але це не зовсім так, оскільки відомі випадки поширення комп'ютерних вірусів у

"захищених" системах.

4. Інтеграція захисту інформації в автоматизовані процеси як невід'ємний елемент. Для того, щоб закріпитися на сучасному ринку інформаційних систем, засоби захисту не повинні суперечити існуючим практикам і усталеним технологіям обробки інформації, а навпаки, бути невід'ємною частиною цих засобів і технологій.

5. Розробити сучасні математичні моделі безпеки, які є надійними, релевантними та ефективними. Якщо ці виклики не будуть вирішені, подальше поширення інформаційних технологій у сфері критичних систем, що обробляють важливу інформацію, рано чи пізно опиниться під загрозою. Починаючи з нуля у сфері інформаційних технологій, наша країна є полігоном для випробування новітніх досягнень в інформаційних технологіях, і нам як ніде в світі необхідно будувати безпечні інформаційні системи.

Для кращого розуміння питання інформаційної безпеки корисно простежити історичну траєкторію розвитку та створення систем захисту інформації (СЗІ).

Питання захисту інформації в автоматизованих системах обробки даних (АСОД) пройшло багато в чому суперечливий шлях від своєї постановки в кінці 60-х років до наших днів. Спочатку існувало два шляхи вирішення проблеми конфіденційності:

- використання криптографічних методів захисту інформації на носіях передачі та зберігання даних;
- розмежування доступу до даних і ресурсів комп'ютерної системи між програмним і апаратним забезпеченням.

Слід зазначити, що в той час автоматизовані системи зберігання даних не були широко розповсюджені, а технології глобальних і локальних мереж перебували в зародковому стані. Тому застосування в цих сферах були дуже успішними; крім того, в цей період була розроблена "евристична" термінологія інформаційної безпеки (наприклад, противник, ресурс, дані).

Ці особливості характеризували перший етап створення СЗІ, основна ідея якого полягала в забезпеченні надійного захисту за допомогою механізмів, що

включають технічні та програмні засоби. Технічні засоби - це засоби, реалізовані у вигляді електричних, електромеханічних та електронних пристроїв. Вони поділяються на апаратні (вбудовані в обладнання СКУД) та фізичні (реалізовані у вигляді електронного та механічного обладнання, автономних пристроїв, таких як охоронна сигналізація, замки та огорожі). Вважалося, що програмне забезпечення є основним засобом захисту і що програми захисту будуть ефективно працювати, якщо вони будуть інтегровані в загальне програмне забезпечення системи. Було створено концепцію ядра безпеки. Це означало спеціальне програмне забезпечення, що містить мінімально необхідні механізми безпеки, які можна було б доповнювати різними інструментами залежно від конкретних обставин. Однак пізніше виявилось, що цього недостатньо.

Зростаюча тенденція до децентралізованих автоматизованих інформаційних систем дала зрозуміти, що в цій сфері існують обмеження, і проблеми автентифікації інтерактивних елементів автоматизованих інформаційних систем і методи управління криптографічними механізмами в децентралізованих системах почали ретельно вивчатися. Стало зрозуміло, що механізми криптографічного захисту не є первинними і повинні розглядатися паралельно з іншими механізмами КЗ.

Зокрема, для перевірки надійності КСЗІ була створена спеціальна команда висококваліфікованих експертів (Tiger Team), яка займалася зломом (часто анонімно) і тестуванням КСЗІ. У цей період також інтенсивно розроблялися заходи технічного захисту та шифрування. Але кількість порушень безпеки не зменшувалася, отже – був отриманий важливий теоретичний результат (теорема Гаррісона). Суть теореми полягала в тому, що неможливо вирішити проблему абсолютного захисту будь-якої системи в умовах проблеми публічного доступу; як писав Д. Хоффман [8], це було все одно, що вилити холодну воду на затятих прихильників безпеки. Дехто навіть був налаштований песимістично, вважаючи, що досягнення сильної безпеки є абсолютно неможливим. Почалися пошуки виходу з цього глухого кута, і це сформувало контекст третього етапу в історії побудови надійних ІПС.

Наступним кроком було відокремлення власне заходів захисту (наприклад, шифрування, контроль доступу) від засобів, що гарантують їх коректне функціонування. Адже раніше інформація захищалася лише опосередковано, а фактично захищалося її середовище (носії, системи обробки тощо). Стало зрозуміло, що необхідно не тільки шукати механізми захисту, а й враховувати весь процес створення КСЗІ на всіх етапах життєвого циклу системи. Таким чином, все (інструменти, методи і заходи) можна було б поєднати в системі захисту найбільш раціональним чином. Крім того, активно розроблялися і застосовувалися на практиці математичні моделі захисту. Вже в Помаранчевій книзі була встановлена необхідність суворого доказу певного рівня захищеності системи.

По-перше, тому що програмне забезпечення все ще відіграє важливу роль у якості обробки інформації; по-друге, тому що програмне забезпечення все частіше стає предметом комерційної таємниці; по-третє, тому що програмне забезпечення є найбільш вразливим з усіх компонентів автоматизованих інформаційних систем.

І по-третє, воно є найбільш вразливим з усіх компонентів автоматизованих інформаційних систем.

Сьогодні тему ІПС можна охарактеризувати кількома ключовими моментами:

- теоретичність, тобто теорія теорією, але більшість положень спочатку реалізуються (принаймні поки що) у вигляді конкретних планів або рекомендацій, а потім узагальнюються і закріплюються як теоретичні положення або методологічні рекомендації;

- багатовимірність, тобто забезпечення безпеки більш ніж на одному фронті;

- невизначеність внаслідок людського фактору - ми не знаємо, хто, коли, де і як може порушити безпеку об'єкта, що захищається;

- усвідомлення того, що неможливо досягти ідеального (абсолютного) захисту;

- застосування оптимізаційного підходу - мінімізація ризиків і можливих збитків внаслідок вибору лише певного ступеня захисту в кожному конкретному випадку залежно від певних умов (наприклад, можливих витрат на захист,

передбачуваних загроз і т.д.);

-іншими словами, завжди береться до уваги час життя інформації та час, необхідний для подолання вразливості (звісно, останній має бути більшим за перший).

До загального уявлення про інформаційну безпеку слід додати ще дещо. Наприклад, багато людей, навіть кваліфікованих комп'ютерних експертів, ототожнюють інформаційну безпеку з криптографією. Можливо, на це є історичні причини, але сьогодні криптографія сама по собі може забезпечити лише певний рівень конфіденційності інформації, а не інформаційну безпеку в цілому.

Насправді в сучасних інформаційних системах інформаційна безпека повинна забезпечувати не тільки конфіденційність інформації (а набагато більше), але в першу чергу її цілісність і доступність. Причому друга якість інформації іноді є найважливішою.

Хакери не сплять ночами, лише думаючи про те, як обійти захист. Насправді переважна більшість інформаційних загроз (це повністю підтверджується статистикою - понад 90%) реалізована в самій системі - це питання банальної некомпетентності, незрілості, недбалості та байдужості тих, хто відповідає за систему. Іншими словами, інформаційна безпека - це не тільки технічні заходи та протидії, але й людські ресурси, їх навчання та правильний відбір (згадайте відомий слоган "кадри вирішують все"). Інша думка полягає в тому, що безпека статична, захист організований і всі сплять спокійно. Але життя не стоїть на місці, все рухається і розвивається. Тому одним з найважливіших принципів організації інформаційної безпеки є безперервний захист, як у часі, так і в просторі.

Багато людей також вважають, що їхня інформація не є достатньо цінною, щоб виправдати зусилля з її захисту. Така точка зору є дуже небезпечною, оскільки оцінка важливості та цінності інформації, особливо власної, є складним і суб'єктивним процесом.

Національна політика інформатизації формується як частина соціально-економічної політики держави в цілому і спрямована на раціональне

використання виробничого, науково-технічного потенціалу, матеріально-технічних і фінансових ресурсів та сучасної інформаційної інфраструктури для розв'язання поточних і перспективних завдань розвитку України як незалежної демократичної держави з ринковою економікою.

З метою прискорення процесу інформатизації, що потребує відповідної концентрації ресурсів, державна політика має базуватися на державному регулюванні процесу інформатизації на основі поєднання принципів централізації та децентралізації, саморозвитку, самофінансування та самоокупності, а також прямої підтримки через системи пільг, системи фінансування та бюджет.

Бюджетні кошти мають спрямовуватися насамперед на реалізацію національних інформаційних проектів:

- побудова національної інформаційно-комунікаційної системи;;
- створення національної інформаційно-комунікаційної системи;
- інформування стратегічних напрямів розвитку національної економіки, безпеки, оборони та соціальної сфери.

Державне регулювання має розвивати національну інформатизацію системно, комплексно та узгоджено, використовуючи традиційні та нетрадиційні форми і методи підтримки та управління.

Пріоритети не повинні бути постійними, а встановлюватися на певний період часу і коригуватися відповідно до ситуації.

Найважливішими пріоритетами є створення нормативно-правової бази у сфері інформації, включаючи системи захисту авторських прав і персональних даних та розробка національних стандартів у сфері інформації; створення телекомунікаційної інфраструктури, головним чином шляхом оптимізації існуючих мереж передачі даних і будівництва нових сучасних каналів, включаючи волоконно-оптичні та супутникові системи зв'язку; створення комп'ютерних мереж для освіти, науки і культури як частини глобальної мережі Інтернет та реалізація інформаційно-комунікаційних заходів.

Не менш важливим інформаційним законом є Закон України "Про

Національну програму інформатизації України". Цей закон був прийнятий 4 лютого 1998 року. Він встановлює загальні засади формування, виконання та координації національної інформаційної програми.

Незалежно від того, наскільки складною є інформаційна тема, повинна бути забезпечена інформаційна безпека.

Найважливішим у цьому напрямку є, звичайно, «Закон про захист інформації в автоматизованих системах», про який більш детально йтиметься нижче, а тут розглянемо основні поняття та напрямки розвитку захисту інформації в Україні, користуючись системою нормативних документів із захисту інформації.

Нагадаємо, що одним з основних понять нашого розгляду є автоматизована система (АС). АС – це організаційно-технічна система, що об'єднує обчислювальну систему, фізичне середовище, персонал і оброблювану інформацію (рис. 1.1).

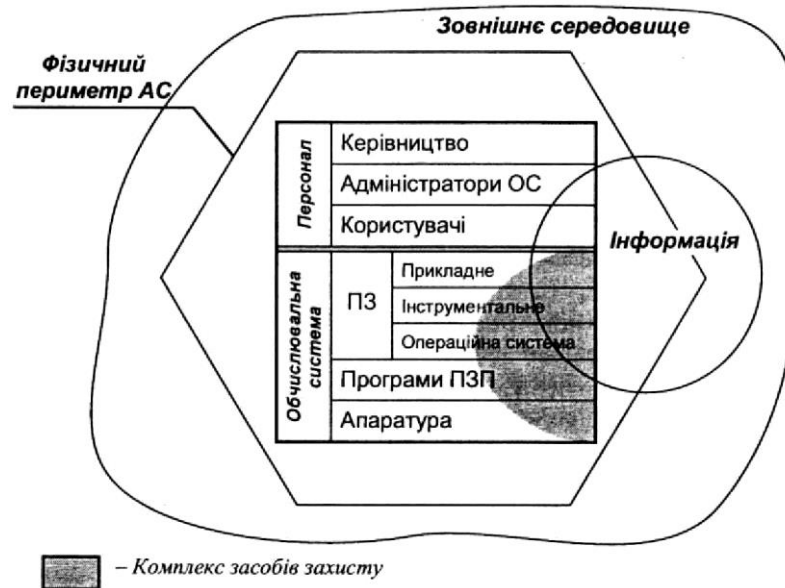


Рис. 1.1. Автоматизована система обробки інформації

Джерело: [14]

Розрізняють два основних напрями технічного захисту інформації в АС – це захист АС і оброблюваної інформації від несанкціонованого доступу (НСД) і захист інформації від витоку технічними каналами (оптичними,

акустичними, захист від витоку каналами побічних електромагнітних випромінювань і наведень (ПЕМВН)).

Якщо в автоматизованій системі обробляється інформація, порядок обробки та захисту якої регулюється законодавством України або іншими нормативно-правовими актами (наприклад, інформація, що становить державну таємницю), необхідно отримати дозвіл відповідного компетентного державного органу на обробку такої інформації в цій автоматизованій системі. Підставою для надання такого дозволу є висновок аудиту автоматизованої системи, тобто перевірка відповідності впровадженої КСЗІ встановленим стандартам.

Автоматизована система комп'ютерна система - це сукупність апаратних і програмних засобів, призначених для обробки інформації; кожен компонент операційної системи може розроблятися і продаватися як самостійний продукт. Кожен з цих компонентів може реалізовувати певні функції захисту інформації, а їх оцінка може виконуватися незалежно від процесу аудиту автоматизованої системи і має характер сертифікації. За результатами сертифікації видається атестат про те, що реалізовані функції безпеки відповідають певним вимогам (критеріям). Атестат на автоматизовану систему або її окремі компоненти може полегшити процес аудиту автоматизованої системи.

Можливі випадки, коли для формування певної КС використовуються компоненти, і кожен компонент або частина компонента має атестат, який підтверджує, що він реалізує певні функції захисту інформації. Однак це не означає, що КС, сформована з таких компонентів, реалізує всі ці функції. Для забезпечення останнього проектування КС має бути реалізовано з метою інтеграції захисту, що надається кожним компонентом, в єдиний захист. Таким чином, сертифікат слід розглядати як потенційну здатність КС реалізовувати конкретні функції, що захищають оброблювану інформацію від конкретних загроз.

Він також розкриває ключові характеристики інформації, які

безпосередньо визначають цінність інформації. Ключовими характеристиками захищеної інформації є конфіденційність, цілісність, доступність та підзвітність.

Конфіденційність, інтуїтивно зрозумілий термін, точніше визначається як властивість інформації, яка не може бути використана несанкціонованими користувачами та/або процесами.

Цілісність інформації - це властивість, яка полягає в тому, що інформація не може бути змінена несанкціонованими користувачами та/або процесами. Цілісність інформації може бути фізичною або логічною.

Доступність інформації - властивість, яка полягає в тому, що інформація може бути використана за запитом користувача з відповідними повноваженнями.

Спостережуваність - це властивість інформації, яка означає, що процеси обробки повинні завжди перебувати під контролем певного органу контролю безпеки.

Потенційні негативні впливи на інформацію, які призводять до порушення хоча б однієї з цих властивостей, називаються інформаційними загрозами. Рівень захищеності інформації в системі - це конкретна міра ймовірності (наприклад, ймовірність) того, що на даному етапі функціонування системи відбудеться небажаний вплив на інформацію, тобто подія, яка може призвести до порушення хоча б однієї з перерахованих вище ФПБ. Базові поняття конфіденційності, цілісності та доступності, які безпосередньо пов'язані з інформацією, мають такі важливі характеристики:

- незалежність - кожне з введених понять не залежить від інших. Це дозволяє визначити конкретну область при моделюванні інформаційної безпеки і розглядати їх цілісність як фундаментальну в цій області;

- конструктивізм - чітке визначення проблемних аспектів ІБ дозволяє використовувати конкретні механізми та заходи для їх реалізації;

- можливість їх багаторазового перекриття при використанні різних механізмів та заходів захисту (як показує практика, механізми та заходи ІБ

завжди сприяють одночасно деяким з вищезазначених характеристик);

- можливість врахування конкретних загроз інформації при формулюванні конкретних завдань захисту;
- визначити послуги із захисту кожної ЗВДТ відповідно до важливості інформації, очікуваних загроз інформації, цілей та завдань.

Не слід плутати конфіденційність і безпеку. Якщо конфіденційність визначає певний стан захисту інформації, то безпека стосується механізмів, які використовуються для підтримання цього стану. Також, на відміну від конфіденційності, цілісність визначає лише ступінь узгодженості певних представлень інформації в системі.

Аналізуючи поточну ситуацію в секторі інформаційної безпеки, можна побачити, що сьогодні компанії, які неодноразово стикаються з незаконними діями інших організацій в процесі своєї діяльності, не звертаються до правоохоронних органів або, в цілому, не бажають розголошувати атаки на свої інформаційні системи. Це пов'язано з тим, що компанії та комерційні банки не "лякають" клієнтів та споживачів тим, що їхні інформаційні системи (та вся інформація, що міститься в них) не захищені належним чином. Потенційний злочин є найбільш шкідливим, оскільки безвідповідальність злочинців дозволяє продовжувати і поширювати незаконну діяльність.

Забезпечення безпеки компаній з боку інформаційних систем є однією з перешкод на шляху до вирішення загальної проблеми безпеки. Захист від злочинів у сфері розповсюдження інформації повинен починатися з розробки концепції інформаційної безпеки на підприємствах.

Методи захисту підприємств від злочинів у сфері розповсюдження інформації можна розділити на дві категорії: організаційні та технічні методи. До організаційних методів захисту належить обмеження несанкціонованого фізичного доступу до інформаційних систем. Технічні методи захисту передбачають використання програмно-технічних засобів, основною метою яких є обмеження доступу до несанкціонованої інформації користувачів, що працюють в інформаційних системах компанії [16].

Практики виділяють такі основні напрямки технічного захисту інформаційних систем, як:

- захист інформаційних ресурсів від несанкціонованого доступу та використання - використання засобів контролю завантаження програмного забезпечення та парольного захисту при вході в систему;

- захист від витоку вторинними шляхами електромагнітних випромінювань та наведень - екранування обладнання та приміщень, використання маскувальних генераторів шуму, додаткові перевірки обладнання на наявність небезпечних випромінювань тощо; - захист від витоку інформації з каналів зв'язку та комутаційних вузлів - процедури аутентифікації;

- захист інформації на каналах зв'язку та вузлах комутації - застосовуються процедури аутентифікації абонентів та повідомлень, шифрування, спеціальні протоколи зв'язку;

- захист юридичної значимості електронних документів - у разі довірчих відносин між двома організаціями або необхідності передачі документів (платіжних доручень, контрактів) через комп'ютерні мережі до документа додається "цифровий підпис" (спеціальна позначка) для визначення автентичності адресата;

- для захисту автоматизованих систем від комп'ютерних вірусів та несанкціонованих модифікацій використовуються програми імунітету та механізми модифікації програмних фактів.

Разом з тим, одним з головних аспектів, на який слід звернути увагу, є підтримка інформаційної безпеки підприємства, яка буде проявлятися протягом усього часу існування підприємства.

РОЗДІЛ 2

ДОСЛІДЖЕННЯ СТАНУ УПРАВЛІННЯ СИСТЕМОЮ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НАПРАТ "КІРОВОГРАДОБЛЕНЕРГО"

2.1. Оцінка виробничо-господарської діяльності ПрАТ "Кіровоградобленерго"

Основою енергетичної галузі України є Об'єднана енергетична система України (ОЕС), яка централізовано постачає електроенергію місцевим споживачам, взаємодіє з енергосистемами сусідніх країн та забезпечує імпорт, експорт і транзит електроенергії. ОЕС об'єднує об'єкти електроенергетики та розподільчі мережі в регіонах України. Оперативно-технічне управління ОЕС, регулювання режимів роботи енергосистеми, забезпечення надійності та паралельної роботи з енергосистемами інших країн здійснює центральна державна компанія ДП НЕК "Укренерго".

Понад десять років в Україні функціонує оптовий ринок електроенергії (ОРЕ) - сучасна система купівлі-продажу електроенергії. Державне регулювання енергетичного ринку здійснює Національна комісія, що здійснює державне регулювання у сфері енергетики (НКРЕ), основними завданнями якої є ліцензування та регулювання діяльності суб'єктів природних монополій, забезпечення реалізації цінової та тарифної політики, захист прав споживачів та дотримання правил користування електроенергією.

Основними завданнями ОРЕ є:

- задоволення попиту споживачів України на електричну енергію за найнижчою можливою ціною на основі конкуренції між генеруючими компаніями та постачальниками;
- забезпечення фінансової стабільності та прибутковості електроенергетичної галузі;
- побудова конкурентоспроможного енергетичного сектору України та створення умов для залучення потенційних інвесторів.

Хоча оптовий ринок почав функціонувати в 1996 році в рамках системи ринку єдиного покупця, функціонування ОРЕ тривалий час залишалося нестабільним, головним чином через несплату рахунків за електроенергію та накопичені боргові проблеми. Однак, починаючи з 2000 року, ситуація з угодами покращилась.

Поточна схема ринку ОРЕ показана на рисунку 2.1.

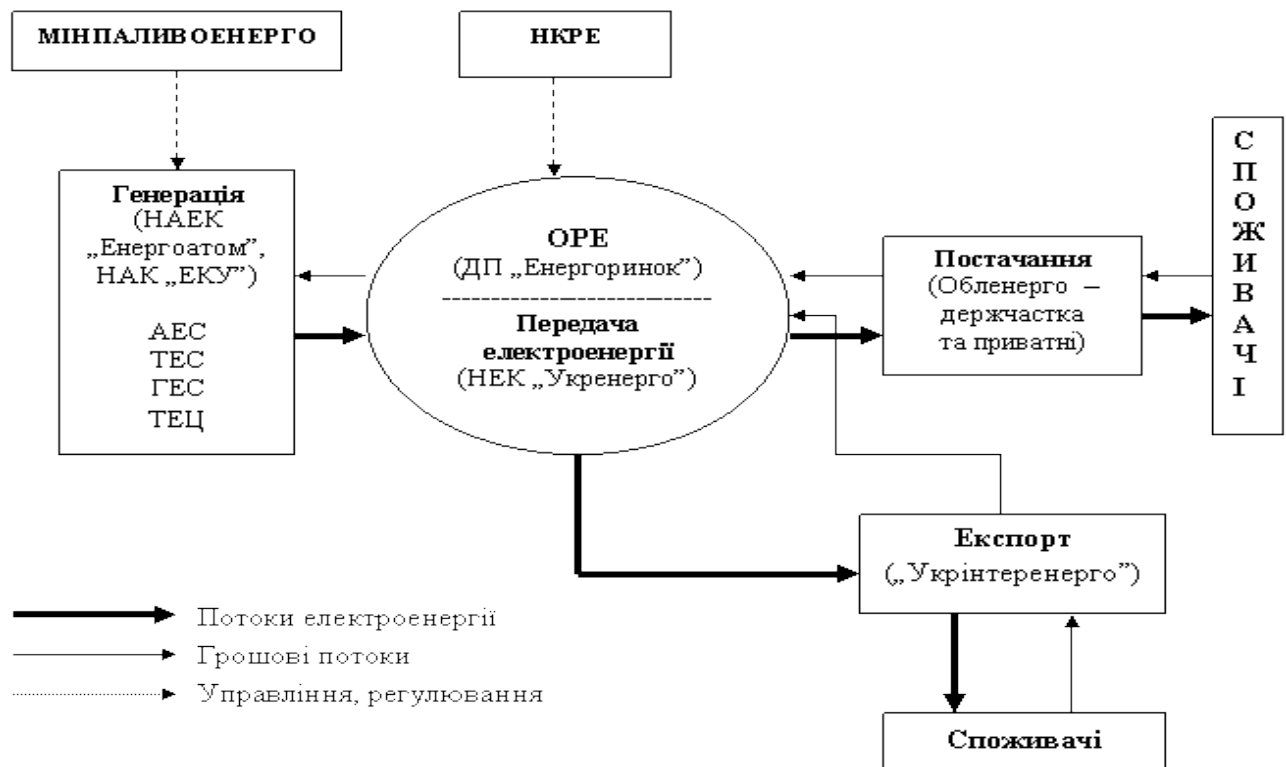


Рис.2.1. Принципова схема діючого ринку електроенергії України

Джерело: [41]

Існує необхідність переходу від моделі єдиного покупця до більш ефективної та орієнтованої на споживача моделі ринку електроенергії. У 2002 році Кабінет Міністрів України прийняв Концепцію функціонування та розвитку оптового ринку електричної енергії України ("Концепція"). Концепція передбачає поступовий перехід до повноцінного конкурентного ринку електроенергії, що складається з двостороннього контрактного ринку,

балансуючого ринку для забезпечення попиту та пропозиції позаконтрактних обсягів електроенергії та ринку допоміжних послуг.

У 2004 році була створена міжвідомча комісія для координації роботи з реалізації концепції. У 2005 році було прийнято план заходів з реалізації другого етапу концепції (2006-2008 роки) та зміни до Закону України "Про електроенергетику" (№ 2362-IV), прийняття Закону України від 23 червня 2005 року № 2711 "Про заходи, спрямовані на забезпечення сталого функціонування підприємств паливно-енергетичного комплексу" призвело до внесення змін до Правил ОРЕ з метою сприяння розвитку конкуренції на ринку, що дало поштовх до покращення фінансового стану галузі та дозволило вжити низку заходів щодо запобігання банкрутству. Прийняття Закону № 2711 "Про заходи, спрямовані на забезпечення сталого функціонування підприємств паливно-енергетичного комплексу" дало поштовх до покращення фінансового стану галузі та дозволило здійснити низку заходів щодо запобігання банкрутствам.

Таким чином, у 2004-2007 роках основні інституційні та економічні умови для поступового запровадження системи двосторонніх договорів купівлі-продажу електроенергії були значною мірою виконані. Однак залишаються проблеми, які можуть бути вирішені за умови подальшої організаційної, ресурсної та законодавчої підтримки реалізації концепції.

Слід зазначити, що у 2004 році внутрішній ринок електроенергії відхилився від шляху лібералізації зі створенням Енергетичної компанії України (ЕКУ), державної монополії, яка централізувала активи українських компаній з виробництва та розподілу електроенергії.

В результаті була створена вертикально інтегрована структура, яка монополізувала різні та взаємозалежні види діяльності в енергетичному секторі, що призвело до значного дисбалансу в структурі ринку.

На сьогоднішній день НЕК "ЕКУ" володіє контрольними пакетами акцій 10 енергогенеруючих компаній, що становить 45% загальної встановленої потужності ОЕС України, а також державними акціями

(контрольними або блокпакетами) 21 з 27 обленерго, які закупають близько 70% електроенергії в ОРЕ.

Розвитку конкурентного середовища на ринку електроенергії України та переходу до нової бізнес-моделі перешкоджають системні проблеми, серед яких:

- надмірне зношення обладнання та об'єктів енергетичної інфраструктури, необхідність технічної та технологічної модернізації відповідно до сучасних стандартів (ефективність, енергоспоживання, екологічна безпека) та брак коштів на ці цілі;
- відсутність конкуренції на ринку первинних енергоносіїв (природного газу та вугілля);
- нереалізований експортний потенціал електроенергетичного сектору (переважно через слабку інтеграцію з об'єднаною енергетичною системою ЄС);
- борги та кредити учасників енергетичного ринку (станом на початок квітня 2018 року заборгованість ДП "Енергоринок" перед енергогенеруючими компаніями та енергопостачальниками перед компаніями-операторами ОРЕ становила 15 млрд. грн. та 14,96 млрд. грн. відповідно).

ПрАТ "Кіровоградобленерго" здійснює діяльність з передачі електроенергії місцевими (локальними) електромережами та з постачання електричної енергії по регульованому тарифу. Це сучасне, потужне та прибуткове підприємство.

Постачання електричної енергії – це господарська діяльність, пов'язана з транспортуванням електричної енергії за допомогою електричних мереж на підставі договору.

Основні види діяльності ПрАТ "Кіровоградобленерго":

- розподілення та постачання електроенергії;
- будівництво будівель;
- діяльність в сфері інжинірингу;
- професійно-технічна освіта;

- виробництво електроенергії;
- інші види оптової торгівлі.

ПрАТ "Кіровоградобленерго" має усі необхідні ліцензії на здійснення обраної діяльності. Інформація про одержані ліцензії (дозволи) на окремі види діяльності зображена в Табл.2.1.

Таблиця 2.1

Інформація про одержані ліцензії на окремі види діяльності

Вид діяльності	Номер ліцензії	Дата видачі	Державний орган, що видав	Дата Закінчення дії ліцензії
1	2	3	4	5
Передача електричної енергії місцевими електричними мережами	АБ № 177350	28.09.2005	Національна комісія регулювання електроенергетики України	Термін дії ліцензії не обмежений
Опис	Термін дії ліцензії не обмежений			
Постачання електричної енергії за регульованим тарифом	АБ № 220501	28.09.2005	Національна комісія регулювання електроенергетики України	Термін дії ліцензії не обмежений
Опис	Термін дії ліцензії не обмежений			
Виробництво електричної енергії	АБ № 177349	28.09.2005	Національна комісія регулювання електроенергетики України	Термін дії ліцензії не обмежений
Опис	Термін дії ліцензії не обмежений			
Будівельна діяльність	АБ № 220449	11.09.2006	Кіровоградська обласна державна адміністрація	11.09.2011р.
Опис	Сфера виробничої діяльності суб'єкта господарювання: 2.00.00 Проектні роботи (для нового будівництва, реконструкції та капітального ремонту) (для звичайних умов); 3.00.00 Зведення несучих та огорожуючих конструкцій будівель і споруд, будівництво та монтаж інженерних та транспортних мереж (для нового будівництва, реконструкції та капітального ремонту, для звичайних умов). Товариство планує продовжувати дію даної ліцензії.			
Надання освітніх послуг навчальними закладами, пов'язаних з одержанням професійної освіти на рівні кваліфікованих вимог до професійно-технічного навчання, підвищення кваліфікації, перепідготовки	АБ № 363940	14.12.2007	Міністерство освіти і науки України	27.11.2012р.
Опис	Товариство планує продовжувати дії даної ліцензії			

Джерело: [41]

Організаційна структура ПрАТ "Кіровоградобленерго" наведена на рис. 2.2.



Рис. 2.2. Організаційна структура ПрАТ "Кіровоградобленерго"

Джерело: [розроблено на основі опрацювання додатку А]

Вищим органом товариства є загальні збори акціонерів, які скликаються щорічно. Створено Наглядову раду з метою захисту інтересів акціонерів і здійснення контролю за діяльністю управління ПрАТ. Правління ПрАТ являється виконавчим органом товариства, яке здійснює керівництво поточною діяльністю товариства, направленою на

отримання прибутку. Ревізійна комісія проводить перевірку фінансової та господарської діяльності товариства, як з власної ініціативи, так і за дорученням вищого органу, Наглядової ради або акціонерів, що володіють більше 10% акцій.

До складу компанії входять 4 малих ГЕС з установленою потужністю гідроагрегатів 12,25 МВт:

- * Гайворонська ГЕС - 5,7 МВт;
- * Краснохутірська ГЕС - 3,3 МВт;
- * Тернівська ГЕС - 1,95 МВт;
- * Новоархангельська ГЕС - 1,3 МВт.

До складу ПрАТ "Кіровоградобленерго" входить 4 райони електромереж – відособлених підрозділів, які не є юридичними особами/

ПрАТ "Кіровоградобленерго" не має конкурентів по послугам постачання електричної енергії. ПрАТ "Кіровоградобленерго" є єдиним постачальником за регульованим державою тарифом на території Кіровоградської області, що має Ліцензію на постачання електричної енергії за регульованим тарифом виданою НКРЕ України №500310. Тобто, ПрАТ "Кіровоградобленерго" є природний монополіст на території Кіровоградської області з передачі та постачання електроенергії споживачам за врегульованими тарифами.

Функції регулювання та сприяння розвитку конкуренції в галузі, та організації ефективного ринку електричної енергії виконує Національна комісія регулювання електроенергетики України (НКРЕ), основними завданнями якої є:

- участь у формуванні та забезпеченні реалізації єдиної державної політики щодо розвитку і функціонування оптового ринку електроенергії, ринків газу, нафти та нафтопродуктів;
- державне регулювання діяльності суб'єктів природних монополій в електроенергетиці, нафтогазовому комплексі, у сфері теплопостачання, якщо теплова енергія виробляється на теплоелектроцентралях,

когенераційних установках та установках з використанням нетрадиційних або поновлюваних джерел енергії;

- сприяння конкуренції у сфері виробництва електричної енергії, постачання електричної енергії та газу, видобутку газу та нафти, зберігання та реалізації газу, нафти і нафтопродуктів та у сфері теплопостачання, якщо теплова енергія виробляється на теплоелектроцентралях, когенераційних установках та установках з використанням нетрадиційних або поновлюваних джерел енергії;

- забезпечення проведення цінової і тарифної політики в електроенергетиці, нафтогазовому комплексі та встановлення тарифів на електричну та теплову енергію, що виробляється на теплоелектроцентралях, ТЕС, АЕС та когенераційних установках і установках з використанням нетрадиційних або поновлюваних джерел енергії;

- забезпечення ефективності функціонування товарних ринків на основі збалансування інтересів суспільства, суб'єктів природних монополій та споживачів їх товарів і послуг;

- захист прав споживачів електричної і теплової енергії, газу, нафти та нафтопродуктів;

- розроблення і затвердження правил користування електричною енергією та газом;

- координація діяльності державних органів у питаннях регулювання ринків енергоносіїв;

- видача суб'єктам підприємницької діяльності ліцензій на виробництво електричної енергії в обсягах, що перевищують рівень, який встановлюється умовами та правилами здійснення підприємницької діяльності з виробництва електричної енергії (ліцензійними умовами), передачу та постачання електричної енергії, зберігання природного газу в обсягах, що перевищують рівень, який встановлюється умовами та правилами здійснення підприємницької діяльності зі зберігання природного газу (ліцензійними умовами), і постачання природного газу, транспортування нафти та

нафтопродуктів магістральними трубопроводами, транспортування природного і нафтового газу трубопроводами;

- ліцензування певних видів господарської діяльності у сфері теплопостачання, якщо теплова енергія виробляється на теплоелектроцентралях, когенераційних установках та установках з використанням нетрадиційних або поновлюваних джерел енергії;

- видача ліцензій на електричну та теплову енергію, що виробляються когенераційними установками.

- контроль за додержанням ліцензіатами умов здійснення ліцензованої діяльності.

Основним постачальником електричної енергії для проведення ліцензованої діяльності ПрАТ "Кіровоградобленерго" є ДП "Енергоринок"- 98,2 % від загальної величини покупної електроенергії. ДП "Енергоринок" знаходиться за адресою: м. Київ, вул. Симона Петлюри, 27. Порівняно з 2020 роком ціна за куповану електроенергію у 2021 році збільшилася на 21%.

Основа успішної діяльності ДП "Енергоринок" - високий професіоналізм фахівців підприємства, вивчення та впровадження світового досвіду, сумлінне та творче ставлення до виконання покладених обов'язків та поставлених завдань, поважне ставлення до партнерів. Високий рівень корпоративної культури та позитивний імідж створюють умови для успішної співпраці ДП "Енергоринок" з партнерами. Діловими партнерами підприємства є понад 600 членів ОРЕ, закордонні енергетичні компанії та інші.

Імпортні матеріали (сировина) комплектуючі та товари не використовуються.

Основні споживачі ПрАТ "Кіровоградобленерго" є юридичні та фізичні особи Кіровоградської області. Структура споживачів ПрАТ "Кіровоградобленерго" помірно диверсифікована, найбільшою категорією споживачів за обсягом споживання у натуральному вимірі залишається населення – 46% від поставленої в 2011 році електроенергії. При цьому у структурі доходу від реалізації електроенергії надходження від населення

становлять лише 22,4% , що пов'язано з нижчими тарифами для населення, порівняно з іншими споживачами.

Питома вага 10 найбільших абонентів у структурі поставленої у 2021 році електроенергії склала 23,2% у грошовому вимірі.

Найбільший споживач, через якого було отримано 7% доходу – Східний ГЗК. Йому було відпущено електричної енергії 156 млн. 563 тис. кВт/год на суму 87 млн.739 тис. грн., сплачено – 87 млн. 460 тис. грн.

Також ПрАТ "Кіровоградобленерго" укладено та діяли у 2021 році 2 договори на постачання електричної енергії : договір № 11 від 01.09.2020 р. та договір № 15 від 28.10.2020 р.

Концентрація постачання електроенергії за окремими споживачами незначна. ПрАТ "Кіровоградобленерго" уклало договір про спільну діяльність № 580 від 24.06.20 р. з ПрАТ "ЕК "Житомиробленерго", ПрАТ "ЕК "Херсонобленерго", ПрАТ "ЕК "Одесаобленерго".

Спільна діяльність Сторін провадиться з метою реалізації проекту щодо впровадження корпоративної автоматизованої системи управління підприємством та груп підприємств на платформі MSАхapta або її аналогу з можливістю консолідації необхідних даних, впровадження корпоративного центру обробки даних та методологічного центру.

Згідно з п.5 Договору про спільну діяльність № 580 від 24.06.21р. придбано 6 ліцензій програмного забезпечення автоматизованої системи управління MicrosoftDynamicsAX на суму 243 787,40 грн.

Кінцевим результатом спільної діяльності є впровадження корпоративної автоматизованої системи управління підприємством та груп підприємств на платформі MSАхapta або її аналогу з можливістю консолідації необхідних даних, що включає інтерфейси взаємодії з існуючими ERP-системами, корпоративний центр обробки даних та методологічний центр.

ПрАТ "Кіровоградобленерго" користується послугами багатьох підприємств. Основні з них наведені у таблиці 2.2.

Таблиця 2.2

**Інформація про юридичних осіб, послугами яких
користується ПрАТ "Кіровоградобленерго"**

Повне найменування	Організаційно-правова форма	Вид діяльності	Назва держ. органу, що видав ліцензію або інш. документ на цей вид діяльності	Дата видачі ліцензії або інш. документа	Номер ліцензії або іншого документа
1	2	3	4	5	6
ПАТ "Всеукраїнський депозитарій цінних паперів"	Акціонерне товариство	Депозитарна діяльність депозитарія цінних паперів	Державна комісія з цінних паперів та фондового ринку	19.11.2009	АВ №498004
ТОВ "Енергетична реєстраційна компанія"	Товариство з обмеженою відповідальністю	Депозитарна діяльність зберігача цінних паперів	Державна комісія з цінних паперів та фондового ринку	16.08.2010	АГ №399074
ТОВ "Аудиторська компанія "Світ"	Товариство з обмеженою відповідальністю	Аудиторська діяльність	Аудиторська Палата України	22.06.2001	№ 2158
ПАТ "Страхова компанія "Провідна"	Приватне акціонерне товариство	Страхова діяльність	Державна комісія з регулювання ринків фінансових послуг	16.02.2010	АВ №520906
ПАТ "Фондова біржа ПФТС"	Приватне акціонерне товариство	Діяльність з організації торгівлі на фондовому ринку	Державна комісія з цінних паперів та фондового ринку	10.06.2011	АВ №581354
ПАТ "Київська міжнародна фондова біржа"	Приватне акціонерне товариство	Діяльність з організації торгівлі на фондовому ринку	Державна комісія з цінних паперів та фондового ринку	05.04.2011	АВ №581164
ПАТ "Перший інвестиційний банк"	Приватне акціонерне товариство	Депозитарна діяльність зберігача цінних паперів	Державна комісія з цінних паперів та фондового ринку	23.09.2011	АВ №579897

Джерело: [41]

Зона діяльності ПрАТ "Кіровоградобленерго" охоплює всю Кіровоградську область. За межі держави Товариство електроенергію не

експортує, це означає, що Товариство працює лише на внутрішньому ринку не виходячи на зовнішній, задовольняє потреби лише мешканців держави.

Основні тенденції розвитку ПрАТ "Кіровоградобленерго" такі: за результатами першого півріччя 2020 року продовжилася тенденція до зростання обсягів генерації та споживання електроенергії, однак до кінця року темпи росту сповільнилися.

Незважаючи на зростання, показники залишаються нижчими за докризові. Спостерігається подальша тенденція до зростання вартості електроенергії на всьому ланцюгу "генерація-споживання".

Подорожчання електроенергії негативно на рівні розрахунків, особливо між енергопостачальними компаніями та кінцевими споживачами, оскільки платоспроможність значної частини останніх залишається недостатньою.

Енергетична стратегія України до 2030 року стала важливим кроком внапрямку формування дієвої системи управління в паливно-енергетичному секторі, здатної працювати на вирішення завдань сьогодення.

Стратегія закладає концептуальні засади енергетичної безпеки держави, визначає головні цілі та завдання енергетичної політики, намічає основні напрямки та показники розвитку енергетики.

Мета Стратегії – сприяти реалізації в Україні енерго зберігаючи її моделі розвитку економіки. Енергетична стратегія є результатом доопрацювання робочою групою Мінпаливенерго проекту "Енергетичної стратегії України до 2030 року та дальшу перспективу" Інституту загальної енергетики Національної академії наук України.

2.2. Аналіз фінансово-економічної діяльності підприємства

Цей розділ кваліфікаційної роботи містить інформацію про основні зміни у фінансово-господарській діяльності підприємства за звітні роки, чинники, які спричинили такі зміни, із зазначенням рівня їх впливу на всю сукупність змін та коротке порівняння динаміки показників за звітні роки.

Таблиця 2.3

Основні фінансово-економічні показники діяльності підприємства, тис. грн.

Показники	Роки					Відносне відхилення, %
	2018	2019	2020	2021	2022	2022/2018
Доход від реалізації продукції	1364967	1658316	2232827	2735349	3056318	123,9
Податок на додану вартість 20%	227494	276386	372882	456803	509386	123,9
Чистий дохід від реалізації продукції	1137473	1381930	1859945	2278546	2546932	123,9
Собівартість реалізованої продукції	1078375	1291864	1760971	2136557	2519291	133,6
Валовий прибуток	59098	90066	98974	141989	27641	-53,2
Інші операц. доходи	0	0	0	0	10701	0,0
Адміністративні витрати	39672	40104	52501	56806	67899	71,2
Інші операц. витрати	102434	126053	54775	18509	0	-100,0
Прибуток (збиток) від операційної діяльності	-83008	-76091	-8302	66674	-29557	-64,4
Інші фінансові доходи	0	0	0	0	0	0,0
Інші доходи	0	983	6867	0	0	0,0
Фінансові витрати	38580	53359	64870	63610	56902	47,5
Інші витрати	1612	0	0	1798	264671	16318,8
Прибуток від звич. д-ті до оподаткування	-123473	-128725	-6632,6	1182	-351076	184,3
Податок на прибуток	11389	1112	11964	11690	60676	432,8
Чистий прибуток	-112084	-127613	-54362	12872	-290400	159,1

Джерело: [складено автором на основі додатків Б-Л]

Аналізуючи показники таблиці 2.3, можна сказати, що у 2019 році порівняно з 2018 роком дохід від реалізації продукції збільшився на 98984 грн., у 2020 році порівняно з 2019 збільшився на 293349 грн., у 2021 році порівняно з 2020 роком збільшився на 574511 грн., у 2022 році порівняно з 2021 роком збільшився на 502522 грн., а в 2022 році порівняно з 2018 роком цей показник збільшився на 1469366 грн. Загалом за 5 років дохід від реалізації продукції зріс більш ніж у 2 рази, темп зростання склав 216%.

У 2019 році порівняно з 2018 роком податок на додану вартість збільшився на 10266 грн., у 2020 році порівняно з 2019 роком збільшився на 30211 грн., у 2021 році порівняно з 2020 роком збільшився на 16497 грн., у 2022 році порівняно з 2021 роком збільшився на 48892 грн., а в 2022 році порівняно з 2018 роком цей показник збільшився на 105866 грн.

У 2019 році порівняно з 2018 роком чистий дохід від реалізації продукції збільшився на 51330 грн., у 2020 році порівняно з 2019 роком збільшився на 151056 грн., у 2021 році порівняно з 2020 роком збільшився на 82487 грн., у 2022 році порівняно з 2021 роком збільшився на 244457 грн., а в 2022 році порівняно з 2018 роком цей показник збільшився на 529330 грн.

У 2019 році порівняно з 2018 роком собівартість реалізованої продукції збільшилась на 150943 грн., у 2020 році порівняно з 2019 роком збільшилась на 103017 грн., у 2021 році порівняно з 2020 роком збільшився на 105697 грн., у 2022 році порівняно з 2021 роком збільшився на 213489 грн., а в 2022 році порівняно з 2018 роком цей показник збільшився на 573146 грн.

У 2019 році порівняно з 2018 роком валовий прибуток зменшився на 99613 грн., у 2020 році порівняно з 2019 збільшився на 48039 грн., у 2021 році порівняно з 2020 роком зменшився на 23210 грн., у 2022 році порівняно з 2021 роком збільшився на 30968 грн., а в 2022 році порівняно з 2018 роком цей показник зменшився на 43816 грн.

У 2019 році порівняно з 2018 роком інші операційні доходи зменшились на 58032 грн., у 2020 році порівняно з 2019 роком зменшились на 73996 грн., у 2021 і 2022 роках інші операційні доходи склали 0 грн.

У 2019 році порівняно з 2018 роком адміністративні витрати збільшились на 4444 грн., у 2020 році порівняно з 2019 роком збільшились на 2953 грн., у 2021 році порівняно з 2020 роком збільшились на 4713 грн., у 2022 році порівняно з 2021 роком збільшились на 432 грн., а в 2022 році порівняно з 2018 роком цей показник збільшився на 12542 грн.

У 2019 році порівняно з 2018 роком інші операційні витрати зменшились на 84580 грн., у 2020 році порівняно з 2019 роком зменшились на 20205 грн., у 2021 році порівняно з 2020 роком збільшились на 102434 грн., у 2022 році порівняно з 2021 роком збільшились на 23619 грн., а в 2022 році порівняно з 2018 роком цей показник збільшився на 21268 грн.

У 2019 році порівняно з 2018 роком прибуток від операційної діяльності зменшився на 77509 грн., у 2020 році порівняно з 2019 роком зменшився на 8705 грн., у 2021 році порівняно з 2020 роком підприємство мало збиток від операційної діяльності у розмірі 83008 грн. Така тенденція збереглась і у 2022 році.

У 2019 році порівняно з 2018 роком інші фінансові доходи збільшились зменшились на 15089 грн., у 2020 році порівняно з 2019 роком зменшилися на 769 грн., у 2022, 2021 і у 2020 роках цей показник склав 0 грн., а в 2022 році порівняно з 2018 роком цей показник зменшився на 15858 грн.

У 2019 році порівняно з 2018 роком фінансові витрати збільшились на 30624 грн., у 2020 році порівняно з 2019 роком зменшилися на 21091 грн., у 2021 році порівняно з 2020 роком зменшилися на 5243 грн., у 2022 році порівняно з 2021 роком збільшились на 14779 грн., а в 2022 році порівняно з 2018 роком цей показник збільшився на 19069 грн.

У 2019 році порівняно з 2018 роком інші витрати зменшилися на 318218 грн., у 2020 році порівняно з 2019 роком зменшилися на 10159 грн., у 2021 році порівняно з 2020 роком зменшилися на 4683 грн., у 2022 році цей показник склав 0 грн., а в 2022 році порівняно з 2018 роком цей показник зменшився на 334672 грн.

У 2019 році порівняно з 2018 роком прибуток від звичайної діяльності

до оподаткування зменшився на 118764грн., у 2020 році порівняно з 2019 роком збільшився на 3682 грн., а у 2021 і 2022 роках прибуток змінився на збиток -123473 грн. і -128725 грн. відповідно.

У 2019 році порівняно з 2018 роком чистий прибуток зменшився на 95803грн., у 2020 році порівняно з 2019 роком збільшився на 12289 грн., у 2021 році порівняно з 2020 роком прибуток змінився на збиток -127373 грн., у 2022 році збиток склав -127613 грн., а в 2022 році порівняно з 2018 роком цей показник зменшився на 226416 грн.

Таблиця 2.4

Показники ліквідності ПрАТ "Кіровоградобленерго"

Показник	2018	2019	2020	2021	2022
Коефіцієнт абсолютної ліквідності	0,11	0,63	0,53	0,32	0,29
Коефіцієнт поточної ліквідності	0,37	0,97	0,71	0,44	0,39
Проміжний коефіцієнт покриття	0,00002	0,00002	0,64	0,41	0,37

Джерело: [складено автором на основі розрахунків даних додатків Б-Л]

Аналізуючи показники таблиці 2.4, можна сказати, що у 2019 році порівняно з 2018 роком коефіцієнт абсолютної ліквідності збільшився на 0,52, у 2020 році порівняно з 2019 роком зменшився на 0,1, у 2021 році порівняно з 2020 роком зменшився на 0,21, у 2022 році порівняно з 2021 роком зменшився на 0,03, а в 2022 порівняно з 2018 роком цей показник збільшився на 0,18.

У 2019 році порівняно з 2018 роком коефіцієнт поточної ліквідності збільшився на 0,60, у 2020 році порівняно з 2019 роком зменшився на 0,2, у 2021 році порівняно з 2020 роком зменшився на 0,27, у 2022 році порівняно з 2021 роком зменшився на 0,05 а в 2022 порівняно з 2018 роком цей показник збільшився на 0,02.

У 2019 році порівняно з 2018 роком проміжний коефіцієнт покриття не

змінився, у 2020 році він дорівнював 0,64, у 2021 році - 0,41, у 2022 році -0,37, а в 2022 році порівняно з 2018 роком цей показник збільшився на 0,36.

Таблиця 2.5

Показники стану та структури капіталу ПрАТ "Кіровоградобленерго"

Показники	2018	2019	2020	2021	2022
Коефіцієнт забезпеченості власними коштами	3,83	1,11	-1,45	-1,72	-1,83
Коефіцієнт фінансової автономії (стабільності)	0,49	0,66	0,61	0,53	0,44
Коефіцієнт заборгованості	0,33	0,51	0,39	0,47	0,55
Коефіцієнт фінансового лівериджу	0,97	1,95	1,53	1,13	0,79
Коефіцієнт співвідношення кредиторської та дебіторської заборгованості	0	1,7	8,9	6,3	6,5

Джерело: [складено автором на основі розрахунків даних додатків Б-Л]

Аналізуючи показники таблиці 2.5, можна сказати, що у 2019 році порівняно з 2018 роком коефіцієнт забезпечення власними коштами зменшився на 2,72, у 2020 році коефіцієнт набув від'ємного значення, у 2021 і у 2022 роках ця тенденція зберігається. З отриманих даних можна зробити висновок, що при будь-яких фінансових проблемах підприємство може опинитися на межі дефолту.

У 2019 році порівняно з 2018 роком коефіцієнт фінансової автономії збільшився на 0,17, у 2020 році порівняно з 2019 роком зменшився 0,05, у 2021 році порівняно з 2020 роком зменшився на 0,08, у 2022 році порівняно з 2021 роком зменшився на 0,09, а в 2022 році порівняно з 2018 роком цей показник зменшився на 0,05.

У 2019 році порівняно з 2018 роком проміжний коефіцієнт заборгованості збільшився на 0,18, у 2020 році порівняно з 2019 роком зменшився 0,12, у 2021 році порівняно з 2020 роком збільшився на 0,08, у 2022 році порівняно з 2021 роком збільшився на 0,08, а в 2022 році порівняно з 2018 роком цей показник збільшився на 0,22.

У 2019 році порівняно з 2018 роком коефіцієнт фінансового левериджу збільшився 0,98, у 2020 році порівняно з 2019 роком зменшився 0,42, у 2021 році порівняно з 2020 роком зменшився на 0,40, у 2022 році порівняно з 2021 роком зменшився на 0,34, а в 2022 порівняно з 2018 роком цей показник зменшився на 0,18.

Таблиця 2.6

Показники оборотності (ділової активності) ПрАТ "Кіровоградобленерго"

Показник	2018	2019	2020	2021	2022
Оборотність обігових коштів	8,3	3,5	4,1	4,3	4,7
Оборотність товарно-матеріальних запасів	20,4	26,2	31,9	25,2	28,9
Оборотність дебіторської заборгованості	30,1	21,7	21,6	23,0	22,7
Оборотність кредиторської заборгованості	2,2	4,2	3,3	2,9	3,3

Джерело: [складено автором на основі розрахунків даних додатків Б-Л]

Аналізуючи таблицю 2.6 ми бачимо, що оборотність обігових коштів - визначає співвідношення між обсягом реалізованої продукції (Р) та розміром (середнім залишком) (Со) оборотних коштів підприємства за певний період (Д). Найбільшою оборотність обігових коштів була у 2018 році і складала 8,3 рази на рік, а вже наступного 2019 р. вона мала найменше значення за аналітичний період і складала лише 3,5.

Оборотність товарно-матеріальних запасів показує, скільки разів в середньому продаються запаси підприємства за певний період часу. У 2020

році була вона найбільшою, а якщо порівнювати 2018 та 2022 роки, то бачимо зростання на 8,5.

Оборотність дебіторської заборгованості показує скільки разів у середньому протягом року дебіторська заборгованість перетворювалась у грошові кошти. Щодо цього показника, то у 2018 році він становив - 30,1; 2019 році - 21,7; у 2020 році - 21,6, у 2021 році - 23,0, у 2022 році - 22,7.

Оборотність кредиторської заборгованості показує скільки потрібно оборотів для оплати виставлених рахунків. На підприємстві «Кіровоградобленерго» оборотність кредиторської заборгованості з 2018 року по 2022 рік збільшилась на 1,1. Це означає, що в 2022 році підприємство повинно швидше виплатити кредиторську заборгованість ніж це було зроблено у 2018 році.

Таблиця 2.7

Показники прибутковості (рентабельності) ПрАТ "Кіровоградобленерго"

Показник	2018 рік	2019 рік	2020 рік	2021 рік	2022 рік
Чиста рентабельність (збитковість) власного капіталу	0,27	0,03	0,01	-0,12	-0,16
Звичайна рентабельність власн. капіталу до оподаткування	0,32	0,009	0,003	-0,13	-0,17
Рентабельність активів (РА)	0,09	0,002	0,009	-0,07	-0,08
Рентабельність обороту (продаж)	0,08	-0,06	0,003	-0,02	-0,002
Рентабельність операційних витрат (РОВ)	1,04	1,15	1,48	-0,58	-0,45

Джерело: [складено автором на основі розрахунків даних додатків Б-ЛІ]

Аналізуючи таблицю 2.7 ми бачимо, що чиста рентабельність власного капіталу - фінансовий коефіцієнт, що характеризує ефективність використання власного капіталу. Показує, яка віддача (норма прибутку) на вкладений власний капітал. Максимізація цього показника – головне завдання

управління підприємством. За період з 2018 року по 2022 рік показник рентабельності власного капіталу змінювався, у 2018 році він становив 0,27, а вже у 2022 році набув від'ємного значення - 0,16, що не може не викликати занепокоєння.

Звичайна рентабельність власного капіталу до оподаткування зростала, а потім знизилася аж до від'ємного значення у 2022 році (-0,17).

Рентабельність активів - фінансовий коефіцієнт, що характеризує ефективність використання всіх активів підприємства. За період з 2018 року по 2022 рік показник рентабельності активів зменшився на 0,17.

Таблиця 2.8

Факторний аналіз валового прибутку (збитку)

Роки	Чистий дохід (виручка) від реалізації продукції (товарів, робіт, послуг), тис. грн.		Собівартість реалізованої продукції (товарів, робіт, послуг), тис. грн.		Валовий прибуток (збиток), тис. грн.		Зростання (зменшення) валового прибутку, тис. грн.		
	За попередній період	за звітний період	за попередній період	за звітний період	за попередній період	за звітний період	Всього	За рахунок зростання (зменшення) чистого доходу, тис. грн.	За рахунок зростання (зменшення) собівартості реалізованої продукції, тис. грн.
1	2	3	4	5	6	7	8	9	10
2018	703 217	852 600	594 527	718 718	108 690	133 882	25 192	149 383	-124 191
2019	856 339	903 930	776 479	869 661	79 860	34 269	-45 591	47 591	-93 182
2020	903 930	1054986	869 661	972 678	34 269	82308	48039	151056	-103017
2021	1054986	1137473	972 678	1078375	82308	59098	-23210	82487	-105697
2022	1137473	1381930	1078375	1291864	59098	90066	30968	244457	-213489

Джерело: [складено автором]

Рентабельність обороту являє собою відношення прибутку від реалізації, чистого або балансового прибутку до отриманої виручки.

Рентабельність обороту показує, скільки прибутку отримує підприємство з однієї гривні виручки. У 2018 році цей показник становив - 0,08, у 2019 році - (-0,06), у 2020 - 0,003, у 2021 році - (-0,02), у 2022 році - (-0,002).

Рентабельність операційних витрат з кожним роком зростала з 1,04 у 2018 році до 1,48 у 2020 році, а вже у 2021 році набула від'ємного значення (-0,58) і така тенденція збереглась і у 2022 році (-0,45).

Як бачимо жоден з розглянутих показників рентабельності не досяг позитивного значення.

Досліджуючи показники таблиці 2.8 можна дійти висновку, що чистий дохід від реалізації продукції (робіт, послуг) у звітних періодах з 2018 по 2022 роки збільшився, що призвело до зростання валового прибутку у 2018 році на 149381 тис. грн., у 2019 році на 47591 тис. грн., у 2020 році на 151056 тис. грн., у 2021 році на 82487 тис. грн., у 2022 році на 244457 тис. грн.

Собівартість реалізованої продукції (робіт, послуг) також збільшувалась у звітних періодах цих років і призвела до зменшення валового прибутку у 2018 році на 124191 тис. грн., у 2019 році на 93182 тис. грн., у 2020 році на 103017 тис. грн., у 2021 році на 105697 тис. грн., у 2022 році на 213489 тис. грн.

Як ми вже зазначали, показники валового прибутку протягом аналітичного періоду динамічно змінювались і найбільшого свого зростання дістали за рахунок зменшення собівартості у 2022 році.

2.3. Характеристика інформаційних ресурсів та системи інформаційного забезпечення процесу управління на ПрАТ "Кіровоградобленерго"

Подальший розвиток компанії "Кіровоградобленерго" залежить від створення ефективної системи управління внутрішнім середовищем компанії. Створення інтегрованої та динамічної інформаційної системи є актуальним завданням для компаній, які прагнуть подальшого розвитку. На жаль, існуючі

інформаційні системи в компаніях мають скоріше фрагментарний, ніж системний характер і не забезпечують достатньої повноти та оперативності збору, обробки та розподілу необхідної інформації до відповідних підрозділів. Щодо останнього, то існує необхідність розробки та впровадження проектів з автоматизації процесу інформаційного забезпечення на підприємствах.

Автоматизовані управлінські інформаційні системи призначені для надання інформації про відхилення від запланованих показників на основі оперативної обробки інформації.

Найбільш ефективне використання комп'ютерів залежить від наступних умов: створення самого комп'ютера, створення програмного забезпечення для комп'ютера і підготовка прикладного середовища.

Використання електронної техніки забезпечує економію адміністративних і накладних витрат, значне підвищення ефективності проектно-конструкторських робіт і забезпечення ефективного прийняття рішень.

Використання інформаційних технологій (ІТ) є одним з найбільш суперечливих питань. Керівництво компанії часто відмовляється вирішувати це питання, оскільки не відчуває себе достатньо компетентним. Проблема часто покладається на ІТ-менеджера або зовнішню спеціалізовану організацію; бізнес-ризики, пов'язані з ІТ, постійно зростають, і незрозуміло, як довго керівництво компанії може сприймати цей важливий стратегічний ресурс як належне. Це правда, що останнім часом топ-менеджмент став більш пильним щодо ІТ. Саме від нього мають виходити рішучі ініціативи щодо зміни ситуації в цій сфері.

Сьогодні ситуація в цій сфері вкрай невизначена.

Насамперед, постійно зростаючий обсяг закупівель технологій, що вимагають великих інвестицій, і, як наслідок, зростаюча залежність від зовнішніх послуг: внутрішні асигнування на потреби ІТ зростають швидше, ніж інші бізнес-витрати; сума витрат на ІТ зростає швидше, ніж інші бізнес-витрати; сума витрат на ІТ зростає швидше, ніж інші бізнес-витрати. В той же

час, топ-менеджмент не має повної інформації про загальні витрати на ІТ. Як наслідок, правильне судження керівництва компанії охоплює лише близько 5 відсотків відповідних витрат.

По-друге, змінюється роль ІТ в бізнес-діяльності багатьох компаній: ІТ-функція більше не є допоміжною функцією у виконанні внутрішніх процесів, а стала невід'ємною частиною продукту та виробничих потужностей. Бізнес-ризики тепер багато в чому визначаються ризиками в цій сфері.

Визначаючи місію інформаційної системи для обслуговування процесу управління, слід пам'ятати, що першими даними для роботи автоматизованої системи управління виробництвом є план виробництва і технічна інформація, що містить всі його елементи.

Звичайно, всю необхідну конструкторську, технічну та оглядову інформацію можна отримати в традиційному паперовому вигляді і ввести в систему управління виробництвом. Але, по-перше, обсяг такої інформації на будь-якому серйозному підприємстві дуже і дуже великий. Спроби вручну ввести цю інформацію у виробничу інформаційну систему часто призводять до затримок у введенні даних, що робить плани і програми безглуздими. По-друге, помилки, що виникають при ручному введенні даних або при перенесенні інформації з однієї автоматизованої системи в іншу, часто призводять до перебоїв у постачанні і виробництві, швидко зводячи нанівець переваги автоматизації. І, нарешті, процес ручного введення регулярного перетворення даних з однієї форми в іншу завжди пов'язаний зі значними накладними витратами, які можуть звести нанівець всі ефекти від впровадження автоматизованого контролю. Таких проблем можна уникнути, якщо не розривати інформаційний ланцюжок підготовки, планування та управління виробництвом.

При комплексному підході до автоматизації конструктори, інженери, працівники планово-диспетчерських служб і самі виробничники повинні працювати в єдиному інформаційному просторі. Дані, що вводяться

конструкторами і технічними фахівцями, які використовують САПР для проектування і документації, повинні бути доступні в структурованому електронному форматі для всіх, хто бере участь в процесі підготовки виробництва і управління ним. Тільки тоді не потрібно буде нічого вводити або переносити при формуванні планів, завдань та інформації. Це пов'язано з тим, що база знань для вирішення більшості завдань планування і виробництва вже створена на етапі проектування і технічної підготовки, і до неї потрібно лише отримати доступ. Робота такої організованої системи може бути спрощена у вигляді блок-схем, що показують потік інформації.

Подальший розвиток Кіровоградобленерго залежить від створення ефективної системи управління внутрішнім середовищем. Створення інтегрованої та динамічної інформаційної системи є актуальним завданням для компаній, які хочуть розвиватися далі. На жаль, існуючі інформаційні системи на підприємствах є скоріше фрагментарними, ніж системними, і не забезпечують достатньої цілісності та оперативності у зборі, обробці та розподілі необхідної інформації до відповідних підрозділів. Щодо останнього, то необхідно розробляти та впроваджувати проекти з автоматизації процесу інформаційного забезпечення на підприємствах.

Автоматизовані інформаційні системи управління покликані надавати інформацію про відхилення від запланованих показників на основі швидкої обробки інформації.

Найбільш ефективне використання комп'ютерів залежить від таких умов: створення самого комп'ютера, створення комп'ютерного програмного забезпечення та підготовки прикладного середовища.

Використання електронної техніки економить адміністративні та накладні витрати, значно підвищує ефективність проектно-конструкторських робіт і забезпечує ефективне прийняття рішень.

Використання інформаційних технологій (ІТ) є одним з найбільш суперечливих питань. Керівництво компаній часто відмовляється вирішувати це питання, оскільки не відчуває себе достатньо компетентним.

Оскільки бізнес-ризик, пов'язаний з ІТ, постійно зростає, і незрозуміло, як довго керівництво компанії може сприймати цей важливий стратегічний ресурс як належне, це питання часто залишають на розсуд ІТ-менеджерів або зовнішніх професійних організацій. Це правда, що в останні роки топ-менеджмент стає все більш обережним у ставленні до ІТ. Вирішальна ініціатива щодо зміни ситуації в цій сфері має виходити саме від них. Сьогодні ситуація в цьому секторі вкрай невизначена.

По-перше, продовжує зростати обсяг закупівель технологій, які потребують значних інвестицій, що призводить до посилення залежності від зовнішніх послуг; внутрішні асигнування на ІТ-потреби зростають швидше, ніж інші операційні витрати; сума витрат на ІТ зростає швидше, ніж інші операційні витрати. При цьому топ-менеджмент не має повної інформації про загальні витрати на ІТ. Як наслідок, правильні рішення, прийняті керівництвом компанії, покривають лише близько 5 відсотків відповідних витрат.

По-друге, змінюється роль ІТ в бізнес-діяльності багатьох компаній: ІТ-функція більше не є функцією підтримки внутрішніх процесів, а невід'ємною частиною продукту та виробничих потужностей. Бізнес-ризик тепер значною мірою визначаються ризиками в цій сфері.

Визначаючи місію інформаційної системи підтримки процесів управління, слід пам'ятати, що першими даними для роботи автоматизованої системи управління виробництвом є виробничий план і технічна інформація, що містить всі його елементи.

Звичайно, всю необхідну конструкторську, технічну та інспекційну інформацію можна отримати в традиційному паперовому вигляді і ввести в систему управління виробництвом. Але, по-перше, обсяг такої інформації на будь-якому серйозному підприємстві дуже і дуже великий. Спроби ручного введення такої інформації у виробничу інформаційну систему часто призводять до затримок у введенні даних, що робить плани і програми безглуздими. По-друге, помилки, що виникають під час ручного введення

даних або при перенесенні інформації з однієї автоматизованої системи в іншу, часто призводять до перебоїв у постачанні та виробництві, швидко зводячи нанівець переваги автоматизації. Нарешті, ручні процеси, які регулярно перетворюють дані з однієї форми в іншу, завжди пов'язані зі значними накладними витратами, які можуть звести нанівець переваги автоматизованого контролю. Цих проблем можна уникнути, якщо не розривати інформаційний ланцюжок підготовки, планування та контролю виробництва. При комплексному підході до автоматизації конструктори, інженери, планово-диспетчерський персонал і самі виробничники повинні працювати в єдиному інформаційному просторі. Дані, що вводяться конструкторами і технічними фахівцями, які використовують САПР для проектування і документації, повинні бути доступні в структурованому електронному форматі для всіх, хто бере участь в підготовці та управлінні виробництвом. Тільки тоді не потрібно буде нічого вводити або переносити при створенні планів, завдань та інформації. Це пов'язано з тим, що база знань для вирішення більшості завдань планування і виробництва вже створена на етапі проектування і технічної підготовки, і до неї потрібно лише отримати доступ. Робота такої організованої системи може бути спрощена у вигляді блок-схем, що показують потік інформації.

Взаємовідносини, інформаційні та функціональні зв'язки між відділами I&CS та корпоративними службами.

Для реалізації промислового функціонування системи управління відділ взаємодіє з наступними підрозділами підприємства:

- техніко-економічне планування (ТЕП) - ПЕВ (планово-економічний відділ), бухгалтерія;
- оперативне управління основним виробництвом (ОУОП) - транспортне господарство, виробничо-конструкторські відділи, ВДО основного виробництва;
- управління логістикою - відділ логістики (відділ матеріально-технічного постачання);

- збут і маркетинг продукції та послуг - відділ збуту, ПЕВ, бухгалтерія;
- управління фінансами - бухгалтерія, ПЕВ, бухгалтерія;
- управління персоналом - відділ кадрів;
- контроль якості продукції – відділ контролю якості, приймально-контрольне бюро, відділ метрології, відділ стандартизації, конструкторський відділ, ТБ, інструментальний цех, відділ виробництва та збуту, виробничо-технічний відділ;
- управління транспортним, ремонтним, енергетичним та інструментальним обслуговуванням виробництва - транспортний цех, ВГМ, бухгалтерія, інструментальний цех.

Це управління взаємодіє з підрозділами підприємства за планом, затвердженим генеральним директором - графіки приймання, обробка інформації на комп'ютері, видача машинних програм структурним підрозділам.

Автоматизовані системи управління призначені для підвищення ефективності управління підприємством за рахунок використання обчислювальної техніки та економіко-математичних методів для вирішення планових, облікових та інших завдань виробничо-господарської діяльності підприємства.

Впровадження послуг інформаційної підтримки дає можливість:

- підвищення продуктивності праці на всіх ланках управлінського ланцюга;
- значне скорочення трудомісткості обробки інформації;
- оптимізацію виробничо-господарської діяльності підприємства.

Система МІС складається з 12 функціональних підсистем, що включають 90 існуючих завдань і 23 завдання на розробку.

Управління технологічною підготовкою виробництва включає:

- розрахунок кількості комплектуючих і складальних одиниць у виробі;
- формування норм витрат матеріалів за компонентами на одиницю продукції (для підприємств); розрахунок застосовності комплектуючих і складальних

одиниць у виробі (для підприємств, підрозділів);

- розрахунок зведених норм витрат матеріалів на виріб для централізованої кооперації;
- формування планів утилізації залишкових відходів;
- інформаційно-пошукові системи для виведення інформації за запитами на термінали для допомоги у виробництві технічного оснащення;
- розрахунок наявності та використання інструменту в інструментальній майстерні заводу.

Техніко-економічне планування включає:

- розрахунок річних, квартальних та місячних планів виробництва (оптові ціни та NPV) для підприємств;
- розрахунок виробничих планів у натуральному вираженні (по галузях, на рік і квартал);
- розрахунок виробничих планів у вартісному вираженні (по галузях, на рік і квартал);
- розрахунок нормативної трудомісткості виробничого плану (по галузях, річний та квартальний);
- розрахунок планової чисельності виробничих робітників на одиницю продукції (по галузях, на рік, поквартально);
- розрахунок планової чисельності виробничих робітників-відрядників (поквартально, на одиницю продукції в місяць);
- розрахунок планового фонду заробітної плати виробничих відрядників (на одиницю продукції, річний, квартальний);
- розрахунок загального фонду заробітної плати та трудомісткості одиниці продукції;
- облік змін нормативної собівартості продукції за прямими статтями витрат у розрізі цехів підприємства;
- аналіз зміни нормативної собівартості товарної продукції за статтями витрат у плановому році підприємства і в періоді до кінця року в розрізі причин, баз і стимулів.

Бухгалтерський облік включає:

- облік грошових коштів (щоденно, по цехам, за місяць);
- облік основних засобів та нарахування амортизації (по цеху, по заводу, за місяць);
- облік втрат від браку (по підприємству, по заводу, за місяць);
- комплекс операцій з обліку руху матеріалів на складах підприємства (облік надходжень і виплат по складах і цехах);
- підготовка залишків на кінець місяця (оборотно-сальдова відомість);
- підготовка залишків матеріалів на складі, які не використовуються на заводі протягом трьох місяців;
- калькуляція нормативних витрат на одиницю продукції (на цех на місяць);
- калькуляція стандартних витрат на одиницю продукції (на цех за місяць);
- повний набір облікових процедур з руху та реалізації готової продукції.

Закупівля матеріалів і технологій:

- розрахунок лімітів матеріалів (щоквартально та щомісячно на одиницю продукції);
- комп'ютеризоване управління запасами матеріалів, виявлення надлишків і нестач;
- підготовка та друк допоміжних лімітних карток матеріалів;
- облік вхідних і вихідних матеріалів, наявність матеріалів, контроль рівня запасів;
- підготовка лімітних карток на ремонт і технічне обслуговування (РТО) та розрахунок сум на них.

Управління основним виробництвом:

- розрахунок детальних планів для компонентів і складальних одиниць, необхідних для комерційного виробництва (по компанії, щорічно і щоквартально по підрозділах);

- розрахунок фізичного плану для решти компонентів і складальних одиниць (по підрозділах, поквартально, помісячно);
- розрахунок планів виробництва комплектуючих і складальних одиниць (на одиницю, щомісяця);
- оперативний облік виконання плану виробництва деталей і складальних одиниць (по цехах, щомісяця);
- оперативний облік виконання плану поставок матеріальних цінностей між цехами (для добових підприємств з початку місяця);
- оперативний облік виконання плану випуску товарної продукції за найменуванням і кількістю (за підрозділами та підприємствами, щоденно з початку місяця);
- оперативний облік простоїв обладнання (за ділянками, щоденно з початку місяця)
- оперативний облік випуску продукції;
- оперативний облік переміщень продукції (по цехах, по місяцях).

Управління технічним обслуговуванням інструменту:

- рух і управління запасами інструменту протягом місяця за допомогою МІС;
- управління ремонтною службою;
- облік і аналіз парків виробничого (верстатного) обладнання (по ділянках і підприємству за місяць, квартал і рік).
- підготовка статистичних звітів.

Управління та реалізація продажів продукції:

- розрахунок поставок (річних, квартальних і місячних, за місцем поставки);
- оперативний облік виконання плану поставок продукції (щоденний, щомісячний, щоквартальний, річний, у розрізі покупців);
- облік руху готової продукції на складі (щоденний, щомісячний).
- автоматичне формування замовлень на відвантаження продукції;
- розрахунок графіків робіт і календарних програм відвантаження

запасних частин на основі квартальних контрактних зобов'язань.

Таким чином, аналізоване підприємство ПрАТ "Кіровоградобленерго" включає наступні джерела інформації:

1) інформація про комерційну таємницю:

- заробітна плата,
- договори з постачальниками та покупцями;
- технологія виробництва;

2) інформація з обмеженим доступом:

- особисті справи працівників;
- трудові договори;
- особові картки працівників;
- бухгалтерські документи та внутрішні бухгалтерські звіти;
- подальші розробки та документи для внутрішнього користування;

3) публічна інформація:

- буклет,
- інформація на веб-сайті,
- Статут,
- тарифи, прейскуранти на продукти та послуги.

2.4. Оцінка системи забезпечення інформаційної безпеки підприємства ПрАТ «Кіровоградобленерго»

Стає все більш очевидним, що загальний рівень економічної безпеки організації залежить від інформаційної складової. Як свідчить практика, ворожі дії проти інтересів організації починаються зі збору інформації. Часто навіть дрібним крадіжкам передують розслідування можливої протиправної діяльності осіб зі злочинними намірами, а без належної розвідувальної підтримки неможливо уявити такі руйнівні прояви, як незаконне привласнення активів компанії або рейдерське захоплення.

Метою існуючої системи інформаційної безпеки в ПрАТ

"Кіровоградобленерго" є забезпечення ефективної інформаційно-аналітичної підтримки господарської діяльності компанії.

Відповідні служби виконують певні функції, які характеризують процес побудови та захисту інформаційної складової економічної безпеки. До таких функцій належать:

- 1) збір всієї інформації про діяльність конкретної організації;
- 2) аналіз отриманої інформації, забезпечення дотримання загальноприйнятих принципів і методів;
- 3) прогнозування тенденцій розвитку науково-технічних, економічних і політичних процесів;
- 4) оцінювання рівня економічної безпеки за всіма складовими та підготовка рекомендацій щодо підвищення цього рівня в цілому в конкретних організаціях;
- 5) інші заходи, спрямовані на розвиток інформаційної складової економічної безпеки.

Організації отримують безперервний потік інформації з різних джерел. Інформацію можна розділити на наступні категорії:

- опублікована офіційна інформація;
- неконфіденційна інформація, яка може бути отримана працівниками організації через неформальний контакт з власником такої інформації;
- конфіденційна інформація, яка, ймовірно, може бути отримана співробітником компанії в неформальному контакті з власником інформації.

Дослідження показують, що 90-95% необхідної інформації можна законно отримати, вивчаючи службові записки співробітників компанії, публікації, індивідуальні звіти співробітників, різноманітні виставки, ярмарки та презентації, дані товарних бірж та фондових ринків, оголошення про прийом на роботу, боротьбу за посади тощо. Тому керівництву компанії слід запровадити правові норми захисту конфіденційності та систему контролю за збереженням комерційної таємниці.

Порушення таких параметрів інформації, як конфіденційність,

цілісність, доступність і надійність в компаніях може мати дуже негативні наслідки:

- вихід з ладу систем управління технологічними процесами та інших критично важливих систем;
- витік інформації, що становить комерційну таємницю або інші види конфіденційності;
- порушення конфіденційності інформації;
- порушення достовірності фінансових документів;
- несанкціонований доступ до персональних даних фізичних осіб та ін.

В результаті вищезазначеного можуть виникнути наступні негативні наслідки:

- погіршення ділових відносин з партнерами;
- зрив переговорів, втрата вигідних контрактів;
- невиконання договірних зобов'язань;
- потреба в додатковому дослідженні ринку;
- відмова від рішень, які стали неефективними через дифузію знань і, як наслідок, економічні втрати, пов'язані з новими розробками;
- втрата можливості отримати патенти або продати ліцензії на результати науково-технічної діяльності;
- зниження цін або обсягів продажів;
- пошкодження комерційної репутації;
- жорсткіші умови кредитування;
- труднощі з пошуком або придбанням обладнання.

У деяких випадках нехтування питаннями інформаційної безпеки може призвести до повного банкрутства.

Тому аналіз загроз і ризиків має вирішальне значення для створення ефективної системи інформаційної безпеки. Однак, за оцінками експертів, лише менше 5% компаній використовують власні методи аналізу ризиків, які дозволяють проводити кількісний аналіз та оптимізацію підсистем інформаційної безпеки. У той же час, дії інсайдерів, такі як недбалість співробітників, крадіжки інформаційних ресурсів та ІТ-обладнання, фінансові

та інші види шахрайства з використанням інформаційних систем і ресурсів, набагато рідше привертають увагу при вирішенні питань інформаційної безпеки, якщо розглядати їх окремо від загальної мети забезпечення економічної безпеки. Дослідження показують, що більшість компаній не мають адекватних заходів для захисту від інсайдерських атак.

Згідно зі статистикою інформаційної безпеки, близько 80 відсотків зловмисників - це інсайдери. Людський фактор завжди був одним з найважливіших ризиків для будь-якого бізнесу, оскільки більшість інцидентів спричинені працівниками. Часто буває важко відрізнити навмисний витік інформації від ненавмисного, але це не завжди необхідно, оскільки обидві ситуації можуть мати руйнівні наслідки для компанії. Той факт, що більшість керівників не знають про причини інсайдерських загроз, свідчить про те, що компанії не приділяють достатньої уваги інформаційній безпеці.

Аналіз середнього бізнесу показав, що випадкові кібератаки трапляються частіше і потенційно завдають більшої шкоди, ніж навмисні атаки інсайдерів. Дослідження показало, що більшість компаній приділяють набагато більше уваги захисту від навмисних інсайдерських атак, ніж більш частим і потенційно більш руйнівним випадковим інсайдерським інцидентам.

Потенційні внутрішні ризики, які несуть співробітники, що мають доступ до критично важливих систем та конфіденційної інформації, залишаються поза увагою. Хоча керівники знають про ці ризики, занепокоєння щодо зовнішньої інформаційної безпеки часто переважає над іншими питаннями. Однак кількість витоків інформації, несанкціонованого доступу та зловживань з боку самих працівників є значною і загрожує основам багатьох компаній.

Керівники опитаних компаній зазначили, що не знають джерел та причин внутрішніх загроз. Водночас, компанії намагаються оцінити потенційні фінансові втрати та операційний вплив цих загроз. Половина респондентів вважають, що більшість внутрішніх загроз є ненавмисними, 20% - що навмисними, 25% - що навмисних і ненавмисних загроз приблизно

порівну, а 5% не змогли відповісти. Однак, коли респондентів попросили проранжувати найбільші загрози за ступенем важливості, майже 85% опитаних не змогли з упевненістю сказати, чи були внутрішні інциденти, спричинені підрядниками або тимчасовим персоналом, навмисними чи випадковими.

Дослідження також показало, що компанії щомісяця стикаються з інцидентом, який підпадає під одну з десяти категорій загроз. Найпоширенішим інцидентом є ненавмисна втрата даних через недбалість співробітників - 15-20 інцидентів на рік. На зловмисні атаки та шпигунство всередині компанії припадає 10 інцидентів на рік, а на несанкціонований доступ до інформації - 20 інцидентів на рік. Відповідно до галузей, опитані компанії стикаються з 20-30 інцидентами на рік. Отримані дані свідчать про те, що універсального рішення для усунення внутрішніх ризиків не існує. Кожна компанія має розробити власний комплексний підхід, враховуючи специфіку своєї структури та діяльності.

Хоча кількість навмисних атак зростає, реальність така, що випадкові помилки та недостатня увага до правил безпеки впливають на роботу компанії набагато більше, ніж шахрайські атаки.

Експерти з інформаційної безпеки дотримуються двох точок зору. Перша полягає в тому, що інформаційній безпеці в компаніях можна повністю запобігти, не витрачаючи жодних коштів. У цьому випадку ризики, на які ми йдемо, можуть бути повністю виправдані. Інша думка полягає в тому, що для створення системи інформаційної безпеки необхідно витратити значні кошти (наприклад, на навчання персоналу, програмне забезпечення тощо) і, таким чином, забезпечити належний рівень безпеки. Однак це залишає прогалини, які рано чи пізно призведуть до витоку або крадіжки конфіденційної інформації.

Для обґрунтування витрат на інформаційну безпеку можна використовувати такі підходи.

Впровадити інструменти для визначення рівня інформаційної безпеки

на практиці. Керівництво компанії має брати участь в оцінці цінності інформаційних ресурсів та визначенні потенційних збитків, спричинених порушенням інформаційної безпеки. Результати цих оцінок значною мірою визначатимуть подальшу діяльність керівництва у сфері інформаційної безпеки. Якщо інформація не має цінності, не існує значної загрози для інформаційних активів і потенційний збиток мінімальний, то проблему інформаційної безпеки можна залишити в спокої. Якщо ж інформація має значну цінність, а загрози і потенційна шкода очевидні, виникають питання бюджетування підсистеми інформаційної безпеки. У цьому випадку керівництво компанії має бути обізнаним у питаннях інформаційної безпеки та допомагати компанії у створенні системи інформаційної безпеки.

Лише створивши ефективну систему інформаційної безпеки, підприємство може бути надійно захищене від описаних вище негативних явищ.

Однак проблеми тут мають як організаційний, так і фінансовий характер. По-перше, найбільшою проблемою у створенні системи інформаційної безпеки є нерозуміння керівництвом необхідності такої системи. Багато керівників не усвідомлюють, що створення системи інформаційної безпеки є вкрай необхідним, адже своєчасне створення такої системи може запобігти збиткам, а іноді навіть врятувати бізнес.

Другою проблемою у створенні систем інформаційної безпеки є відсутність достатніх фінансових ресурсів. Відсутність фінансування з мінімальних бюджетів на створення систем інформаційної безпеки також є дуже поширеним явищем. Наприклад, у США та Європейському Союзі (ЄС) на створення та підтримку систем інформаційної безпеки виділяється 30% прибутку компанії. В Україні ж, навіть коли ці кошти виділяються, вони носять разовий і недостатній характер. Достатнім може бути продовження ліцензій на антивірусні програми. Крім того, дуже мало компаній планують і затверджують бюджети на інформаційну безпеку, виходячи з реальних потреб.

Третьою небезпечною проблемою є ситуація, коли, незважаючи на розуміння керівництва та необхідне фінансування, встановлення систем інформаційної безпеки доручається фахівцям без відповідної підготовки та достатнього досвіду. Зазвичай це системний адміністратор або відділ технічної підтримки. Вони ставляться до цього як до встановлення та налаштування антивірусу. Присутність інсайдерських зловмисників зазвичай взагалі не береться до уваги. Статистика показує, що 70 відсотків порушень відбувається саме через інсайдерів. Найчастіше не приділяється належна увага каналам комунікації, залишаються незахищеними взаємодії керівництва компанії з бізнес-партнерами та клієнтами. В результаті таких дій витрачаються гроші, а інформаційна безпека залишається на тому ж рівні.

Багато керівників підприємств можуть не бачити очевидного зв'язку між втратою доходів і браком фінансових ресурсів на системи інформаційної безпеки. Тому перший крок полягає в тому, щоб сформулювати проблему таким чином, щоб вона була зрозумілою для бізнесу. Це завдання лягає на плечі керівництва служби інформаційної безпеки компанії. Менеджери повинні виявити і чітко представити власникам бізнесу всі загрози в інформаційній сфері та переконати їх у тому, що протистояти цим загрозам можна лише шляхом створення та впровадження ефективних систем інформаційної безпеки.

При створенні такої системи необхідно, по-перше, враховувати необхідність реалізації комплексу різномірних заходів для ефективного захисту інформаційних ресурсів, які умовно можна поділити на три групи: правові, організаційні, економічні та технічні. По-друге, формулюванням заходів у кожній з трьох груп повинні займатися фахівці у відповідних галузях знань, які будуть використовувати власні методи і прийоми для досягнення поставлених цілей, але кінцевий успіх буде залежати від того, наскільки вдасться визначити взаємозв'язки між відповідними визначеннями, принципами, методами і механізмами захисту і планомірно впроваджувати їх в рамках системного підходу.

Основними проблемами та загрозами у сфері інформаційної безпеки в ПрАТ "Кіровоградобленерго", є наступні:

- фізичний доступ зломисників до робочого місця;
- відсутність системи контролю доступу працівників до чужих робочих місць;
- відсутність систем відеоспостереження на підприємствах;
- розголошення конфіденційної інформації, що зберігається на робочому місці працівника;
- відсутність угод про конфіденційність між працівниками та роботодавцями;
- нечіткість положень щодо відповідальності працівників на підприємстві;
- пошкодження або втрата інформації через спеціальне програмне забезпечення або віруси;
- відсутність обмежень на доступ до Інтернету та мереж підприємства;
- поломка системи контролю доступу в організації;
- несанкціоноване копіювання, друк або відтворення конфіденційної інформації;
- необмежений доступ працівників до копіювальної або розмножувальної техніки;
- знищення або втрата інформації через віруси; пошкодження обладнання; надзвичайні ситуації (пожежа);
- знищення або втрата інформації через збої в інфраструктурі, включаючи пошкодження телекомунікаційних систем, електрики, джерел тепла, кондиціонування або обладнання.

Крім ризику втрати інформації, ПрАТ "Кіровоградобленерго" також враховує загрози, пов'язані з порушенням цілісності інформації:

- неправильне введення даних;
- крадіжка інформації;
- дублювання даних;

- втрата інформації на жорстких дисках;
- загрози цілісності корпоративних баз даних;
- встановлення неоригінального програмного забезпечення.

Таким чином, в сучасних умовах інформаційна безпека є невід'ємною частиною системи економічної безпеки підприємства. Надійний інформаційний захист є необхідною умовою переходу до моделі сталого розвитку не тільки окремих підприємств, а й національної економіки в цілому. На нашу думку, особливу увагу слід приділяти формуванню та реалізації інформаційної політики підприємства та практичній реалізації запропонованих заходів щодо забезпечення інформаційної безпеки, які повинні стати основою захисту інформації від внутрішніх та зовнішніх загроз.

Отже, аналіз стану інформаційної безпеки в ПрАТ "Кіровоградобленерго" дозволив виявити наступні загрози:

1. передача комп'ютерних вірусів через знімні носії інформації, комп'ютерні мережі та Інтернет;
2. помилки персоналу, тобто некоректне введення або зміна даних;
3. внутрішні збої інформаційних систем, тобто програмні або апаратні збої, пошкодження обладнання;
4. загрози технічного характеру;
5. загрози нетехнічного або некомп'ютеризованого характеру - відсутність паролів, зберігання конфіденційної інформації про інформаційну систему на папері;
6. несанкціонований доступ до інформації (використання ресурсів без попереднього дозволу). Сюди входить: несанкціонований перегляд інформації; несанкціонована модифікація інформації; несанкціоноване знищення інформації;
7. крадіжка програмного забезпечення, обладнання тощо.

РОЗДІЛ 3

НАПРЯМИ ВДОСКОНАЛЕННЯ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

3.1. Формування сучасної системи інформаційної безпеки підприємства

В компанії нашого розміру зовсім не доцільно пропонувати створення організаційної структури, завданням якої є забезпечення інформаційної безпеки.

Тому в ПрАТ "Кіровоградобленерго" пропонується вдосконалити існуючу систему інформаційної безпеки шляхом розширення функцій існуючого в компанії відділу інформаційного забезпечення для забезпечення виконання функції захисту інформації та досягнення бажаного рівня інформаційної безпеки. Також пропонується перейменувати цей відділ у Службу корпоративної інформаційної безпеки.

Проаналізувавши погляди та концептуальні підходи до створення ефективної сучасної корпоративної системи інформаційної безпеки, вдалося сформулювати основні функції та завдання, а також окреслити організаційні засади, на яких буде функціонувати відповідний відділ інформаційної безпеки.

У сучасному уявленні про рольові функції служби інформаційної безпеки можна виділити чотири напрямки:

- 1) розробка методологій і методик аналізу загроз і оцінки рівня інформаційної безпеки та її забезпечення в компанії
- 2) організація та здійснення окремих видів діяльності з інформаційної безпеки; та
- 3) експлуатація технічних засобів захисту інформації.
- 4) аудит та управління системою інформаційної безпеки підприємства.

Перший напрямок охоплює такі основні питання:

- аналіз та узагальнення причин виникнення потенційних загроз та фактичних порушень вимог інформаційної безпеки;
- аналіз ступеня безперервності бізнес-процесів, що базуються на ІТ, з точки зору інформаційної безпеки;
- дослідження нових загроз та вразливостей, пов'язаних з інформаційними взаємодіями;
- розробка методів оцінки інформаційних ризиків;
- дослідження інформації про бізнес та джерела інформації;
- розробка методів захисту інформації та ІТ-безпеки і способів їх застосування в бізнесі;
- розробка та модифікація концепцій та політик інформаційної безпеки;
- розробка регіональної нормативно-правової бази з цих питань з урахуванням комплексного підходу до економічної безпеки;
- розробка методології оцінки рівня інформаційної безпеки та визначення адекватності захисту інформації та ІТ з урахуванням потреб бізнесу та існуючої і майбутньої нормативно-правової бази;
- аналіз відповідності вимогам інформаційної безпеки всіх використовуваних процедур;
- створення, обробка, передача, зберігання та знищення інформації;
- процедури інформаційної взаємодії між підрозділами компанії та із зовнішніми організаціями;
- процедури доступу до інформаційних ресурсів та зовнішніх комп'ютерних мереж працівників компанії та суміжних організацій, а також клієнтів.
- проекти розвитку ІТ, включаючи телекомунікації та телекомунікаційні системи;
- пропоновані угоди із зовнішніми організаціями щодо обміну інформацією;
- проекти інших нормативних документів, що регулюють обмін інформацією;

- підготовка аналітичних записок, що містять результати аналізів та рекомендації щодо впровадження заходів із захисту інформації.

Другий напрямок в основному включає в себе наступні завдання:

- планування діяльності компанії у сфері інформаційної безпеки на основі координації діяльності всіх підрозділів;
- організація та участь у впровадженні методів захисту інформації в діяльність компанії;
- робота з персоналом, партнерами та клієнтами;
- затвердження запитів і процедур доступу співробітників і зовнішніх організацій до інформаційних ресурсів компанії;
- процедури обміну інформацією між підрозділами та зовнішніми організаціями;
- угоди, що укладаються при обміні інформацією;
- проекти наказів, інструкцій та інших нормативних документів;
- вирішення практичних проблем, пов'язаних з інформаційною безпекою, що виникають в різних підрозділах.

У третьому напрямку основними питаннями, що потребують вирішення, є наступні:

- підтримка ключових структур, що використовуються зовнішніми та вбудованими засобами криптографічного захисту інформації;
- операційна підтримка інших засобів захисту інформації.

Четвертий напрямок спрямований на вирішення наступних основних завдань:

- перевірка дотримання вимог інформаційної безпеки співробітниками компанії та іншими особами, які мають доступ до інформаційних ресурсів;
- моніторинг поведінки користувачів ІТ (наприклад, несанкціоновані зміни інформації, використання пошти або інших інтернет-сервісів для передачі конфіденційної інформації за межі організації);
- контроль за своєчасною зміною дозволів користувачів в інформаційних системах; блокування облікових записів користувачів, які були

звільнені (переведені на інші завдання);

- контроль за дотриманням налаштувань безпеки, включаючи політики паролів, інші вбудовані системи інформаційної безпеки та зовнішні засоби захисту інформації;

- моніторинг роботи систем виявлення (запобігання) мережних вторгнень, систем оцінки якості мережі та інших автоматизованих систем комп'ютерної безпеки;

- участь в аналізі виявлених порушень інформаційної безпеки та вимог нормативних документів з цих питань;

- підготовка пропозицій щодо запобігання порушенням;

- проведення внутрішніх аудитів з питань інформаційної безпеки;

- підготовка пропозицій щодо використання зовнішніх аудитів;

- моніторинг можливих порушень конфіденційної інформації технічними каналами.

Враховуючи міждисциплінарний характер питань, що входять до блоку інформаційної безпеки, деякі з перелічених функцій можуть виконуватися лише у взаємодії з іншими структурними службами підприємства (наприклад, кадровою, юридичною, бізнес-службами).

Це вимагає визначення організаційної політики безпеки (набір керівних принципів, правил, процедур і практик у сфері інформаційної безпеки, які регулюють управління, захист і розподіл цінної інформації на підприємстві).

Як правило, такий набір правил є частиною функціональності програмного продукту, необхідного для використання в конкретній організації.

У більш формальному розумінні, політика безпеки - це відомчий документ, що містить конкретні вимоги до функціонування системи безпеки.

Основною причиною появи політик безпеки є те, що такі документи часто запитують організації, які визначають правила роботи для компаній цього сектору. У цьому випадку відсутність політики може призвести до прийняття репресивних заходів щодо компанії або навіть до повного

припинення її діяльності.

Крім того, конкретні вимоги та рекомендації встановлюються галузевими або загальними, регіональними чи міжнародними стандартами. Часто це виражається у вигляді зауважень зовнішнього аудитора, який перевіряє діяльність компанії. Відсутність політики призводить до негативної оцінки, що, в свою чергу, впливає на публічні показники компанії, тобто на її позицію в рейтингах та рівень довіри до неї.

Втрати від настання інформаційного ризику можуть бути подані у вигляді таблиці (табл. 3.1).

Таблиця 3.1

Градація втрат від інформаційного ризику

Величина ризику	Опис
0,1-0,2	Оголошення інформації принесе незначні моральні і фінансові втрати підприємству
0,2-0,3	Втрати від інформаційної атаки є, але вони незначні, основні фінансові операції і становище підприємства на ринку не порушено
0,3-0,4	Фінансові операції не ведуться про-тягом деякого часу, за цей час підприємство зазнає збитків, але його становище на ринку і кількість клієнтів змінюються мінімально
0,4-0,6	Значні втрати на ринку й у прибутку. Підприємство втрачає значну частину клієнтів
0,6-0,8	Втрати дуже значні, підприємство на період до року втрачає становище на ринку. Для відновлення становища потрібні великі фінансові інвестиції
0,8-1,0	Підприємство припиняє існування

Джерело:[21]

Наступний крок - з'ясувати, наскільки серйозних збитків може зазнати компанія в разі настання інформаційного ризику для конкретного

інформаційного об'єкта. Існує ряд методів розрахунку ризику, але тут розглядається найпростіший метод.

Слід зазначити, що класифікацію шкоди, завданої атакою, повинен оцінювати власник інформації або особа, відповідальна за її використання. Оцінку ймовірності атаки найкраще доручити технічному персоналу підприємства.

Серед різних організаційних схем функціонування підрозділів, відповідальних за інформаційну безпеку підприємства (функції таких підрозділів покладаються на системного адміністратора, а відповідний підрозділ входить до структури служби інформаційної безпеки, що підпорядковується вищому керівництву), найкращим варіантом є служба економічної безпеки, де підрозділ інформаційної безпеки входить до складу служби економічної безпеки. Це створює чудову можливість вирішувати проблеми інформаційної безпеки в рамках загальних операцій із забезпечення безпеки бізнесу.

3.2. Механізм збереження комерційної таємниці на підприємстві

У промислово розвинених країнах захист комерційної таємниці є обов'язком як окремих осіб, так і підрозділів компаній. Однак, оскільки не всі вітчизняні компанії мають служби безпеки, доцільно приділяти особливу увагу питанню конфіденційності під час підписання трудових договорів між керівництвом компанії та працівниками. Це відображає особисту відповідальність працівників за захист комерційної таємниці.

Згідно з опитуванням західних експертів, 25% працівників готові зрадити інтереси компанії в будь-який час і за будь-яких обставин, 50% можуть зробити це в залежності від обставин, і лише 25% є патріотами, які ніколи не зрадять інтереси компанії.

У найзагальнішому вигляді втрати компанії полягають у наступному:

- 1) зменшення можливостей продажу ліцензій на власні наукові

розробки, втрата пріоритетності в напрямках науково-технічного прогресу та збільшення витрат на переорієнтацію діяльності науково-дослідного підрозділу

2) труднощі із закупівлею сировини, технологій, обладнання та інших складових нормальної виробничої діяльності; та

3) Обмеження співпраці з постачальниками, зменшення можливостей укладання вигідних контрактів та проблеми з виконанням договірних зобов'язань.

Точно оцінити загальну суму всіх втрат дуже складно, а іноді навіть неможливо через відсутність достовірних вихідних даних. Тому достатньо загальної оцінки фахівцями втрат компанії, спричинених недотриманням вимог інформаційної безпеки.

Компенсація таких втрат вимагає значних додаткових витрат, що знижує загальну ефективність виробництва і можливість успіху в конкурентній боротьбі. Тому, зважаючи на те, що захисту комерційної таємниці надається все більше значення, має сенс запроваджувати більш детальні заходи щодо забезпечення конфіденційності інформації в компаніях.

Ці заходи можна умовно поділити на зовнішні та внутрішні, а також на правові, організаційні, технічні та психологічні (рис. 3.1). Крім того, деякі джерела виділяють страхування, тобто страхування від розголошення комерційної таємниці.

Крім того, захист комерційної таємниці включає в себе:

- процедури визначення інформації, що становить КТ, та періоду її дії;
- системи допуску працівників, відряджених осіб та осіб з обмеженим доступом до інформації, що становить КТ;
- процедури, пов'язані з документами та печатками з грифом КТ;
- безпека документів, справ і публікацій з грифом КТ;
- обов'язки осіб, які мають доступ до інформації, що становить КТ;
- принципи організації та контролю за забезпеченням безпеки систем при використанні інформації, що становить КТ;

- відповідальність за розголошення інформації та втрату документів, що становлять КТ.

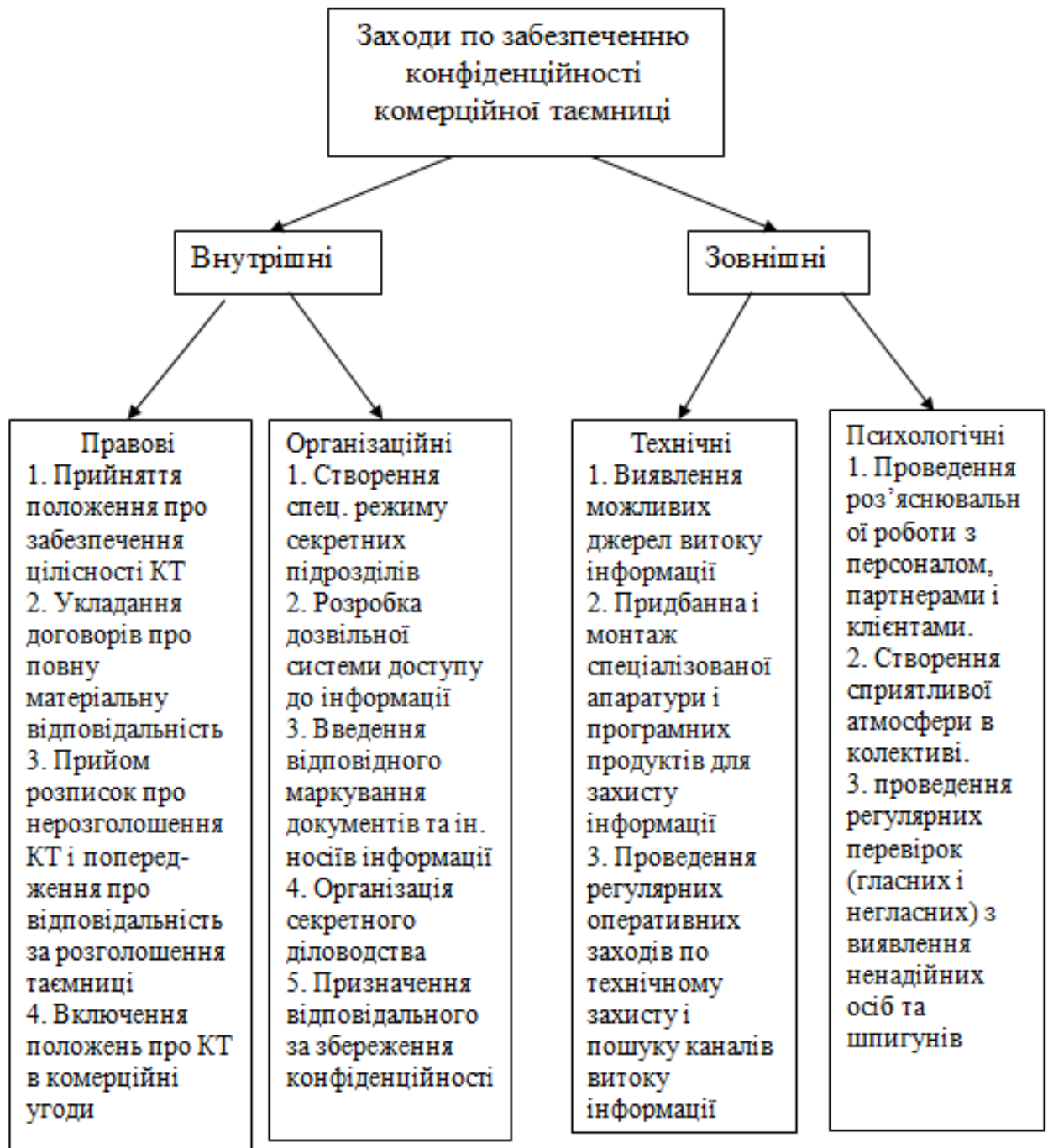


Рис. 3.1. Заходи по забезпеченню конфіденційності комерційної таємниці ПрАТ "Кіровоградобленерго"

Джерело:[розроблено автором]

Контроль за обліком, розмноженням, зберіганням і використанням документів, справ і видань з грифом "КТ" покладається на уповноважені

органи з питань безпеки.

Слід звернути увагу на перелік відомостей, які не становлять комерційної таємниці:

- установчі документи, документи, що дають право на участь у корпоративній або господарській діяльності та їх окремі види;
- відомості за всіма встановленими формами державної звітності;
- дані, необхідні для перевірки обчислення і сплати податків та інших обов'язкових платежів;
- відомості про чисельність і склад трудового колективу, загальну заробітну плату, заробітну плату за професіями та посадами, наявність вакантних робочих місць;
- документи про сплату податків та обов'язкових платежів;
- відомості про забруднення навколишнього середовища, недотримання безпечних умов праці, реалізацію небезпечної для здоров'я продукції та інші порушення законодавства України, розмір завданих збитків;
- документи про платоспроможність;
- відомості про участь посадових осіб підприємства в кооперативах, малих підприємствах, асоціаціях, товариствах та інших організаціях, що займаються підприємницькою діяльністю;
- інформація, розкриття якої передбачено чинним законодавством.

Іншими словами, компанії зобов'язані надавати вищезазначену інформацію на вимогу органів державного управління, контролюючих органів, правоохоронних органів та інших юридичних осіб.

Перелік та обсяг відомостей, що становлять комерційну таємницю компанії, умови конфіденційності, порядок захисту доступу до конфіденційної інформації та правила їх використання визначаються відповідальною особою організації. Для виконання цього завдання керівництво може залучати аналітиків.

Як зазначають експерти, основною метою захисту конфіденційної інформації є запобігання її поширенню серед конкурентів. У деяких випадках

необхідно також захищати комерційну таємницю "інших", довірену компанії іншими особами або організаціями. За відсутності такого захисту компанія може втратити вигідних партнерів та клієнтів.

Забезпечення захисту комерційної таємниці включає:

- введення в дію правил віднесення інформації до комерційної таємниці;
- розробку та доведення до відома осіб, уповноважених отримувати інформацію, що становить комерційну таємницю, інструкцій щодо дотримання режиму конфіденційності;
- обмеження доступу до носіїв інформації, що містять комерційну таємницю;
- використання організаційних, технічних та інших засобів захисту конфіденційної інформації;
- контроль за дотриманням встановленого режиму охорони комерційної таємниці.

Як і всі працівники компанії, менеджери повинні підписувати зобов'язання про нерозголошення комерційної таємниці (відповідальність за захист) при прийомі на роботу та приступаючи до роботи.

Основними зобов'язаннями в цьому документі є:

- 1) не розголошувати інформацію, що має характер комерційної таємниці, яка стала відома під час виконання службових обов'язків, у тому числі протягом певного періоду після виходу на пенсію;
 - 2) дотримуватися вимог щодо захисту комерційної таємниці, доведених до відома працівників;
 - 3) не використовувати інформацію, що становить комерційну таємницю, без згоди власника;
 - 4) не брати на себе зобов'язань перед іншими особами або компаніями.
- За рівнем знань менеджери в більшості компаній поступаються лише генеральному директору.

Менеджери є контактною особою для людей, які отримують доступ до різноманітної інформації. Тому вони повинні приділяти належну увагу

спілкуванню з потенційними партнерами та клієнтами. У зв'язку з цим експерти дають наступні поради.

1) Менеджери повинні добре відповідати на низку запитань. Завжди слід чітко розрізняти звичайні рутинні запитання та "слизькі" запитання, відповідь на які може розкрити конфіденційну інформацію компанії. У такому випадку слід запитати себе: "Чи має право інша сторона знати цю інформацію? Чи має право інша сторона знати цю інформацію? Відповідь на "слизьке" питання повинна бути ухильною. На думку японських експертів, найбільш прийнятною відповіддю на таке питання є "я не знаю". Згідно з діловою етикою, такі відповіді взагалі небажані для менеджерів. Вони також можуть порадити своїм співрозмовникам поставити це питання керівнику компанії.

2) У більшості випадків щодо конфіденційної інформації слід прислухатися до порад керівника компанії або служби безпеки компанії. Менеджери повинні знати, хто має доступ до якої інформації та обладнання за родом своєї діяльності, і дотримуватися встановлених правил. Крім того, якщо, наприклад, рядовий співробітник компанії раптом зацікавився конфіденційними документами, цю ініціативу необхідно швидко і тактично заблокувати.

3) Особливу увагу слід приділяти предметам, які "забувають" відвідувачі. Звичайні блокноти, фломастери, гаманці та інші предмети можуть стати технічними пристроями для прослуховування або "перехоплення" найважливішої інформації, наприклад, відразу після співбесіди або коли відвідувач йде. Професіонали можуть легко встановити підслуховуючі пристрої в будь-який момент, тому відвідувачі не повинні залишатися в офісі наодинці. Усі забуті або знайдені речі слід негайно передавати службі безпеки компанії. Це робота професіоналів - піклуватися про них.

4) Керівники, як і інші працівники компанії, повинні усвідомлювати важливість конфіденційної інформації для успішної роботи і процвітання компанії та бути обізнаними з прийомами і методами, які можуть використовувати конкуренти для збору такої інформації [9]. Існують

практичні рекомендації щодо захисту конфіденційної інформації.

Для обмеження доступу до інформації, що становить комерційну таємницю, керівники повинні видати відповідні накази, описати способи захисту цієї інформації в "переліку відомостей, що становлять комерційну таємницю компанії", визначити коло осіб, які мають доступ до цієї інформації, а також встановити правила поводження з документами з грифом "комерційна таємниця". Працівники компанії зобов'язані ознайомитися з цим наказом та додатками до нього.

Приблизний перелік інформації, що становить комерційну таємницю підприємства:

- сума кредиту компанії або сума кредиту, яку вона отримала або має намір отримати;
- найменування контрагентів
- розмір прибутку (щомісяця, щокварталу, щороку);
- розподіл прибутку;
- цілі, завдання і тактика переговорів з партнерами;
- умови комерційних контрактів та послуг;
- рівень готовності купувати товари та послуги;
- заробітна плата працівників;
- характер і репутація працівників;
- напрямки маркетингових досліджень компанії.

При необхідності цей перелік може бути доповнений.

Отже, проблема захисту комерційної таємниці підприємства діалектично пов'язана з його економічною безпекою.

3.3. Впровадження додаткових показників оцінки ефективності управління забезпеченням інформаційної безпеки

Фахівці розуміють термін "інформаційна безпека" по-різному, часто маючи на увазі лише один аспект проблеми. Наприклад, з точки зору

керівників компаній, серйозною загрозою є крадіжка конфіденційних документів, з точки зору розробників антивірусного програмного забезпечення - ризик знищення цінних даних. Кожен з цих аспектів заслуговує на окреме дослідження, але для споживачів важливо забезпечити загальну безпеку, а не тільки з точки зору окремих ризиків.

На наш погляд, інформаційна безпека для компаній складається з конкретних дій, спрямованих на виявлення, усунення та нейтралізацію джерел, причин та умов, несприятливих для інформації.

Водночас поняття "інформаційна безпека" описує стан захищеності інформації організаційного утворення, за якого можуть виникати загрози. Це реалізується за допомогою систем протидії, спрямованих на попередження, виявлення та усунення інформаційних загроз.

Для того, щоб більш точно та об'єктивно оцінити рівень інформаційної безпеки компанії, розглянемо більш детально індикатори інформаційної безпеки компанії.

Продуктивність інформації (Пін) обчислюється за формулою:

$$П_{ін} = \frac{П_{п}}{В_{ін}}, \text{ до зростання} \quad (3.1)$$

де $П_{п}$ - обсяг промислової продукції, грн.;

$В_{ін}$ - витрати на придбання інформаційних ресурсів, грн.

Наступним показником є коефіцієнт інформаційної озброєності:

$$К_{ін.озб.} = \frac{В_{ін.}}{Ч_{с.с.}} * 100\%, > 20\%, \quad (3.2)$$

де $В_{ін.}$ - витрати на придбання інформаційних ресурсів, грн;

$Ч_{с.с.}$ - середньоспискова чисельність працівників, осіб.

Коефіцієнт захищеності інформації обчислюється за формулою:

$$К_{з.ін.} = \frac{В_{з.ін.}}{В_{ін.}} * 100\%, \leq 20\%, \quad (3.3)$$

де $В_{з.ін.}$ - витрати підприємства на захист інформаційних ресурсів, грн;

$В_{ін.}$ - витрати на придбання інформаційних ресурсів, грн.

Реалізація заходів щодо розвитку та захисту інформаційної складової економічної безпеки здійснюється шляхом послідовного виконання

наступного комплексу завдань

- а) збір різних видів необхідної інформації;
- б) обробка та систематизація отриманої інформації;
- в) аналіз цієї інформації;
- г) захист інформаційного середовища підприємства.

До переліку процедур пов'язаних із інформаційним середовищем підприємства, перш за все, належать наступні:

- заходи щодо захисту організацій від промислового шпигунства з боку конкурентів або інших юридичних чи фізичних осіб;
- технічний захист об'єктів, транспорту, зв'язку, переговорів і різних документів від несанкціонованого доступу до конфіденційної інформації з боку зацікавлених юридичних або фізичних осіб;
- збір інформації про потенційних суб'єктів промислового шпигунства та вжиття необхідних заходів для запобігання таким спробам;
- діяльність у сфері зовнішньої розвідки.

Рівень інформаційної складової економічної безпеки визначається тим, наскільки при прийнятті управлінських рішень використовується неповна, неточна або суперечлива інформація.

Як індикатори рівня інформаційної безпеки також використовуються наступні коефіцієнти:

✓ Повнота інформації (П): розраховується як співвідношення між обсягом інформації, доступної особі, яка приймає рішення, та обсягом інформації, необхідної для прийняття цього рішення;

✓ Точність інформації (А): визначається як відношення кількості релевантної (достовірної) інформації до загального обсягу наявної інформації;

✓ Суперечливість інформації (А). Це відношення загальної кількості незалежних доказів на користь того чи іншого рішення до загального обсягу релевантної інформації. Рівень інформаційної безпеки можна визначити як добуток коефіцієнта.

Коефіцієнт більше 0,7 означає "високий", менше 0,7 і більше 0,3 -

"середній", менше 0,3 - "низький".

Основними цілями системи інформаційної безпеки є забезпечення сталого функціонування підприємства, запобігання загрозам безпеці підприємства, захист законних інтересів клієнтів від незаконних порушень, запобігання розкраданню коштів, розголошенню, втраті, витоку, спотворенню та знищенню приватної інформації, а також забезпечення нормальної виробничої діяльності в усіх підрозділах підприємства. Системи інформаційної безпеки також повинні сприяти підвищенню якості.

Без централізованого контролю всіх компонентів системи інформаційної безпеки, а також засобів збору, аналізу та зберігання інформації про стан системи інформаційної безпеки ефективність системи інформаційної безпеки та роботи менеджера з інформаційної безпеки дуже низька. Адже кожен захід безпеки реалізує певну складову політики безпеки, яка визначається набором параметрів і вимог на рівні підсистем.

Політиці інформаційної безпеки повинні відповідати не тільки окремі підсистеми та заходи безпеки, але й система інформаційної безпеки в цілому. Інструменти моніторингу та управління необхідні в системах інформаційної безпеки для відстеження працездатності компонентів системи, застосованих правил та інших подій. Інструменти моніторингу, аудиту та звітності необхідні для аналізу зібраних даних, формування звітів та прийняття управлінських рішень.

Інформація, що надходить до компанії, проходить різні етапи обробки проти загроз програмної, мережевої та фізичної безпеки, перш ніж вона буде використана співробітниками організації.

За безпеку в першу чергу відповідає системний адміністратор, який налаштовує все програмне та апаратне забезпечення для захисту бізнесу. Все це регулюється правилами компанії, політиками безпеки та посадовими інструкціями. В результаті співробітники отримують захищену інформацію та формуються звіти про події процесів.

Доступ до файлів і каталогів обмежується системним адміністратором,

який надає кожному користувачеві ексклюзивний доступ до відповідних дисків, папок і файлів.

Регулярне сканування робочих станцій та оновлення антивірусних баз. Виявляє і знешкоджує шкідливе програмне забезпечення та усуває джерело зараження. Необхідно встановити, налаштувати і забезпечити функціональність антивірусних інструментів і систем. Для цього антивірусне програмне забезпечення має бути налаштоване на регулярне сканування комп'ютера та оновлення бази даних з сервера.

Наступним заходом щодо підвищення забезпечення рівня інформаційної безпеки підприємства є установка на комп'ютер-сервер мережевого екрану AgnitumOutpostFireWall, який блокує атаки з мережі Інтернет.

До основних переваг використання мережевого екрану Agnitum Outpost FireWall:

- контролює поведінку та взаємодію програм, блокує хакерів і запобігає несанкціонованому зовнішньому та внутрішньому доступу до мережі;
- відстежує поведінку та взаємодію додатків, забезпечує проактивний захист від несанкціонованих дій, блокує трояни, шпигунські програми та всі сучасні хакерські технології для злому комп'ютерів і крадіжки персональних даних;
- ефективний сканер шкідливих програм автоматично виявляє і поміщає в карантин або видаляє віруси, шпигунські програми та інші шкідливі програми;
- вбудований антиспам.

В процесі дослідження рівня інформаційної безпеки в ПрАТ "Кіровоградобленерго" також було проаналізовано рівень захищеності об'єктів комп'ютерної мережі та, як спосіб підвищення цього рівня, проаналізовано захищеність комп'ютерних мереж від внутрішніх та зовнішніх загроз Scanner-VS виконує наступні функції:

- аналіз захищеності мережі або її окремих сегментів від різних зовнішніх і внутрішніх загроз;

- аудит безпеки мережі;
- інвентаризація мережевих ресурсів;
- збір інформації про окремі вузли мережі (zareєстровані користувачі, робочі групи/домени, IP-адреси, сервіси тощо);
- максимізація ймовірності успішної атаки на захищену ціль;
- перевірити стійкість мережі до злому з урахуванням виявлених і усунутих слабких місць;
- автоматичне виявлення мережевих пристроїв, підключених до комп'ютерної мережі;
- отримання залишкової інформації на дисках, підключених до мережевих вузлів (для різних кодувань);
- перевірка мережевих і локальних паролів;
- інвентаризація ресурсів комп'ютерної мережі (вузлів, портів, служб).

Не менш ефективним способом підвищення інформаційної безпеки є використання антиспам-програм. Ці програми передбачають як захист користувачів від спаму, так і технічну підтримку інструментів, що забезпечують цей захист. Захист досягається шляхом позначення небажаних електронних повідомлень, які надходять до поштової скриньки користувача.

Можливе використання програми *antispat* СПАМОЕД, програма дозволяє блокувати спам на комп'ютері. *Spmoed* - це програмне забезпечення для боротьби зі спамом, що забезпечує фільтрацію пошти. Основні принципи роботи програми полягають у тому, що *Spmoed* може видаляти небажану пошту самостійно або в поєднанні з *TheBat*, *Outlook* та іншими поштовими програмами, а також може працювати з невеликими (до 50 поштових скриньок) поштовими серверами.

Використання джерел безперебійного живлення - найнадійніший спосіб запобігти втраті інформації в разі короткочасного відключення електроенергії. Хоча їхні технічні та споживчі характеристики різняться, такі пристрої можуть жити цілу локальну мережу або один комп'ютер протягом часу, достатнього для відновлення живлення або збереження інформації на

магнітних носіях. В іншому випадку використовуються наступні особливості таких пристроїв Комп'ютер отримує сигнал про те, що ДБЖ перейшов на роботу від власної батареї, але час такої автономної роботи обмежений. Після цього комп'ютер вживає заходів для коректного завершення всіх запущених програм і вимикається (команда SHUTDOWN). Більшість джерел безперебійного живлення також діють як стабілізатори напруги, забезпечуючи додатковий захист від стрибків напруги. Багато сучасних мережевих пристроїв (наприклад, сервери, концентратори, мости) мають власні автономні системи електроживлення.

Під час виконання магістерської роботи було проаналізовано систему інформаційної безпеки ПрАТ "Кіровоградобленерго", виявлено недоліки в її функціонуванні та запропоновано заходи з удосконалення.

Впровадження цих заходів забезпечить:

- 1) розмежування прав доступу до інформаційних систем компанії;
- 2) підвищити рівень інформаційної безпеки для кожного користувача та системи в цілому;
- 3) розробити та впровадити політику інформаційної безпеки, спрямовану на захист інформації та пов'язаних з нею ресурсів;
- 4) зменшити обсяг спаму;
- 5) боротися з кібератаками через мережі;
- 6) підвищити рівень захисту робочих станцій.

ВИСНОВКИ

Таким чином, інформаційна безпека в сучасних умовах є невід'ємною частиною системи економічної безпеки компанії. У свою чергу, надійний захист інформації є фундаментальною умовою переходу не тільки окремих підприємств, а й національної економіки в цілому до моделі сталого розвитку. На нашу думку, особливу увагу слід приділити практичній реалізації запропонованих заходів щодо забезпечення інформаційної безпеки, які повинні слугувати основою для формування та реалізації інформаційної політики підприємства та захищати інформацію від внутрішніх і зовнішніх загроз.

На практиці інформаційна безпека підприємства включає в себе сукупність напрямів, методів, засобів і заходів, спрямованих на зниження вразливості інформації та запобігання несанкціонованому доступу, розголошенню і витоку інформації. Елементами цієї системи є правові, організаційні та інженерно-технічні засоби захисту інформації, основною характеристикою яких є комплексність. Структура системи, склад і зміст її елементів та їх взаємозв'язки залежать від обсягу та цінності інформації, що підлягає захисту, характеру можливих загроз інформаційній безпеці, необхідної надійності захисту та вартості системи.

Не слід забувати, що ключовими гравцями в забезпеченні інформаційної безпеки підприємства є його персонал. Основні заходи, які необхідно вживати по відношенню до співробітників, включають в себе аналітичні процедури найму і звільнення, навчання і інструктаж практичним заходам інформаційної безпеки, контроль за дотриманням вимог інформаційної безпеки і заохочення відповідального ставлення до інформаційної безпеки.

Не менш важливим є питання економічного обґрунтування витрат на інформаційну безпеку. Адже чим вищий рівень інформаційної безпеки, тим менші очікувані збитки, але тим більші витрати на захист. Оптимальний розмір витрат на захист - це витрати, які забезпечують рівень захисту, що

дорівнює найменшим сумарним витратам. Вартість втрат визначається двома параметрами: ймовірністю виникнення різних загроз для інформації та цінністю (важливістю) інформації, безпека якої може бути порушена внаслідок різних загроз. Оскільки кількісно оцінити можливий збиток (суму збитків або упущену вигоду), який може спричинити порушення або втрата інформації, що захищається, досить складно, найбільш прийнятним підходом на сьогоднішній день є використання експертних оцінок. На основі експертних оцінок можна отримати статистично достовірну оцінку можливих збитків.

Захист інформаційних ресурсів компанії є одним з найважливіших завдань в умовах зростання внутрішніх і зовнішніх загроз інформаційній безпеці, які можуть безпосередньо впливати на фінансові показники компанії та її ринкову стабільність. Підприємствам необхідно створити ефективну систему управління інформаційною безпекою, щоб підтримувати і розвивати свій бізнес та отримувати конкурентні переваги. З огляду на вищезазначене, можна стверджувати, що в сучасних умовах неможливо забезпечити економічну безпеку інформаційного середовища компанії без належного захисту.

Аналіз стану інформаційної безпеки на підприємстві ПрАТ "Кіровоградобленерго" дозволив виявити наступні загрози:

1. передача комп'ютерних вірусів через знімні носії інформації, комп'ютерні мережі та Інтернет;
2. помилки персоналу, тобто неправильне введення або зміна даних;
3. внутрішні збої інформаційних систем, тобто програмні або апаратні збої чи пошкодження обладнання;
4. загрози технічного характеру;
5. загрози нетехнічного або некомп'ютеризованого характеру - відсутність паролів, зберігання конфіденційної інформації про інформаційну систему на папері;
6. несанкціонований доступ до інформації (використання ресурсів без

попереднього дозволу). Сюди входить: несанкціонований перегляд інформації; несанкціонована модифікація інформації; несанкціоноване знищення інформації;

7. крадіжка програмного забезпечення, обладнання тощо.

Заходи, яких слід вжити для запобігання цим загрозам, є наступними:

- часто вводити та змінювати паролі.
- використання методів шифрування для захисту інформації.

Заходи щодо запобігання цим загрозам включають в себе:

- встановлення антивірусних програм;
- резервне копіювання даних на знімні носії, щоб у разі збою системи можна було швидко відновити втрачені дані;
- встановлення аварійного джерела безперебійного живлення;
- живлення повинно здійснюватися щонайменше від двох незалежних ліній електропередач;
- розмежування доступу до файлів, каталогів і дисків.

Доступ до файлів і каталогів повинен бути обмежений системним адміністратором, який повинен санкціонувати доступ до відповідних дисків, папок і файлів для кожного користувача.

Він регулярно сканує робочі станції та оновлює антивірусну базу. Це дозволяє виявити і знешкодити шкідливе програмне забезпечення та усунути причину зараження. Антивірусні інструменти та системи повинні бути встановлені, налаштовані та надійно функціонувати. Для цього антивірусне програмне забезпечення має бути налаштоване на регулярне сканування комп'ютера та оновлення бази даних з сервера.

Наступним заходом щодо підвищення забезпечення рівня інформаційної безпеки підприємства є установка на комп'ютер-сервер мережевого екрану Agnitum Outpost FireWall, який блокує атаки з мережі Інтернет. До основних переваг використання мережевого екрану Agnitum Outpost FireWall:

- NativeSecurity контролює поведінку та взаємодію програм, блокує хакерів і запобігає несанкціонованому зовнішньому та внутрішньому доступу

до мережі;

- NativeSecurity відстежує поведінку та взаємодію додатків, забезпечує проактивний захист від несанкціонованих дій, блокує трояни, шпигунські програми та всі сучасні хакерські технології для злому комп'ютерів і крадіжки персональних даних;

- ефективний сканер шкідливих програм автоматично виявляє і поміщає в карантин або видаляє віруси, шпигунські програми та інші шкідливі програми;

- будований антиспам.

В процесі дослідження рівня інформаційної безпеки в ПрАТ "Кіровоградобленерго" також було проаналізовано рівень захищеності об'єктів комп'ютерної мережі та, як спосіб підвищення цього рівня, проаналізовано захищеність комп'ютерних мереж від внутрішніх та зовнішніх загроз Scanner-VS виконує наступні функції:

- 1) аналіз захищеності мережі або її окремих сегментів від різних зовнішніх і внутрішніх загроз;

- 2) аудит безпеки мережі;

- 3) інвентаризація мережевих ресурсів - збір інформації про окремі вузли мережі (zareestrovani korystuvachi, robochi grupy/domeni, IP-adresi, servisi tocho);

- 4) максимізація ймовірності успішної атаки на захищену ціль;

- 5) перевірити стійкість мережі до злому з урахуванням виявлених і усунутих слабких місць;

- 6) автоматичне виявлення мережевих пристроїв, підключених до комп'ютерної мережі;

- 7) отримання залишкової інформації на дисках, підключених до мережевих вузлів (для різних кодувань);

- 8) перевірка мережевих і локальних паролів;

- 9) інвентаризація ресурсів комп'ютерної мережі (вузлів, портів, служб).

Не менш ефективним способом підвищення інформаційної безпеки є

використання антиспам-програм. Ці програми передбачають як захист користувачів від спаму, так і технічну підтримку інструментів, що забезпечують цей захист. Захист досягається шляхом позначення небажаних електронних повідомлень, які надходять до поштової скриньки користувача.

Крім того, користувачі можуть використовувати антиспам-програму SpamoeD, яка може блокувати спам на їхніх комп'ютерах. SpamoeD - це антиспам-програма, яка забезпечує фільтрацію електронної пошти. Основний принцип роботи програми полягає в тому, що SpamoeD працює з невеликим (до 50 поштових скриньок) поштовим сервером, таким як TheBat, Outlook та іншими поштовими програмами, які можуть видаляти небажані для користувача електронні листи.

Використання джерел безперебійного живлення є найнадійнішим способом запобігти втраті інформації в разі короткочасного відключення електроенергії. Хоча їхні технічні та споживчі характеристики можуть відрізнятися, такі пристрої можуть жити цілу локальну мережу або один комп'ютер протягом часу, достатнього для відновлення живлення або збереження інформації на магнітних носіях. В іншому випадку використовуються наступні особливості таких пристроїв. Комп'ютер отримує сигнал про те, що ДБЖ перейшов на роботу від власної батареї, але тривалість такої автономної роботи обмежена. Після цього комп'ютер вживає заходів для коректного завершення всіх запущених програм і вимикається (команда SHUTDOWN). Більшість джерел безперебійного живлення також діють як стабілізатори напруги, забезпечуючи додатковий захист від стрибків напруги. Багато сучасних мережевих пристроїв, таких як сервери, концентратори та мости, мають власні системи автономного живлення.

Під час виконання магістерської роботи було проведено аналіз засобів захисту інформації, корпоративних інформаційних ресурсів та загроз інформаційної безпеки ПрАТ "Кіровоградобленерго" та виявлено відповідні недоліки. На основі виявлених недоліків рекомендуються заходи щодо їх усунення, які підвищують ефективність заходів безпеки компанії та знижують

ризик втрати інформації або корупції. Слід зазначити, що ефективність цих заходів можлива лише завдяки спільним зусиллям персоналу, програмно-технічних засобів та засобів захисту інформації.

На досліджуваному підприємстві, ПрАТ "Кіровоградобленерго", циркулює велика кількість конфіденційної інформації, доступ до якої має бути обмежений. Тому, хоча компанія розробила систему захисту інформації, яка мінімізує загрозу витоку конфіденційної інформації, слід підкреслити, що жодне апаратне, програмне чи інше рішення не може гарантувати абсолютну надійність і безпеку даних в комп'ютерних мережах. У той же час, тільки комплексний підхід до забезпечення безпеки може мінімізувати ризик втрат.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Баранов А. Інформаційний сувереніт та інформаційна безпека? / А. Баранов // *Національна безпека та оборона*. – 2011. – № 1. – С. 70-76.
2. Гуцу С.Ф. Правові основи інформаційної діяльності: навчальний посібник / С.Ф. Гуцу. – Х.: Нац. аерокосм. ун-т «Харк. авіац. ін-т», 2019. – 48 с.
3. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. – НД ТЗІ 1.1-002-99, ДСТСЗІ СБУ України, Київ, 1998.
4. Закон України «Про інформацію» від 02.10.92, № 2658-ХІІ.
5. Закон України «Про захист інформації в автоматизованих системах» від 05.07.94, № 80/94.
6. Закон України «Про державну таємницю» від 21.01.94, № 3855-ХІІ.
7. Інформаційне законодавство: зб. законодавчих актів у 6 т. / за заг. ред. Ю.С. Шемшученка, К.С. Чижа. – Т. 5: Міжнародно-правові акти в інформаційній сфері. – К.: Юридична думка, 2015. – 328 с.
8. Кормич Б.А. Організаційно-правові засади політики інформаційної безпеки України: Монографія / Б.А. Кормич. – Одеса: Юридична література, 2013. – 472 с.
9. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.- НД ТЗІ 2.2-004-99, ДСТСЗІ СБУ України, Київ, 2014.
10. Концепція інформаційної безпеки України. URL: [http://mip.gov.ua/files/banners/Final%20Проект%20концепції%20\(Текст\)%20-%2030.09.15.pdf](http://mip.gov.ua/files/banners/Final%20Проект%20концепції%20(Текст)%20-%2030.09.15.pdf).
11. Кравченко М.О., Бояринова К.О., Копішинська К.О. (2021). Управління ризиками. Навчальний наочний посібник. Київ : КПП ім. Ігоря Сікорського, 2021. 432 с.
12. Кравчук П. Я. Сутність та передумови виникнення поняття

корпоративної безпеки підприємства. Науковий вісник Волинського держ. Ун-ту ім. Лесі Українки. № 1. С.165–170.

13. Марущак А. І. Інформаційно-правові напрями дослідження проблем інформаційної безпеки // *Державна безпека України* / А.І. Марущак. – 2011. – № 21. – С. 92–95.

14. Організаційно-правові основи захисту інформації з обмеженим доступом: Навч. посібник / А. Б.Стоцький, А. М. Гуз, А. І. Марущак та ін.; За заг. ред. В. С. Сідака – К.: Вид-во Європ. ун-ту, 2006. – 232 с.

15. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 31 травня 2005 р. // Відомості Верховної Ради України. – 2005. – № 26. – Ст. 286.

16. Про електронні комунікації : Закон України від 16.12.2020 р. № 1089-IX: станом на 1 берез. 2023 р. URL: <https://zakon.rada.gov.ua/laws/show/1089-20#Text>

17. Про Стратегію національної безпеки України: Указ Президента України від 12 лютого 2007 року № 105/200 // Офіційний вісник України. – 2007. – № 11. – Ст. 389.

18. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26.08.2021р. № 447.URL: <https://zakon.rada.gov.ua/go/n0055525-21>

19. Проценко П. П. Проблематика переходу до інформаційного суспільства // Політ. менеджмент. – 2014. – № 6 (9). – С. 129–137.

20. Смолев Є. С. Дослідження шляхів та розроблення рекомендацій щодо підвищення можливостей виявлення загроз корпоративній інформаційній системі

21. Сороківська О. А., Гевко Л. В, Інформаційна безпека підприємства: нові загрози та перспективи. *Вісник Хмельницького нац. ун-ту*. 2010. № 2, т. 2. С. 32–35.

22. Степанов В. Ю. Інформаційна безпека як складова державної

інформаційної політики. Державне будівництво. 2016. № 2. С. 19.

23. Технології захисту інформації. URL: <https://www.uzhnu.edu.ua/uk/infocentre/get/4186>

24. Сороківська О.А. Інформаційна безпека підприємства: нові загрози та перспективи [Електронний ресурс] /Режим доступу:http://nbuv.gov.ua/portal/Soc_Gum/Vchnu_ekon/2010_2_2/032-035.pdf.

25. Тацюра М.Ю. Проблемні аспекти стандартизації у галузі інформаційної безпеки підприємства // Матеріали Другої наук.-практ.конф. «Сталий розвиток та екологічна безпека суспільства в економічних трансформаціях» 23-24 вересня 2013 р. м. Бахчисарай, НДІ сталогорозвитку та природокористування, РВПС України НАН України, Кримський інститут КНЕУ ім. Вадима Гетьмана / М.Ю. Тацюра. – Сімферополь: Фенікс, 2013. – С. 451–453

26. Функції системи захисту інформації і кібербезпеки критичної інформаційної інфраструктури / Ю. І. Хлапонін та ін. Кібербезпека: освіта, наука, техніка. 2022. Т. 3, № 15. С. 124–134. URL: <https://doi.org/10.28925/2663-4023.2022.15.124134>

27. Фурашев В.М. Питання законодавчого визначення понятійно-категорійного апарату у сфері інформаційної безпеки / В.М. Фурашев // Інформація і право: науковий журнал. – К.: НДЦПІ НАПрН України, 2012. – № 1(4). – С.46– 56.

28. Харченко Л.С. Інформаційна безпека України: Глосарій / Л.С. Харченко, В.А. Ліпкан, О.В. Логінов. – К.: Текст, 2014. – 136 с.

29. . Юдін О. К., Корченко О. Г., Конахович Г. Ф. Захист інформації в мережах передачі даних: Підручник. – К.: Вид-во ТОВ «НВП» ІНТЕРСЕРВІС», 2009. – 716 с.

30. 2015 Global Cybersecurity Status Repor. (2015, January). ISACA International. Retrieved from https://www.isaca.org/cyber/Documents/2015-Global-Cybersecurity-StatusReport-Data-Sheet_mkt_Eng_0115.pdf

31. Abe, S. et al. (2016) ‘Security Threats of Internet-reachable Industrial

Control System (ICS)', in Society of Instrument and Control Engineers of Japan (SICE) Annual Conference 2016. Tsukuba: IEEE Xplore, pp. 750–755.

32. Cisco 2016. Annual Security Report. (2016). Cisco. Retrieved from <http://signalpartners.fi/wpcontent/uploads/2016/01/Cisco-securityreport-2016.pdf>

33. DaVeiga, A. and Eloff, J.H.P. (2010) "A framework and assessment instrument for Information Security Culture", *Computers & Security*, Vol. 29, No. 2010.

34. David Kushner, "The Real Story of Stuxnet". *IEEE Spectrum*, March 2013. IT best of breed. IT Best of Breed. URL: <http://i.crn.com>.

35. Hitt M. Strategic management: competitiveness & globalization. Concepts and cases / Michael Hitt. – Boston: Cengage Learning, 2017. – 743 p

36. Human factor security: evaluating the cybersecurity capacity of the industrial workforce Ani, Uchenna Daniel; He, Hongmei; Tiwari, Ashutosh *Journal of Systems and Information Technology*, Volume 21, Number 1, 2019, pp. 2-35(34).

37. Macrae I. High potential: how to spot, manage and develop talented people at work / I. Macrae, A. Furnham, M. Reed. – London: Bloomsbury, 2018. – 342 p.

38. Parsons, K. et al. (2014) 'Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)', *Computers and Security*. Elsevier Ltd, 42, pp. 165–176.

39. Schneider B. Organizational Climate and Culture: Reflections on the History of the Constructs in JAP. California, 2017. 49 p. URL: <https://psycnet.apa.org/doiLanding?doi=10.1037%2Fap10000090>

40. Sharkey L. The future-proof workplace: six strategies to accelerate talent development, reshape your culture, and succeed with purpose / L. Sharkey. – United States: John Wiley & Sons Inc, 2017. – 240 p.

41. <https://kiroe.com.ua/dlya-aktsioneriv-ta-stejkholderiv/> Офіційний сайт ПрАТ «Кіровоградобленерго»