

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ ІМЕНІ
ВАДИМА ГЕТЬМАНА

Навчально-науковий інститут «Інститут інформаційних технологій в економіці»

Кафедра системного аналізу та кібербезпеки

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «СИСТЕМНИЙ АНАЛІЗ»

Галузь знань 12 «Інформаційні технології»

Спеціальність 124 «Системний аналіз»

Форма навчання: очна (денна)

КВАЛІФІКАЦІЙНА БАКАЛАВРСЬКА РОБОТА

на тему « Системний аналіз управління інформаційною безпекою підприємства
(на прикладі ТОВ «Сучасні технології будівництва 2016»)»

здобувача Рудухи В'ячеслава Віталійовича

(підпис)

Науковий керівник к.е.н. доцент Корзаченко О.В.

(підпис)

Робота допущена до захисту перед екзаменаційною комісією
з атестації здобувачів вищої освіти (ЕК)

Завідувач кафедри: д.ф.-м.н., проф. Джалладова І.А.

(підпис)

Київ 2024

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАДИМА ГЕТЬМАНА

Навчально-науковий інститут «Інститут інформаційних технологій в економіці»

Кафедра системного аналізу та кібербезпеки

ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА «СИСТЕМНИЙ АНАЛІЗ»
СПЕЦІАЛЬНІСТЬ 124 «СИСТЕМНИЙ АНАЛІЗ»

ПОГОДЖЕНО

Керівник проектної групи (гарант)
освітньо-професійної програми
д.ф.-м.н., проф. Галіцин В.К.

(підпис)

_____ 2024 р.

ЗАТВЕРДЖУЮ

Завідувач кафедри системного аналізу та
кібербезпеки
д.ф.-м.н., проф. Джалладова І.А.

(підпис)

_____ 2024 р.

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ

здобувачу вищої освіти **Рудусі В'ячеславу Віталійовичу**
очної (денної) форми навчання
на підготовку кваліфікаційної бакалаврської роботи

на тему « Системний аналіз управління інформаційною безпекою підприємства (на прикладі ТОВ «Сучасні технології будівництва 2016»)»

Тему затверджено наказом ректора Університету від " _____ " _____ 2024 р. № _____

Кваліфікаційна бакалаврська робота виконується на матеріалах ТОВ «Сучасні технології будівництва 2016 »

План кваліфікаційної бакалаврської роботи

Розділ 1	Теоретичні засади формування і захисту інформаційних ресурсів підприємства
Розділ 2	Системний аналіз важелів управління інформаційною безпекою підприємства
Розділ 3	Механізм управління захистом інформаційних ресурсів підприємства

Об'єкт дослідження:	Інформаційні ресурси підприємства та процеси їх захисту
Предмет дослідження:	Методи та засоби управління інформаційною безпекою підприємства
Мета кваліфікаційної бакалаврської роботи:	Розробка ефективного механізму управління захистом інформаційних ресурсів підприємства

Конкретні завдання, які здобувач повинен виконати для досягнення поставленої мети:

У розділі 1	Провести системний аналіз економічної діяльності підприємства
	Оцінити вартість інформаційних ресурсів підприємства
	Визначити основні напрями управління інформаційною безпекою

У розділі 2	Проаналізувати уразливості та загрози інформаційної системи підприємства
	Оцінити можливі ризики інформаційної безпеки підприємства
	Запропонувати шляхи підвищення рівня інформаційної безпеки

У розділі 3	Розробити концепцію створення системи управління інформаційною безпекою
	Формування системи показників та підходу для оцінювання захищеності інформаційних ресурсів

**Завдання підготував
науковий керівник**

(підпис)

Корзаченко О.В.

(ініціали, прізвище)

«_____» _____ 2024 р.

**Завдання одержав
здобувач**

(підпис)

Рудуха В.В.

(ініціали, прізвище)

«_____» _____ 2024 р.

Реферат

Кваліфікаційна бакалаврська робота містить 79 сторінок, 19 таблиць, 8 рисунків, список використаних джерел з 17 найменувань, додатки.

« Системний аналіз управління інформаційною безпекою підприємства (на прикладі ТОВ «Сучасні технології будівництва 2016»)»

Об'єкт дослідження: інформаційні ресурси підприємства та процеси їх захисту.

Предмет дослідження: методи та засоби управління інформаційною безпекою підприємства.

Мета роботи: розробка ефективного механізму управління захистом інформаційних ресурсів підприємства.

Відповідно до поставленої мети були визначені такі *завдання*:

- провести системний аналіз економічної діяльності підприємства;
- оцінити вартість інформаційних ресурсів підприємства;
- визначити основні напрями управління інформаційною безпекою;
- проаналізувати уразливості та загрози інформаційної системи підприємства;
- оцінити можливі ризики інформаційної безпеки підприємства;
- запропонувати шляхи підвищення рівня інформаційної безпеки;
- розробити концепцію створення системи управління інформаційною безпекою;
- формування системи показників та підходу для оцінювання захищеності інформаційних ресурсів.

Практичне значення отриманих результатів. Теоретичні та методологічні підходи до оцінки вартості інформаційних ресурсів та ризиків інформаційної безпеки, розроблені в цьому дослідженні, можуть бути застосовані на практиці для покращення управління інформаційною безпекою підприємств. Для ТОВ «СТБ 2016» це означає зниження ризику витоку інформації та забезпечення стабільної роботи інформаційних систем.

Ключові слова: інформаційні ресурси, інформаційна безпека, системний аналіз, управління ризиками, захист даних.

В і д г у к

про кваліфікаційну бакалаврську роботу
здобувача навчально-наукового інституту
«Інститут інформаційних технологій в економіці»
освітньо-професійної програми «Системний аналіз»

Рудухи В.В.

на тему « Системний аналіз управління інформаційною безпекою підприємства
(на прикладі ТОВ «Сучасні технології будівництва 2016»)»

Нині інформаційна безпека є необхідною умовою успішного функціонування все більшої кількості підприємств. Щоб зберегти бізнес, розвиватися і бути конкурентоспроможним підприємством, необхідно створювати ефективну систему управління інформаційною безпекою. Оскільки сучасні системи забезпечення інформаційної безпеки підприємства, як досить складні організаційно-технічні системи, функціонують в умовах невизначеності стану зовнішнього і внутрішнього інформаційного середовища, управління такими системами мають ґрунтуватися тільки на результатах застосуванні системного аналізу. Це й обумовлює актуальність теми кваліфікаційної бакалаврської роботи Рудухи В.В.

Структура роботи та викладення матеріалу характеризуються логічністю та послідовністю. Вимоги до написання кожного розділу дотримані. На особливу увагу заслуговує комплексне дослідження теоретичних засад формування і захисту інформаційних ресурсів підприємства, аналіз вразливостей і загроз для інформаційної системи, а також аналіз ризиків інформаційної безпеки підприємства в цілому. Обґрунтовано можливість застосування існуючих методичних підходів до оцінювання рівня підтримування інформаційної безпеки підприємства та визначено доцільність використання методів математичного моделювання та доречність застосування загальних принципів економічного оцінювання визначення ціни і витрат на створення й експлуатацію комплексної системи захисту інформації. Позитивною рисою кваліфікаційної бакалаврської роботи є практична реалізація дослідження на прикладі діяльності ТОВ «СТБ 2016».

Робота містить самостійні розробки, а саме сформовано методологічну платформу формування та управління інформаційною безпекою підприємства ТОВ «СТБ 2016». З метою уточнення впливу чинників зовнішнього середовища на інформаційну безпеку компанії, запропоновано підхід оцінювання впливу на базі кількісних методів.

Результати дослідження обумовлюють практичну значимість роботи, що полягає у можливості застосування власних розробок підприємствами різних сфер діяльності для управління інформаційною безпекою та до вартісного оцінювання інформаційних ресурсів з метою запобігання шкоди інформаційній безпеці.

Суттєвих недоліків не встановлено. Студент добросовісно працював та виконувала всі рекомендації наукового керівника.

Кваліфікаційна бакалаврська робота в цілому відповідає вимогам, заслуговує високої оцінки і допускається до захисту перед ЕК, а її автору Рудусі В.В. може бути присвоєний ступінь бакалавра системного аналізу.

Науковий керівник

доцент кафедри системного аналізу та кібербезпеки,
доцент, кандидат економічних наук

Корзаченко О.В.

«10» червня 2024 р.

Рецензія

на кваліфікаційну бакалаврську роботу здобувача
Інституту інформаційних технологій в економіці
Київського національного економічного університету імені
Вадима Гетьмана Рудухи В'ячеслава Віталійовичка
на тему : «Системний аналіз управління інформаційною безпекою
підприємства на прикладі ТОВ «Сучасні технології будівництва 2016»

Актуальність теми роботи пов'язана із зростанням ролі інформаційної безпеки в нарощуванні конкурентних переваг в умовах повномасштабного вторгнення російської федерації в Україну. Забезпечення інформаційної безпеки підприємства дозволяє не лише зберегти дані, але й запобігти можливим фінансовим втратам, але зберегти репутацію та довіру клієнтів. Особливо це актуально для компанії, що активно використовують інформаційні системи у своїх зовнішніх економічних стратегіях зокрема в контексті виходу на ринок Європейського Союзу.

Оцінюючи бакалаврську роботу Рудухи В.В.

в цілому, варзтл зазнати її логічну обґрунтованість. В першому розділі обґрунтовані теоретичні засади формування і захисту інформаційних ресурсів підприємства з урахуванням сучасних інструментів інформаційної безпеки. В другому розділі проведено ґрунтовий аналіз важелів управління інформаційною безпекою ТОВ «Сучасні технології будівництва 2016»

В заключному розділі обґрунтовані напрями удосконалення системи напрями удосконалення системи управління захистом інформаційної безпеки підприємства.

Но стосується з одного боку інстрментальних комплексів управління безпекою ТОВ «Сучасні технології будівництва 2016»

Висновком і пропозиції бакалаврської роботи є обґрунтованими і будуть і будуть виконані в діяльності ТОВ «Сучасні технології будівництва 2016» у розробці заходів що до нарощування міжнародної стратегії компанії на думку Європейського союзу.

В цілому кваліфікаційна бакалаврська робота Рудухи В.В. відповідає встановленим вимогам і заслуговує високої оцінки

Директор ТОВ «Сучасні технології будівництва 2016» Магістр ділового адміністрування

Кузьменко О.М.

ЗМІСТ

ВСТУП	3
РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ФОРМУВАННЯ І ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ПІДПРИЄМСТВА	5
1.1 Системний аналіз економічної діяльності підприємства	5
1.2 Оцінювання вартості інформаційних ресурсів підприємства	24
1.3 Основні напрями управління інформаційною безпекою підприємства	32
РОЗДІЛ 2. СИСТЕМНИЙ АНАЛІЗ ВАЖЕЛІВ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА	42
2.1 Аналіз уразливостей і загроз інформаційної системи підприємства	42
2.2 Аналіз можливих ризиків інформаційної безпеки підприємства	47
2.3 Шляхи підвищення рівня інформаційної безпеки підприємства	50
РОЗДІЛ 3. МЕХАНІЗМ УПРАВЛІННЯ ЗАХИСТОМ ІНФОРМАЦІЙНИХ РЕСУРСІВ ПІДПРИЄМСТВА	69
3.1 Концепція створення системи управління інформаційною безпекою компанії ТОВ «СТБ 2016»	69
3.2 Економічні та інші показники захищеності інформаційних ресурсів	75
ВИСНОВКИ	80
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	82
ДОДАТКИ	

ВСТУП

Актуальність теми. У сучасному світі інформаційні ресурси підприємства стають однією з ключових складових його успіху та конкурентоспроможності. З огляду на швидкий розвиток технологій та зростання кількості кіберзагроз, питання формування і захисту інформаційних ресурсів набувають особливої актуальності. Забезпечення інформаційної безпеки підприємства дозволяє не лише зберегти важливі дані, але й запобігти можливим фінансовим втратам, зберегти репутацію та довіру клієнтів. Особливо актуально це для компаній, таких як ТОВ «СТБ 2016», що активно використовують інформаційні системи у своїй діяльності.

Аналіз останніх досліджень і публікацій. Проблеми інформаційної безпеки досліджувалися багатьма вченими та фахівцями у сфері інформаційних технологій. Серед них слід виділити праці таких авторів, як Джон Сміт, який аналізував моделі захисту інформаційних систем, та Анна Джонс, яка досліджувала економічні аспекти управління інформаційною безпекою. Крім того, значний внесок у розвиток цієї тематики внесли роботи Михайла Петрова, що зосереджувалися на оцінці вартості інформаційних ресурсів, та Олени Коваленко, яка розробляла методології оцінки ризиків інформаційної безпеки.

Мета дослідження полягає у розробці ефективного механізму управління захистом інформаційних ресурсів підприємства.

Завдання дослідження:

1. Провести системний аналіз економічної діяльності підприємства.
2. Оцінити вартість інформаційних ресурсів підприємства.
3. Визначити основні напрями управління інформаційною безпекою.
4. Проаналізувати уразливості та загрози інформаційної системи підприємства.
5. Оцінити можливі ризики інформаційної безпеки підприємства.
6. Запропонувати шляхи підвищення рівня інформаційної безпеки.
7. Розробити концепцію створення системи управління інформаційною безпекою.

8. Формування системи показників та підходу для оцінювання захищеності інформаційних ресурсів.

Об'єктом дослідження є інформаційні ресурси підприємства та процеси їх захисту.

Предметом дослідження є методи та засоби управління інформаційною безпекою підприємства.

Методи дослідження. У процесі дослідження застосовувались такі методи: системний аналіз, методи економічного моделювання, методи оцінки ризиків, а також методи аналізу загроз та уразливостей.

Теоретична, методична та практична значущість отриманих результатів. Теоретична значущість дослідження полягає у розвитку наукових уявлень про механізми управління інформаційною безпекою підприємств. Методична значущість полягає у розробці нових підходів до оцінки вартості інформаційних ресурсів та ризиків інформаційної безпеки.

Практична значущість полягає у впровадженні запропонованих методів і моделей у реальну практику управління підприємствами, що дозволить підвищити рівень їх інформаційної безпеки. Для ТОВ «СТБ 2016» це означає можливість знизити ризики витоку інформації та забезпечити стабільну роботу інформаційних систем.

Інформаційна база дослідження. Інформаційною базою дослідження стали наукові праці з питань інформаційної безпеки, офіційні документи та звіти підприємств, статистичні дані, а також результати власних досліджень автора.

РОЗДІЛ 1

ТЕОРЕТИЧНІ ЗАСАДИ ФОРМУВАННЯ І ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ПІДПРИЄМСТВА

1.1 Системний аналіз економічної діяльності підприємства

Сучасне суспільне життя не може існувати без ефективного функціонування будівельної галузі. Будівельна галузь є однією з найважливіших галузей економіки, від якої залежить функціонування всієї економічної системи країни. Важливість цієї галузі в економічній діяльності будь-якої країни можна пояснити наступним чином. Капітальне будівництво створює велику кількість робочих місць і використовує продукцію багатьох галузей економіки. Економічний ефект від розвитку цієї галузі полягає в мультиплікативному ефекті вкладених у будівництво коштів.

Тому що з розвитком будівельної індустрії такі галузі, як виробництво будівельних матеріалів та супутнього обладнання, машинобудування, металургія та металообробка, нафтохімічна промисловість, виробництво скла, деревообробка та фарфоро-фаянсова промисловість, транспорт, енергетика тощо.

Будівельна галузь також сприяє розвитку малого та середнього підприємництва. Розвиток будівельної галузі неминуче призведе до економічного зростання країни та вирішення багатьох соціальних проблем [1].

Наразі про конкурентоспроможність цієї галузі говорити дуже важко. Навіть якщо на регіональному рівні простежується чітка тенденція домінування будівельних організацій центральних регіонів та заможних міст через їхні більші можливості та інвестиційну привабливість, то на світовому рівні українська будівельна галузь суттєво відстає через відсутність . Необхідні фінансові та організаційні зміни [1].

Потенційні споживачі в будівельній галузі, як правило, у віці, коли вони створюють або розширюють сім'ю, тому віддають перевагу лише будинкам найвищої якості та в умовах, придатних для сучасного життя[2].

Отже, потенційні споживачі знаходяться у віковій категорії від 30 до 45 років. Ця група характеризується стабільною зайнятістю та доходом вище середнього.

В умовах ринкової економіки України стрімкий розвиток будівельної галузі створює поштовх для розвитку конкуренції, що дозволяє будівельним компаніям підвищувати якість своїх послуг, чітко дотримуватися прийнятих зобов'язань, розвивати методики та методики постійно вдосконалюватися.

Індивідуальний підхід до клієнтів, пошук нових нестандартних рішень, впровадження нових технологій, використання високоякісних матеріалів. На будівельному ринку Києва субпідрядниками, що надають інжинірингові послуги, є до 150 компаній.

У зв'язку з реформуванням ДАБІ (регулюючого органу, відповідального за управління галуззю) створення нових компаній значно скоротилося. Тому не можна сказати, що конкуренція на ринку значно зросла.

Загальна рентабельність будівельної галузі приблизно на 5% нижча, ніж в інших секторах світової економіки. Будівельна галузь часто займає високі позиції в рейтингах банкрутства в різних регіонах через поєднання низької прибутковості та високого ризику.

Однією з причин такої тенденції є те, що будівельні проекти зазвичай тривають на 20% довше, ніж заплановано, а фактичний бюджет може перевищувати бюджет на 80%, що призводить до судових позовів, незадоволеності клієнтів і складних і тривалих процедур перевірки. Це тому, що є багато випадків [3].

Будівельна галузь стикається з проблемами та викликами всюди. У той же час ці проблеми загострюються в країнах, що розвиваються, на тлі несприятливих макроекономічних умов, спричинених хронічною нестачею ресурсів, інституційною слабкістю та відсутністю внутрішньої пропозиції інноваційних технологій для кваліфікованої робочої сили [4].

Темпи зростання будівельної галузі, особливо ринку інженерних послуг, прямо залежали від рівня внутрішніх і зовнішніх інвестицій. До 2019 року галузь, ймовірно, спостерігатиме та реалізує значне зростання виробництва. Дуже активно велось будівництво житлових комплексів, торгових центрів, комерційних об'єктів. Іноземні інвестиції забезпечили активний розвиток промислових підприємств. Ці компанії були засновані в основному в західному регіоні країни.

З початку пандемії в галузі суттєво впало виробництво. Через нинішню війну в країні ринок стрімко скорочується. Чекаємо, коли почнеться відновлення країни.

Під будівельною галуззю розуміється галузь, що споживає більшу частину природної сировини країни та значну частину продукції багатьох інших галузей. Будівельна галузь споживає 20-32% виробленої в країні сталі, 17-34% алюмінію, 20-25% пластику, 20-25% деревини. Подальший економічний розвиток будівельної галузі в умовах високої енерго- та ресурсоемності потребує збільшення використання сумісної сировини. Особливо це стосується мінеральної сировини та палива. Вони мають значний вплив на зниження витрат на будівництво та є найважливішими факторами в оцінці ступеня консолідації будівельної галузі.

Відомо, що зниження міцності матеріалів конструкції, як за обсягом одиниці будівельної продукції, так і за найменуванням використовуваних матеріалів і виробів, має значний вплив на загальну економіку [5]. будівельні послуги та всі товари (послуги), які пропонуються поділяють на преміальний сегмент, середній клас та економ-клас. Технічні об'єкти можуть бути реалізовані в якісних пристроях або пристроях економічного сегмента.

Вивчаючи економічні фактори макросередовища, можна зрозуміти, як формуються та розподіляються ресурси. Спад в економіці держави значно зменшує здатність організації отримувати фінансування та інші ресурси, необхідні для належного функціонування.

Основні фактори економічного середовища, які вимагають постійної діагностики та оцінки потенційного впливу змін на бізнес, включають: рівень і рівень інфляції, обмінний курс національної валюти по відношенню до валюти; наступні принципи ринкової економіки. Свобода відкриття бізнесу, повна

фінансова незалежність. Використання різних форм власності, передусім приватної власності. Безкоштовні призи. Антимонопольна діяльність [6].

Відкритість внутрішнього ринку (свобода доступу на зовнішні ринки). Форма договору між суб'єктами господарювання. Вибір стратегії і тактики будівельних організацій у новій економічній ситуації визначається такими положеннями: Недостатнє ресурсне забезпечення споживачів будівельної продукції. Зростають ціни на будівельні матеріали, конструкції, енергетичні, транспортні та інші послуги, що призведе до подорожчання будівельно-монтажних робіт, а також підвищення умов будівництва об'єктів, що будуються.

Стратегія управління будівельною компанією залежить від організаційно-правової форми зареєстрованої компанії та від того, як на неї впливає державне регулювання.

У нашому випадку на прийняття бізнес-рішень завжди впливають обставини, які виникають у процесі ведення бізнесу та надання інжинірингових послуг.

Ще раз наголошуємо, що рішення завжди приймаються на користь замовника, і ми прагнемо вирішити будь-які питання. Специфіка реалізації товарів та послуг побудована на співпраці з такими ключовими партнерами, як ТОВ «MERX», ТОВ «МЕТА КАПІТАЛ», ТОВ «БГ МОДУС», ТОВ «СВІТЕКО» ТОВ «KESZ-UA». Підприємство виконує функції субпідрядника на об'єктах наших замовників, що виконують функції генпідряду.

Саме якісне надання послуг оптимально впливає на конкурентоспроможність компанії будівельних послуг. Це наш підхід до постпроектної підтримки наших клієнтів.

Сучасні тенденції ринку будівельних послуг вимагають від компаній наявності кваліфікованого персоналу з великим досвідом роботи в різних сферах економіки [7].

Проте ринкові реалії, що склалися в довоєнній Україні, не дозволяли укомплектувати всі об'єкти сфери обслуговування достатньою кількістю кваліфікованих кадрів. Ось загальна картина: Кілька висококваліфікованих фахівців оточені менш кваліфікованими людьми.

Хоча така структура не є особливо ефективною, вона дозволяє охопити більші сегменти ринку. Екологічне середовище – характеризує природне середовище організації.

До основних екологічних факторів відносяться викиди забруднюючих і токсичних речовин у навколишнє середовище, рівень фізичного впливу на навколишнє середовище, надійність і соціально-екологічна безпека виробничої системи, кількість і якість виробленої продукції, ці фактори детально розглядаються [8].

Зручність у використанні, природні умови навколишнього середовища, розташування підприємства тощо. Робота компанії мало впливає на навколишнє середовище. Як правило, вплив на природні компоненти можна спостерігати лише під час будівельних робіт.

Утилізуються відходи виробництва (картон, кольорові та чорні метали, пластмаси).

Проаналізуємо конкуренцію компанії у сфері будівельних послуг (будівельні роботи, обладнання).

Відповідно до моделі Майкла Портера, на конкуренцію в галузі впливають такі зовнішні фактори:

1. Загроза появи нових конкурентів.
2. Здатність постачальників «диктувати умови».
3. Здатність споживачів «диктувати умови»
4. Загроза появи товарів-замінників.

Для більш детального аналізу конкуренції в галузі розглянемо кожен чинник більш детально.

Що стосується загрози появи нових конкурентів. До початку війни в Україні галузь будівництва та інжинірингу розвивалась досить швидкими темпами. До 2020 року на ринку з'являлись нові гравці. Це було пов'язане з досить не складною процедурою отримання ліцензії та виходу на ринок. Також слід відмітити, що починати роботи на ринку будівельних послуг можна не маючи великого капіталу та ресурсів. Головне - бажання працювати та відповідальність перед замовниками. З моменту реформи ДАБІ все суттєво змінилось. Нових

гравців майже немає. На сьогоднішній день конкуренція, в основному, відбувається у внутрішньому середовищі. Тому можна вважати, що сьогодні не існує загрози з боку нових гравців [9].

Розглянемо загрозу з боку покупців та постачальників, що впливає на конкурентну стратегію на ринку будівельних послуг.

Замовники (покупці) будівельних та інжинірингових послуг в основному сконцентровані в великих містах України. До початку війни в Україні висока концентрація іноземних замовників була сконцентрована в західному регіоні України. Найбільша кількість замовників та будівельних об'єктів зосереджена в Києві. Відповідно підрядні організації концентруються навкруги об'єктів будівництва.

Альтернативними джерелами постачання для замовників є вибір підрядника за допомогою тендерних процедур. Тендерні процедури завжди призводять до зниження вартості послуги. Існує особиста думка та досвід експертів, які вказують на те, що суттєве зниження цінової пропозиції завжди призводить до зниження якості послуги. Фахівці не розділяють сучасні тенденції у виборі підрядника за нижчою ціною. Але на сьогоднішній день більшість замовників рухаються цим шляхом [9].

Розглядаючи структуру цінової пропозиції будівельної послуги можна сказати, що матеріалоемність складає 60 відсотків від загальної послуги. Гравці, що намагаються блефувати при наданні комерційної пропозиції закладають матеріали більш низької якості не доводячи цей факт до замовника, помірковано занижують вартість робіт, щоб в процесі виконання «добрати» на додаткових роботах. Інжинірингові послуги практично не мають матеріальної складової тому тут складніше оцінити рівень ціноутворення. В даному сегменті немає безвідповідальних гравців. Тому, той, хто переміг, отримає якісний комерційний результат.

Постачальники, що працюють на ринок будівельних послуг також концентруються в центрах розподілення обсягів робіт. Найбільш великі гравці ринку зосереджені в великих містах та промислових хабах. Розглядаючи досвід роботи з постачальниками слід сказати, що на початковому етапі налагодження

зв'язків кожен намагається бути кращим, оперативним та надавати усілякі преференції. З часом такий підхід змінюється на загальний, той що не викликає захвату від співробітництва.

Питання заміни постачальника продукції на іншого не є проблемою. Якщо розглядати, наприклад, Київ, то маємо таку кількість постачальників продукції для будівництва, що підприємству не складно вирішити питання заміни у випадку зниження надійності співробітництва. При цьому це ніяк не впливає на фінансову і господарську діяльність підприємства. Загалом, всі постачальники надають майже однакові умови.

В умовах сучасного ринку інжинірингових послуг постачальник не може диктувати умови покупцю. Така тенденція зберігається на всіх етапах взаємовідносин. Сьогодення сформувало такий тип взаємовідносин, що у всіх випадках постачальник бореться за покупця[10].

Не можна замінювати інженерні показники та показники організації будівництва іншими показниками. Тому ризику конфлікту в цьому випадку немає.

Зростання споживчого попиту на будівельному ринку свідчить про посилення конкуренції між компаніями, наприклад, швидший час реагування на інноваційні технологічні зміни, що впливає на покращення конкурентних переваг компаній.

Зміцнення конкурентних позицій підприємства на сучасних ринках неможливе без розробки стратегій управління конкуренцією, в основі яких лежать комплексні механізми досягнення переваги підприємства над конкурентами.

Головною метою підвищення конкурентоспроможності компанії є суттєве підвищення прибутковості та мінімізація витрат. Реалізація цього принципу стає можливою завдяки раціональному розподілу прав і обов'язків між структурними підрозділами підприємства[11].

Поліпшення фінансових результатів залежить від побудови відносин з посередниками, вибору економічно ефективних стратегій, впровадження інноваційних технологій у корпоративну діяльність, вжиття заходів щодо оптимізації ведення господарської діяльності (при низьких витратах).

Підвищення конкурентних позицій на ринку будівельних послуг характеризує стратегічне управління конкурентоспроможністю та розробку організаційно-економічних моделей, спрямованих на комплексні механізми досягнення конкурентних переваг.

Зовнішні та внутрішні фактори впливають на конкурентне зростання цієї компанії. Зовнішні фактори - це фактори, на які компанія не може вплинути, тоді як внутрішні фактори залежать від компанії.

Зовнішніми факторами є [13]:

- постійні зміни в законодавчій базі;
- рівень ринкових цін на матеріали;
- зниження платоспроможності населення;
- форс-мажорні обставини.

Внутрішніми факторами є [13]:

- раціоналізація використання основних засобів, матеріалів, фінансових ресурсів;
- підвищення рівня організації праці;
- впровадження інноваційних технологій у виробничу діяльність;

Таким чином для досліджуємого підприємства в пріоритеті стає питання підвищення ефективності діяльності за рахунок використання внутрішніх резервів: організаційних, фінансових, трудових, матеріальних.

Проаналізуємо конкуренцію в галузі (конкурентні позиції) за допомогою карти стратегічних груп (рисунок 1).

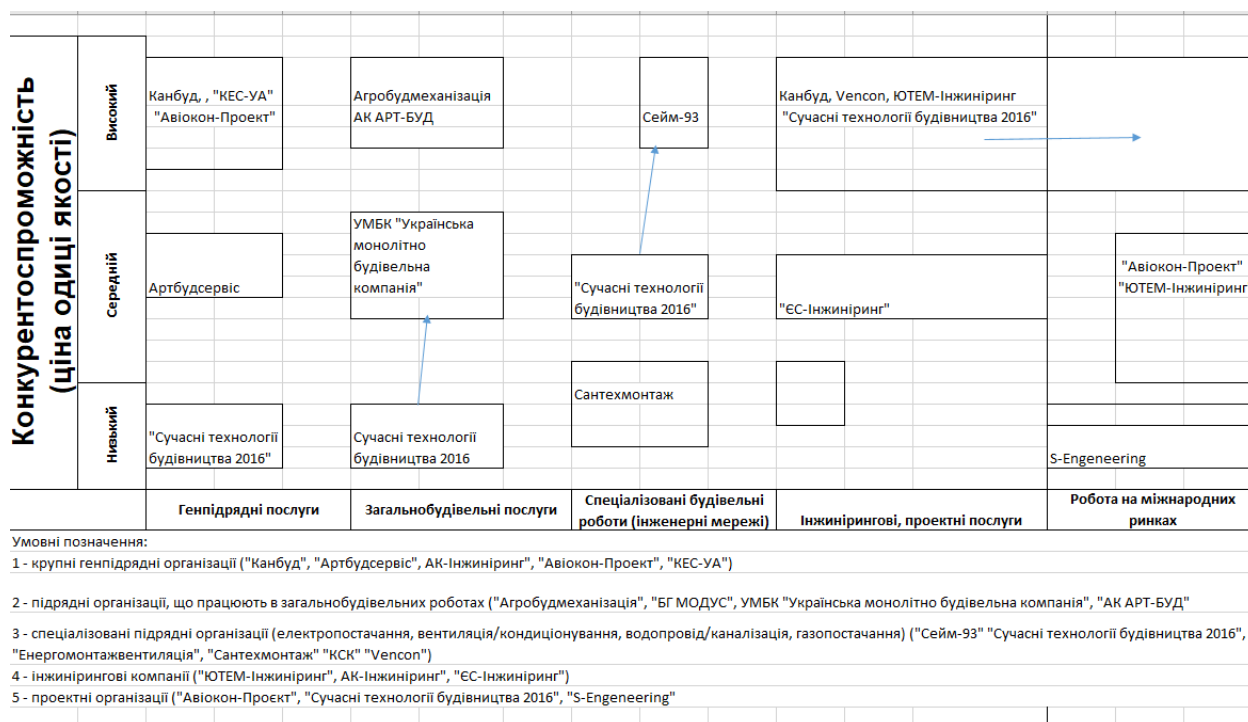


Рисунок 1.1 – Карта стратегічних груп

Джерело: розроблено автором на основі [13]

На підставі сформованої карти бачимо, що сформовано низку конкурентних груп, які конкурують у різних галузях будівельної сфери.

Аналіз поточного стану показує, що компанія не дуже конкурентоспроможна щодо генпідряду та будівельних послуг.

Наша компанія має середню конкурентоспроможність на ринку спеціалізованого будівництва (електрообладнання). Ми маємо високу конкурентоспроможність на ринку в сфері реалізації проектів та інжинірингових послуг.

У всіх сферах діяльності плануються стратегії зміцнення конкурентоспроможності підприємств і переведення їх з нижчого рівня на вищий.

У планах – вивести на міжнародний ринок конкурентоспроможні сервісні роботи (інженерні послуги, проектні роботи).

План полягає в тому, щоб досягти середньої та високої конкурентоспроможності на ринку спеціального будівництва, а потім представити ці послуги на міжнародних ринках.

За результатами аналізу для підвищення конкурентоспроможності ТОВ «Новітні будівельні технології 2016» можуть бути вжиті наступні заходи: - Зміна структури капіталу підприємства за рахунок збільшення частки власних коштів.

Зменшення суми позикових коштів порівняно з власними коштами. Компенсація короткострокової заборгованості шляхом збільшення прибуткових активів. Будь-який тип послуги, який планується отримати конкурентну перевагу, слід проаналізувати, щоб визначити його життєвий цикл.

Це дозволяє формувати ефективну цінову та асортиментну політику, яка впливає на показники діяльності вашої компанії та відповідно впливає на рівні. Йдеться про конкурентоспроможність.

Вищенаведені заходи мають бути вирішальними, покращуючи ефективне використання ресурсного потенціалу, фінансову стійкість, показники прибутковості та конкурентоспроможності підприємства, водночас зосереджуючи зусилля на стратегічному управлінні конкурентоспроможністю.

Для компаній, що надають будівельні послуги, стратегія компанії з низькою заробітною платою є прийнятною з точки зору стратегічного управління конкурентоспроможністю. Ця стратегія має бути спрямована на ціноутворення з урахуванням сучасних реалій цінової політики в будівництві. Розрахунок базової зарплати базується на фактичних витратах на оплату праці.

Організаційно-технологічні інновації дозволяють підвищити продуктивність праці та зберегти трудові ресурси. Розгляньте витрати на експлуатацію машин і обладнання відповідно до фактичних потреб.

Використання програмних комплексів для автоматизації процесу проектування (BIM Engineering). Тому для ТОВ «СТБ 2016» зниження витрат є найефективнішим способом досягнення конкурентних переваг на ринку будівельних та інженерних послуг [14].

У сучасній бізнес-ситуації ТОВ «СТБ 2016» висуває чіткі вимоги щодо поступового підвищення своєї конкурентоспроможності та оперативного

реагування на зміни в бізнес-діяльності з метою підтримки стабільності свого фінансового становища. Надання доказів зовнішніх і внутрішніх факторів є важливим для підвищення конкурентоспроможності компанії.

Завдяки зовнішнім факторам можна буде інвестувати в новітні технології, послуги та розробки в будівельній галузі. Внутрішні фактори дають змогу підвищувати кваліфікаційний рівень працівників, запроваджувати системи економічного стимулювання тощо.

Збалансований розвиток підприємства та покращення його іміджу на ринку потребують поступового впровадження від ТОВ «СТБ 2016». Це соціально відповідальна стратегія, завдяки якій компанії можуть інвестувати в людські ресурси та навколишнє середовище, збільшуючи свою конкурентну перевагу та покращуючи своє фінансове становище.

Сьогодні для ТОВ «СТБ 2016» важливо не тільки посилити свою конкурентоспроможність на українському ринку будівельних послуг та інжинірингової діяльності, а й вивести свою діяльність на міжнародний ринок. Тому ми повинні використовувати новітні матеріали та методи надання послуг, щоб задовольнити потреби нашого унікального ринку.

Здобувши високу репутацію на внутрішньому ринку, ми будемо поступово виходити на закордонні ринки. Аналіз внутрішнього середовища компанії. Дивлячись на те, як функціонує компанія, можна виділити кілька функціональних підсистем, таких як людські ресурси, фінанси, виробництво та інноваційні методи управління.

На мою думку, HR є найбільш складною і фундаментальною підсистемою. За шість років з моменту заснування компанія зросла з трьох до 50 співробітників. У рамках процесу зростання відбувався постійний якісний підбір персоналу.

За два роки діяльності сформувався фундамент колективу. Кризове явище, яке необхідно подолати (пандемія, війна), сильно впливає на кадровий потенціал компанії, але основна команда залишається незмінною.

На сьогоднішній день, не дивлячись на проблеми на ринку надання будівельних послуг, компанія поступово відновлює кадрову структуру підприємства.

Аналізуючи підсистему фінанси можна відмітити, що на сьогоднішній день підприємство не має резервних фондів чи інших накопичень. Кошти, які поступають, спрямовуються на реалізацію проєктів (завдань) замовників, а саме: оплата матеріальної складової, фонд оплати праці, обов'язкові платежі, лізингові платежі. В період призупинення виробничої діяльності (початок пандемії, початок військової агресії) відбувалось використання резервних коштів за для збереження основних активів підприємства.

Не дивлячись на всі складнощі сьогодення згідно з даними управлінського обліку підприємство є прибутковим та виконує всі зобов'язання перед державою, співробітниками, постачальниками, кредиторами.

Виробнича діяльність ТОВ «СТБ 2016» на сьогоднішній день складається з двох основних напрямків [15]:

- виконання монтажних робіт в інженерних мережах на об'єктах будівництва;
- виконання проектних робіт;

Інжинірингова діяльність, виготовлення нестандартизованого щитового обладнання на сьогоднішній день майже не виконується.

До початку кризових подій структура доходів підприємства поділялась наступним чином:

- будівельно – монтажні роботи – 65% обсягів;
- проектні роботи – 15% обсягів;
- виготовлення електрощитового обладнання – 10 %
- інжинірингові послуги – 10%.

В перспективі планується освоєння нових ринків та напрямків діяльності, але сьогодення не дозволяє стратегічно рухатись в заданому напрямку у зв'язку з відсутністю можливості для інвестицій в ресурсний та кадровий потенціали.

До ключових компетенцій підприємства віднесемо наступні:

- якісний підхід до реалізації задач (незважаючи на всі перешкоди, що є на шляху доводиться почата справа до кінця, а саме до результату, який буде задовільняти замовника);

- продуктивність праці персоналу - люди повинні мати можливість підвищувати продуктивність своєї діяльності, повноцінно брати участь у

формуванні доходу і трудитися за грошову винагороду. Економічне зростання є однією зі складових моделей розвитку людського потенціалу;

- рівність. Всі люди повинні мати рівні можливості брати участь у реалізації цих можливостей і користуватися їх благами;

- стійкість. Доступ до можливостей повинен бути забезпечений не тільки нинішнім, а й майбутнім поколінням. Належить забезпечити заповнення всіх форм капіталу - матеріального, людського, екологічного;

- розширення можливостей. Розвиток повинен здійснюватися зусиллями людей, а не тільки в інтересах людей. Люди повинні всіляко брати участь у процесі прийняття рішень та інших процесах, що визначають життя.

Ключовими потенційними загрозами підприємства є проблеми, які можуть виникнути при відсутності достатньої кількості кваліфікованих кадрів. Позиція така, що не можна надавати неякісних послуг тому відсутність кадрів може вдарити по репутації.

Друга ключова загроза – відсутність обсягів робіт. Особливо актуально в сьогодення. Ринок будівельних та інжинірингових послуг переживає не найкращі часи тому вижити тут вдається не кожному. Сьогодні компанія «на плаву» та маємо обсяги робіт, що буде завтра, ніхто не знає.

Основними факторами, що впливають на діяльність підприємства є:

- загальна ситуація на ринку будівельних та інжинірингових послуг;
- рівень економічного розвитку держави (рівень доходів населення);
- державна політика (забезпечення підтримки на всіх етапах розвитку підприємства, у разі необхідності кредитування у певних розмірах;
- наявність основних фондів в необхідній кількості для реалізації робіт;
- вплив діяльності підприємства на екології підприємства;
- інновації в управлінні та виробництві.

SWOT – аналіз.

Складемо матрицю основних параметрів ТОВ «СУЧАСНІ ТЕХНОЛОГІЇ БУДІВНИЦТВА 2016» для проведення SWOT-аналізу. Результати аналізу зведемо в таблицю 1.2.

Таблиця 1.2 – SWOT – аналіз ТОВ «СТБ 2016»

Сильні сторони ТОВ «СТБ 2016» - якісне виконання робіт; - високий рівень відповідальності перед замовниками; - кваліфікований ІТР персонал; - оперативне реагування на запити замовників; - розвинена матеріально-технічна база.	Слабкі сторони ТОВ «СТБ 2016» - відсутність фінансових резервів у підприємства; - вузьке коло замовників; - відсутність можливості мінімізації витрат за рахунок оптимізації виробничих процесів; - відсутність зв'язків в адміністрації міста, районів.
Можливості ТОВ «СТБ 2016» - ринок, який не має кордонів в Україні, а також європейський ринок; - можливість комплектації кваліфікованим кадровим персоналом у зв'язку з війною в Україні; - - можливість економічного зростання у зв'язку зі збільшенням обсягів будівельних робіт на етапі відновлення країни.	Загрози для ТОВ «СТБ 2016» - будь-які економічні коливання, що можуть призвести до невиконання повного обсягу робіт на об'єкті замовника; - фізичний стан (здоров'я співробітників (пандемія, інші захворювання)); - відсутність чіткої політики держави по відношенню до будівельних організацій - недостатній рівень захисту інформаційних ресурсів.

Джерело: за матеріалами підприємства, власна розробка, складено автором

Як бачимо, можливості, що має ТОВ «СТБ 2016» можуть бути реалізовані за рахунок «сильних сторін» та, можливо, за рахунок матеріальної складової на підприємстві. Що мається на увазі? Такі сильні сторони ТОВ «СТБ 2016», як якісне виконання робіт, високий рівень відповідальності перед замовниками, оперативне реагування допоможе підприємству розпочати діяльність на ринку будівельних послуг за кордоном.

Завдяки сильним сторонам компанії, тобто досвіду та підходу до організації роботи, вдається нейтралізувати потенційні загрози, які існують на ринку та для компанії в цілому.

З досвідом і відповідальністю є можливість запобігти негативним явищам, які можуть виникнути в разі нестабільності на ринку (економічні коливання, планування праці, реакція на зміни в політиці галузі). Навпаки, розуміється, що слабкі сторони компанії завадили їй використати надані можливості. Це означає,

що відсутність у компанії фінансових резервів буде перешкоджати її агресивній експансії на європейський ринок. Також можна побачити та зрозуміти, що слабкі сторони компанії посилюють вплив загроз на роботу.

Відсутність фінансових резервів суттєво вплине на загальний стан підприємства у разі виникнення кризового явища, про що йдеться у розділі «Загрози». Найбільший ризик у таких ситуаціях – це закриття бізнесу, від якого постраждають як власники, так і працівники. Які конкретні дії можна вжити для усунення «слабких сторін» бізнесу та мінімізації загроз? До цього часу компанія вирішила накопичити стабілізаційний фонд. П'ять відсотків від суми рахунку буде перераховано на банківський депозитний рахунок. У майбутньому це допоможе мати резервні кошти на випадок кризових явищ та обігові кошти на випадок інвестиційних потреб. Крім того, необхідно знайти велику аудиторію, яка може працювати в плановому режимі з довгостроковим баченням. Це дозволить мінімізувати витрати на організаційні потреби.

Розширити коло клієнтів можливо за рахунок організації рекламних кампаній (Інтернет, соціальні мережі), участі у виставкових заходах, нетворкінгу тощо. За рахунок реалізації заходів з усунення слабких сторін можна зменшити загрозу впливу кризових явищ на роботу підприємства. Постійний моніторинг законодавства дозволить оперативно реагувати на будь-які зміни в державній політиці по відношенню до підприємств галузі.

Маючи якісний кадровий потенціал компанія повинна рухатись у напрямку розвитку підприємства на нових ринках (європейських). Також необхідне проведення стабільної кадрової політики по підбору найкращих кадрів для робітничих підрозділів.

Філософією ТОВ «СУЧАСНІ ТЕХНОЛОГІЇ БУДІВНИЦТВА 2016» є - «сучасний підхід, якісний результат». Компанія цілеспрямована на якість послуги. Всі співробітники націлені на якісне виконання роботи. Ніхто не буде відступати від якісних критеріїв за для мінімізації часу або витрат.

Концепцією підприємства є створення цінностей для замовників у будівельній галузі, галузі надання інжинірингових послуг, проектуванні інженерних мереж. З кожним роком роботи підприємство набуває більше досвіду,

вдосконалює підходи до виконання робіт, опановує новітні технології. На сьогоднішній день активно освоюється BIM – проєктування, як необхідну складову при проєктуванні в недалекому майбутньому.

Завдяки засновникам (власникам) та співробітникам на сьогоднішній день сформований позитивний імідж підприємства. Компанія відома в колі замовників, як відповідальний підрядник, який виконує договірні зобов'язання в повному обсязі. Продуктами що реалізує підприємство є – виконання будівельних послуг, виконання проєктних робіт, надання інжинірингових послуг, виготовлення електрощитового обладнання.

Основними споживачами (клієнтами) підприємства є – крупні забудовники (генпідрядні організації), власники комерційної нерухомості, будівельні організації (дрібний бізнес), генпроектувальні організації, постачальники електротехнічного обладнання.

Основною відмінністю, що відрізняє компанію від конкурентів є особий підхід до виконання робіт та лояльне ставлення до замовника (клієнта). Компанія завжди доводить розпочату справу до кінця навіть якщо це може негативно вплинути на прибутковість підприємства. В основному, спеціалізовані монтажні організації намагаються «вижимати» з замовників максимум. Спочатку демпінгують на розрахунках вартості робіт, потім добирають на додаткових роботах. Ціни в компанії завжди відповідають дійсності. Вона не низька, але є правдивою і дозволяє замовнику вірно розраховувати свої витрати.

Основними галузями, в яких відбувається цілепокладання підприємства є галузі, в яких працює компанія [16].

1. Будівельна галузь:

- В 2023 році розпочати роботи в програмах відновлювальних робіт в Україні. Розширити спектр послуг за рахунок залучених спеціалістів.
- 2023 – 2024 роки вийти на виконання 1 000 000 – 1 500 000 грн. в місяць по основному напрямку (електромонтажні роботи).
- У 2023 році збільшити чисельність робочих до 50 робітників.

2. Галузь проєктування інженерних мереж:

- 2023 рік - виконувати проєктні роботи, які вимагають використання BIM-технологій;
- До кінця 2023 року вийти на рівень виконання по проєктному відділу на 150 000 – 180 000 грн. в місяць
- Початок 2023 року провести додаткове навчання по технологіям BIM для інженерів-проєктувальників.

3. Галузь надання інжинірингових послуг:

- 2023 рік сформувати групу співробітників для забезпечення обслуговування об'єктів замовників;
- 2023 рік рекламувати послугу обслуговування інженерних мереж об'єктів. Отримати обсяги робіт з обслуговування.

4. Галузь виготовлення електрощитового обладнання:

- 2023 рік – забезпечити планомірне та ритмічне завантаження цеху з виготовлення. Вийти на обсяг реалізації від 100 000 грн. в місяць;

Кінець 2022 року – початок 2023 року запустити рекламу з виготовлення нестандартизованого обладнання для побутових споживачів (квартири, котеджі). Закріпитись на вказаному ринку.

Стратегічними напрямками розвитку для підприємства на сьогоднішній день є:

- нарощування цінності підприємства і його здатності створювати стійкий прибуток протягом тривалого часу;
- утримання та постійне розширення частки ринку, швидке і гнучке реагування на зміну ринкової ситуації і діяльність конкурентів;
- лояльність, довіра і перевага споживачів;
- взаємовідносини із зацікавленими в діяльності підприємства сторонами, засновані на партнерстві, прозорості та справедливості, розподілі вигоди між сторонами відповідно до їхнього внеску;
- співпраця з органами влади та управління, підтримка соціальної сфери.

Візією ТОВ «СУЧАСНІ ТЕХНОЛОГІЇ БУДІВНИЦТВА 2016» є те, що – це українська компанія високого рівня, яка знаходить оптимальні рішення для всіх проєктів у сфері промислового громадського та комерційного будівництва.

Плани на найближчі 3-5 років - є виведення послуг (проектування, будівельно-монтажні роботи) на європейський ринок. На українському ринку компанія повинна тримати впевнені позиції з реалізації продукції та послуг.

Як бачиться вихід на європейський ринок? На сьогоднішній день низка партнерів, з якими працював компанія в довоєнний період виїхала за межі України в різні європейські країни. Сьогодні їм доволі успішно вдається проводити розвідку ринку будівельних та інжинірингових послуг. Частина партнерів вже працюють з європейськими колегами на ринку проектування та інжинірингу.

Процес виходу підприємства на європейський ринок буде супроводжуватись складнощами в різниці законодавств, які регулюють діяльність підприємств будівельної галузі в Україні та на європейському ринку. Питання, які будуть виникати з регуляторами вирішуємі, потрібен тільки час.

Основною конкурентною стратегією при виході на нові ринки буде фокусування. Компанія зосередить всі зусилля на тому, що краще всього можемо робити (електромонтажні роботи, проектування електричних мереж), направляти на стартовому етапі найкращих спеціалістів підприємства з метою отримання позитивного іміджу серед місцевих замовників.

На сьогоднішній день компанія має попередні напрацювання з генпідрядними підприємствами Польщі стосовно спільної участі у масштабних проєктах. Також налагоджено попередній зв'язок з потужними проєктними організаціями в Литві. Підприємства, з якими налагоджені зв'язки мають потребу в закритті вузьких місць на будівельних об'єктах (виконання електромонтажних робіт). В галузі проектування основний фокус потрібно буде зробити на проектуванні мереж зовнішнього електропостачання. На сьогоднішній день компанія працює на економічному фронті за для перемоги України, після будемо розпочинати впровадження стратегічних планів.

Конкурентна стратегія, яка буде застосована в найближчі п'ять років на території України є стратегія диверсифікації. Розпочинаючи процес занурення в роботу на об'єктах відновлення країни, компанія буде опановувати нові види робіт (демонтажні, загальнобудівельні, опоряджувальні). Процес розширення сфер

діяльності буде виконуватись за допомогою залучення відповідних профільних спеціалістів, що мають кваліфікацію та досвід на виконання даних видів робіт.

Робота на різних ринках та за різними напрямками діяльності дозволить підприємству знизити ризики зупинки діяльності у зв'язку зі зменшенням обсягів виробництва за тим чи іншим напрямком діяльності. В свою чергу плани на закріплення позицій на українському ринку можуть бути скориговані новими гравцями, що планують приймати участь у відновленні країни. В даному випадку маються на увазі європейські партнери України (Польща, Велика Британія), які готові долучатись та приймати активну участь у процесі відновлення.

Україна вже отримала чіткі підтвердження низки країн щодо ініціативи про шефство у відновленні окремих міст, регіонів чи галузей. Згідно з інформацією з Офісу Президента Велика Британія висловила згоду підтримати Київ та Київську область, Данія – Миколаїв та Миколаївську область, Балтійські держави готові підтримувати Житомирську область. Глава держави запропонував країнам-партнерам узяти шефство над регіонами та галузями України, які постраждали від війни[17].

Таким чином вже зараз зрозуміло, що конкуренція на ринку відновлення країни буде жорсткою. Але, маючи досвід роботи в Україні, компанія зможе бути достойним гравцем та отримувати перемогу в конкурентній боротьбі.

1.2 Оцінювання вартості інформаційних ресурсів підприємства

Інформаційні системи і технології є невід'ємною частиною будь-якої організації, що забезпечують управління виробництвом, фінансами, персоналом, документами, тощо. Інформація є повноцінним ресурсом на рівні з капіталом, землею та людьми. Тому організація режиму інформаційної безпеки підприємства стає критично важливим стратегічним чинником розвитку сучасного виробництва.

Використання організацією (підприємством) інформаційних ресурсів необхідно для реалізації зовнішньої і внутрішньої діяльності. Чинниками

зовнішній діяльності є економічні, соціальні, політичні та інші об'єкти, що діють за межами підприємства та пов'язані з певними відносинами з ними. До них також належать фінансові організації, клієнти, постачальники, конкуренти.

Внутрішні фактори діяльності – господарські відносини в колективі, які обумовлені інформаційними процесами і знаннями, сформованими в процесі їх функціонування; це також фінанси підприємства, організація виробничих процесів, якість продукції, що випускається підприємством, прийнята виробнича стратегія підприємства тощо.

Інформаційні ресурси підприємства дозволяють забезпечити ефективну взаємодію фінансових, матеріальних, інтелектуальних та інших ресурсів. Досягнення цього можливо за допомогою:

- підтримки моніторингу виробничих та адміністративно-господарських процесів,
- забезпечення оперативного доступу до архівів технологічних і управлінських документів,
- отримання інформації про завантаженість робочих місць, рух матеріалів, витрати робочого часу тощо,
- реєстрації та підготовки аналітичних матеріалів про запаси, комплектуючі і готову продукцію,
- підтримки системи обліку і класифікації витрат,
- пошуку і встановлення партнерських зв'язків та співробітництва,
- аналізу даних про стан бізнесу і розробки проєктів розвитку підприємства,
- модифікації інформаційної системи підприємства.

З вищепереліченого бачимо, що для реалізації ефективного управління необхідна інформація з зовнішніх у відношенні до підприємства джерел, достовірність якої має дуже важливе значення. Однією з основних проблем у даному випадку є проблема знаходження найбільш релевантних джерел інформації.

Ефективне використання інформаційних ресурсів дозволяє підприємству отримати переваги в наступних напрямках його діяльності:

- організація бізнесу,

- ефективне управління власністю,
- пошук і розвиток нового бізнесу.

Інформаційні ресурси (ІР) охоплюють усі підрозділи та служби підприємства. Так, якщо в деяких відділах і службах підприємства відсутня обчислювальна техніка і/або вона не підключена до локальної мережі, вони є постачальниками визначеної інформації, що виникає тільки в даному підрозділі. Інформація в базу даних може надходити централізовано, але її формування відбувається в кожному конкретному підрозділі або службі підприємства.

Таким чином, необхідно розглядати інформаційний простір підприємства, тобто не тільки ІР і засоби обробки інформації, але і географію інформаційних відносин. В залежності від форми взаємодії та використання кожного з компонентів можна виділити п'ять основних рівнів реалізації інформаційного простору підприємства (ІПП).

Перший рівень реалізації ІПП фіксує інформацію про виконання господарських дій у вигляді таблиць, що дає можливість вести основні види обліку: оперативний, бухгалтерський, адміністративний, податковий.

Реалізація ІПП другого рівня передбачає використання СУБД, яка дозволяє не тільки виконувати основні операції з обробки фактичної інформації та підтримувати всі види обліку, але і дає можливість підготовки різноманітних аналітичних документів. Цей рівень на практиці базується на використанні локальної мережі, що дозволяє застосовувати електронний документообіг і узагальнювати корпоративну інформацію.

Третій рівень ІПП відображає його розподіл на окремі ІС: логістика, облік і звітність, управління персоналом, заробітна плата, управління виробництвом та інше. Тут також визначена загальна ІС для відображення інформації для управління. Цей рівень передбачає реалізацію господарської діяльності в Інтернеті.

ІПП четвертого рівня передбачає його розширення за рахунок застосування фронт-офісних структур, які можуть за допомогою Інтернету надавати постачальникам, партнерам, клієнтам та інвесторам необхідну інформацію відповідно до визначених повноважень.

Функціонування ІС підприємства засноване на використанні різноманітних джерел інформації, у тому числі зовнішніх. Одне з основних завдань, пов'язаних з цим, – забезпечення високого рівня інформаційної безпеки, захисту інформації, яка надходить з різних джерел.

У зв'язку з тим, що інформаційні ресурси вже внесені в ІС та використовуються, основне спрямування забезпечення ІБ повинно бути орієнтоване на оцінювання вартості інформаційних ресурсів підприємства. Така задача, на наш погляд, є непростюю.

Нехай усі інформаційні ресурси представлені у вигляді кінцевої множини елементів і необхідно оцінити їх вартість у грошовому еквіваленті. Оцінювання вартості ІР в ІС визначається в плановому періоді, який дорівнює одному року. Виходячи з витрат на придбання, обслуговування, прибутку, що отриманий від використання інформаційних ресурсів протягом одного року, вартість таких ресурсів відносять до 1-ої категорії.

вартість k-го ресурсу з 1-ої категорії буде дорівнювати за формулою:

$$S_{I.k}^{\text{кат1}} = S_{k<t>}^{\text{прид}} + S_{k<t>}^{\text{розр}} + S_k^{\text{обсл}} + \Pi_k, k = \overline{1, Z_{\text{кат1}}} \quad (1.1)$$

де $S_{k<t>}^{\text{прид}}$ - зведена до поточного року

$S_{k<t>}^{\text{розр}}$ – вартість розробленого ІР

$S_k^{\text{обсл}}$ – вартість обслуговування ресурсу протягом року,

Π_k – прибуток від використання ресурсу протягом року.

Приведена до t-го року експлуатації вартість придбаного k-го ресурсу:

$$S_{k<t>}^{\text{придб}} = (S_k^{\text{первин}} \cdot \prod_{g=1}^{t_k-1} I_g) \cdot \left(1 - \frac{t_k-1}{T_k^{\text{план}}}\right) \quad (1.2)$$

де $S_k^{\text{первин}}$ – вартість ІР на рік його придбання,

t_k – поточний рік експлуатації,

I_g – галузевий індекс зміни цін після g-го року експлуатації ІР,

$T_k^{\text{план}}$ – запланований термін експлуатації ІР, причому $T_k^{\text{план}} \geq t_k$

Якщо ця умова не виконана, то запланований термін експлуатації необхідно збільшити до значення поточного року експлуатації.

Базова вартість розробки k-го ІР у g-му році розробки:

$$S_{k<g>}^{\text{баз}} = \sum_{c=1}^{N_{\text{comp}}} (S_{k.c<g>}^{\text{прац}} + S_{k.c<g>}^{\text{відр}}) + S_{k<g>}^{\text{витрат}} \quad (1.3)$$

де $S_{k.c<g>}^{\text{прац}}$ – витрати на оплату праці c -го співробітника, але розробці k -го ІР

$S_{k.c<g>}^{\text{відр}}$ – відрахування до фондів страхування

$S_{k<g>}^{\text{витрат}}$ – загальні витрати на витратні матеріали при розробці k -го ІР

Приведена до t -го року розробки накопичена вартість 4-го ІР, що розробляється, за формулою:

$$S_k^{\text{накопич}} = S_{k<t>}^{\text{накопич}} = S_{k<t-1>}^{\text{накопич}} \cdot I_{t-1} + S_{k<t>}^{\text{баз}}, \forall t > 1, \quad (1.4)$$

для першого року розробки:

$$S_{k<1>}^{\text{накопич}} = S_{k<1>}^{\text{баз}} \quad (1.5)$$

Приведена до 1-го року експлуатації вартість розробленого k -го ІР:

$$S_{k<t>}^{\text{розр}} = (S_k^{\text{накопич}} \cdot \prod_{g=t_k}^{l_k-1} I_g) \cdot \left(1 - \frac{t_k-1}{T_k^{\text{план}}}\right) \quad (1.6)$$

де t_k – поточний рік експлуатації, після закінчення розробки,

I_g – галузевий індекс зміни цін після g -го року експлуатації ІР

$T_k^{\text{план}}$ – запланований термін експлуатації ІР, причому $T_k^{\text{план}} \geq t_k$

Якщо ця умова не виконана, то запланований термін експлуатації необхідно збільшити до значення поточного року експлуатації.

Вартість обслуговування k -го ІР у поточному році:

$$S_k^{\text{обс}} = \sum_{c=1}^{N_{\text{comp}}} (S_{k.c}^{\text{прац}} + S_{k.c}^{\text{відр}}) + S_k^{\text{витрат}} \quad (1.7)$$

де $S_{k.c}^{\text{прац}}$ – витрати на оплату праці c -го співробітника, що обслуговує k -й ІР (визначаються через об'єм витраченого часу та розмір заробітної плати),

$S_{k.c}^{\text{відр}}$ – відрахування до фондів страхування (відсоток від витрат на оплату праці),

$S_k^{\text{витрат}}$ – загальні витрати на витратні матеріали, необхідні обслуговування k -го ІР.

ІР, цінність яких є концептуальною, не визначається лише вартістю придбання, розробки та обслуговування, ІР, які не приносять безпосереднього

прибутку, але порушення захищеності яких призводить до значних фінансових втрат, відносять до ресурсів 2-ї категорії.

Розглянемо алгоритм оцінки вартості ІР 2-ї категорії.

1 етап. Побудова вектора рангів ІР 1-ї та 2-ї категорії.

$$C = \{c_1, c_2, \dots, c_z\} \quad (1.8)$$

2 етап. Угрупування оцінок ресурсів 1-ї категорії в такий спосіб, щоб у групі були ресурси з однаковим значенням рангу.

3 етап. Обчислення середньої вартості ресурсів з тим самим рангом:

$$E_R = \frac{1}{Z_R} \sum_{k=1}^{Z_R} S_{И.k}^{1 \text{ кат}}, \quad (1.9)$$

де - кількість ресурсів з рангом R .

4 етап. Перевірка виконання умов ранжування, застосованих до середньої вартості ресурсів кожного з наявних рангів:

$$\begin{cases} E_R < E_{R+1}, \forall R \in [1, 8] \\ E_{R_1} \underset{R}{\Leftarrow} E_{R_2}, R_2 \geq R_1 + 2 \end{cases} \quad (1.10)$$

де $\underset{R}{\Leftarrow}$ - оператор рангової переваги вартості ресурсів рангу R_2 над ресурсами рангу R_1 . Оцінка такої переваги ґрунтується на таких розрахунках.

1. Для кожної пари цін ІР $E_{R_1}, E_{R_2}, \forall R, R_2 > R_1$ оцінимо величину відношення

$$dE_k = \frac{R_2 - R_1}{\sqrt{\frac{E_{R_2}}{E_{R_1}}}}, \text{ де } k = \overline{1, m} - \text{номер пари, } m - \text{кількість пар.}$$

Примітка: під парою цін ІР у цьому випадку розумітимемо два значення середньої вартості двох груп ІР, що мають два різних ранги, між якими ІР інших рангів немає.

2. Обчислимо середнє геометричне таких відносин:

$$sE = \sqrt[m]{\prod_{k=1}^m dE_k} \quad (1.11)$$

3. З усіх пар залишимо ті, для яких середнє зростання вартості менше за показник. У цих парах умова зростання вартості є недостатньою щодо інших пар, що послаблює рангову перевагу. Але якщо для кожної з цих пар виконується умова:

$$dE_i < dE_j, i < j, \forall i, j \in [1, m], \text{ при } dE_i < sE, dE_j < sE \quad (1.12)$$

тобто набір відносин є строго зростаючим, то рангову перевагу можна вважати достатнім.

Також якщо така пара єдина, то рангову перевагу не порушено.

5 етап. Невиконання умов (1.10) призводить до необхідності корекції рангів окремих ІР (повернення до 1-го етапу алгоритму). Корекцію необхідно проводити з таких міркувань.

1. У кожній групі вибрати ІР, вартість якого значно нижча інших, чи значно вище.

2. ІР із низькою вартістю перенести до групи попереднього рангу, а ІР із високою вартістю — до групи наступного рангу.

3. Дії 1 та 2 необхідно виконувати з кожним ресурсом окремо, після чого повторювати 2-й, 3-й та 4-й етапи алгоритму до виконання умов (1.10).

Зауваження. За дуже малої кількості ІР (до десяти), розподіленої кількості груп (2-4) можлива ситуація, за якої

Умова (1.10) ніколи не може бути виконана. У цьому випадку доцільно залишити такий розподіл ІР за групами, що дає умови, що є найбільш близькими до 1.10.

6 етап. Всім інформаційним ресурсам з 2-ї категорії, що мають ранг R присвоїти значення вартості рівне E_R .

7 етап. Якщо у 2-й категорії є ресурси, віднесені до рангу, який представлений жодним ресурсом 1-ї категорії, необхідно виконати інтерполяцію (екстраполяцію) невідомих значень по відомим.

Алгоритм інтерполяції:

1. Для кожної пари значень E_{R_1} та E_{R_2} , де $E_{R_1} < E_{R_2}$ визначити величину зростання вартості одного ступеня:

$$\delta E_i = \sqrt[n]{\frac{E_{R_2}}{E_{R_1}}}, X = R_2 - R_1 \quad (1.13)$$

де $i = \overline{1, n}$ — номер пари, n — загальна кількість пар.

Примітка: під парою значень середньої вартості ІР у цьому випадку розумітимемо два значення середньої вартості двох груп ІР, які мають два різні ранги (враховуються всі поєднання)[18].

2. Обчислити середню величину зростання вартості одного ступеня;

$$\Delta E = \sqrt[n]{\prod_{i=1}^n \delta E_i}. \quad (1.14)$$

3. Нехай E_{R_1} – найближче відоме значення зліва, а E_{R_2} – праворуч від того значення, яке необхідно визначити. Тоді знайдемо межі діапазону можливих значень E_R як:

$$\alpha = E_{R_1} \cdot (\Delta E)^X, \quad X = R - R_1 \quad \beta = \frac{E_{R_2}}{(\Delta E)^Y}, \quad X = R_2 - R \quad (1.15)$$

4. Шукане значення вартості ресурсів даного рангу дорівнює середньому значенню обчисленого відрізка:

$$E_R = \frac{\alpha + \beta}{2} \quad (1.16)$$

Алгоритм екстраполяції:

1. Аналогічно п.1 алгоритму інтерполяції з обчисленням за формулою (1.16).
2. Аналогічно п.2 алгоритму інтерполяції з обчисленням за формулою (1.17).
3. Якщо точка E_R знаходиться ліворуч від усіх відомих точок і E_{R_2} – найближча до неї точка праворуч, то:

$$E_R = \frac{E_{R_2}}{(\Delta E)^Y}, \quad X = R_2 - R \quad (1.17)$$

- 4) якщо E_R знаходиться праворуч від усіх відомих точок і E_{R_1} – найближча до неї точка зліва, то:

$$E_R = E_{R_1} \cdot (\Delta E)^X, \quad X = R - R_1 \quad (1.18)$$

Значення вартості IP 2-ї категорії отримуємо підстановкою обчислених значень вартості IP відповідного рангу 1-ї категорії:

$$E_R \xrightarrow{c=R} S_{\text{И.к}}^{2 \text{ кат}}, \quad (\forall k = \overline{1, z_{2 \text{ кат}}}).$$

Для дослідження важелів і тенденцій розвитку стану зберігання управління інформаційними ресурсами підприємства існують відповідні поняття та позначення інформаційної безпеки, які регламентуються міжнародними та національними стандартами.

Згідно зі стандартом ISO/IEC 27001:2013, інформаційна безпека – це збереження конфіденційності, цілісності та доступності інформації; крім того, можуть враховуватися інші властивості, такі, як автентичність, відстежуваність, неспростовність та надійність. Це комплекс заходів, спрямованих на забезпечення захищеності інформації від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки, запису чи

знищення [6].

1.3 Основні напрями управління інформаційною безпекою підприємства

Аналіз наукових праць [4, 5, 7, 8] показує, що інформаційна система підприємства визначає сукупність взаємопов'язаних засобів забезпечення функціонування необхідних інформаційних процесів, необхідних для виконання виробничих і управлінських завдань.

Ефективне виконання цих завдань базується на забезпеченні необхідного рівня безпеки інформаційних ресурсів компанії. Такий рівень можливий лише за умови комплексної та достовірної оцінки поточного рівня безпеки інформаційних ресурсів, який визначається низкою різноманітних факторів.

Технологія оцінки поточного рівня інформаційної безпеки, наприклад здатності зберігати атрибути інформації в інформаційних системах під впливом загроз інформаційній безпеці, потребує дослідження наступних критеріїв: - відносна частота загроз інформаційній безпеці RRZ, - здатність RRZ розпізнавати загрози інформаційній безпеці.

Підвищення рівня безпеки інформаційних ресурсів в інформаційних системах тоді може здійснюватися за двома основними напрямками: - навіть зменшення кількості вразливостей за рахунок зміни структури самої інформаційної системи вважають; - покращує якість систем захисту інформації, що призведе до зниження ймовірності реалізації загроз з боку зловмисників.

Необхідною умовою досягнення необхідного УЗІР в ІБ є розробка комплексних систем захисту інформації [4, 5]. Окремі організації та більшість підприємств існують у системі товарно-грошових відносин, їх діяльність характеризується економічною ефективністю, яка полягає в економному використанні матеріальних ресурсів для проведення будь-яких заходів, у тому числі заходів МОК.

Відповідно, оцінка УЗІР та прийняття рішення про впровадження заходів, спрямованих на його зміцнення, ставить завдання оцінки економічної ефективності їх впровадження. Таким чином, загальний підхід до оцінки УЗІР також включає такі додаткові критерії [7]:

- вартість ІР S_{IP} .
- вартість елементів ЗОІ S_{ZOI} .
- вартість ЗЗІ S_{ZZI} .
- сумарний ризик порушення захищених властивостей ІР R_{IP} .
- сумарний ризик ЗЗІ S_{ZZI} .
- сумарний ризик засобів обробки інформації R_{ZOI} .

Ймовірності P_{nr} , S_{con} та критерії їх оцінки розглядатимемо надалі як параметри ІС. А критерій та обидва показники захищеності ІР D_{IP} та економічної ефективності Eff , є показниками якості ЗЗІ.

[6] Існують наступні залежності між параметрами ІС [6]:

$$P_{BU} = f(S_{IP}, S_{ZOI}).$$

$$P_{PY} = f(P_{BU}, S_{IP}, S_{ZOI}, S_{ZZI}).$$

$$R_{IP} = f(S_{IP}, S_{ZZI}, P_{BU}, P_{PY}). \quad (1.19)$$

$$R_{ZOI} = f(S_{ZOI}, S_{ZZI}, P_{BU}, P_{PY})$$

$$R_{ZZI} = f(S_{ZZI}, P_{BU}, P_{PY})$$

Таким чином, оцінка поточного УЗІР необхідна для оптимального управління ІС з метою підвищення захищеності інформації в ІС шляхом вдосконалення засобів, спрямованих на порушення цілісності інформації [5].

Вирішення завдання управління ІБ реалізується через систему управління ІБ. Процес забезпечення полягає у прийнятті рішень щодо дій з виявлення вразливостей та загроз ІБ, застосування ресурсів, найбільш доцільних в умовах обмежених ресурсів. Прийняття рішення лягає на особу, яка приймає рішення, управління процесом в умовах невизначеності в процесі реалізації, фінансування його на основних принципах оптимізації параметрів ІС, в тому числі потенціалу злоумисника.

Загальна структура будьякого процесу управління представлена на рисунку 1.2.

Мета управління в завданні СУ підтримка необхідного УЗІР протягом всього терміну експлуатації ІС та інтегрованого циклу ІР.

СУ являє собою систему: ІС та інтегрована з нею ЗЗІ. Модель СУ представлена системою: ІС та інтегрована з нею ЗЗІ. Моделлю параметрів ІС та параметрів ЗЗІ, а також невідомих взаємозв'язків параметрів ІР та значень величин, що вирішують завдання різних організацій (представлений змістом управління системи параметрів, завдань, ЗЗІ).



Рисунок 1.2. – Структура процесу управління

Джерело: розроблено автором

Пристрій управління виступає особа, яка приймає рішення щодо розробки, конфігурації, налаштування та вдосконалення механізму захисту ІС.

Керуючий вплив реалізується за допомогою заходів щодо забезпечення необхідного УЗІР. Зворотній зв'язок служить для передачі особі, яка приймає рішення, інформації про стан ІС та ЗЗІ [19].

Алгоритм управління це опис того, як повинні використовуватись ЗЗІ залежно від стану СУ, інформації про який надходить каналом зворотного зв'язку.

Алгоритм управління полягає у такій зміні структури ЗЗІ та ІС, при якій буде забезпечено необхідний УЗІР протягом контрольованого періоду (1 рік).

Зміна структури ІС полягає у зміні складу, структури, налаштувань та інших характеристик механізму захисту ІС. Зміна складу механізмів захисту ЗЗІ призводить до зміни витрат на СУ.

Зміна структури ІС полягає в ліквідації вразливостей шляхом зміни структури, локалізації, способів представлення ІР, а також схеми впливу на СУ. Зміна структури ІС та ЗЗІ здійснюється за допомогою організаційно-розпорядчих директив.

Загальна структура СУІБ представлена на рисунку 1.3.

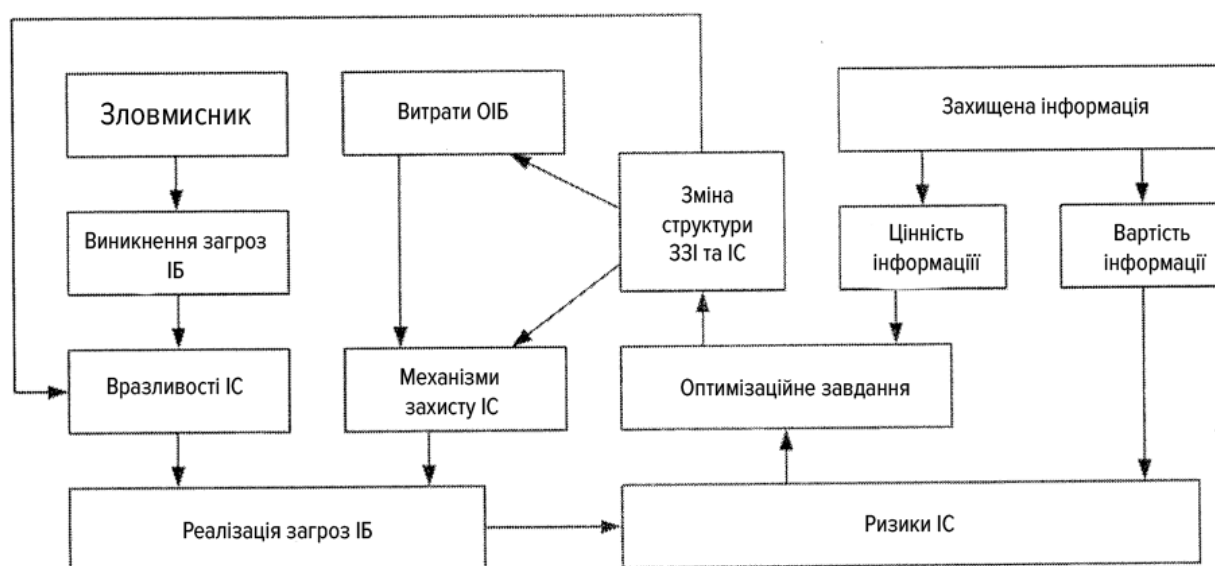


Рисунок 1.3 – Загальна структура СУІБ

Джерело: розроблено автором

Деталізація окремих складових загальної структури, виділення низки приватних показників якості ЗЗІ в цілому, вирішення таких низки супутніх завдань призводить до наступних уявлень про цілі моделі контролю показників якості ЗЗІ.

Практика показує, що залежність (1.19) має ймовірнісний характер [12, 13]. Тому в більшій мірі визначальними є "людський фактор", але також для достовірної оцінки показників якості оперують, зокрема, поняттям "теорії нечітких множин", яка якраз і враховує неточність та дозволяє досліджувати питання реалізації загроз ІБ.

Відносні частоти виникнення загроз ІБ є числовими характеристиками і можуть бути визначені статистичними методами. Але ІС включають в себе безліч

різних компонентів і характеризуються змінним складом (для підприємства та організації захисту різного профілю). Внаслідок цього отримати та інтерпретувати статистику по якомусь типу ІС та ефективно використовувати рішення для якоїсь проблеми є досить складно[19].

Для показників захищеності ІС використовують експертну оцінку. Необхідно отримання кількісних результатів, що суттєво ускладнюється такими факторами, як [9]:

- наявність складної взаємозв'язку параметрів ІС.
- необхідність врахування та формалізації ряду цих показників з параметрами ІС.
- багато з елементів є якісними величинами і мають значну невизначеність.
- наявність суттєвих взаємозв'язків та взаємозалежності цих параметрів, що мають суперечливий характер, ускладнює отримання необхідних даних, особливо на ранніх етапах проєктування ЗЗІ.

Етапи проєктування, організації та експлуатації ЗЗІ завжди пов'язані з непередбачуваними (актуальними для прийняття рішення) факторами. Крім того, можлива неповність вимірювань, "людський фактор", які можуть суттєво впливати на завдання оптимізації ЗЗІ, тому доводиться враховувати психологічні фактори та форс-мажорні обставини, отже [2, 6]:

- переважно нечіткий опис безлічі вихідних даних, зокрема стандартних, що використовуються при побудові ЗЗІ, завдання вибору форми зазвичай є нечітким.
- постановка завдань у формі ЗЗІ вимагає знань, при цьому інформація того чи іншого засобу визначається експертно.

З багатокритеріальної точки зору [10].

Більш ефективним буде такий комплекс заходів щодо підвищення УЗІР в ІС, при якому виконуються такі умови:

$$\begin{cases} S_{\text{ЗЗІ}} \leq \Delta R_{\text{ІР}} + \Delta R_{\text{ЗОІ}} + \Delta R_{\text{ЗЗІ}} \\ S_{\text{ЗЗІ}} \leq S_{\text{ІР}} + S_{\text{ЗОІ}} \end{cases} \quad (1.20)$$

де $\Delta R_{IP} + \Delta R_{3OI} + \Delta R_{33I}$ – загальне зниження ризиків в ІС, можливе завдяки функціонуванню ЗЗІ.

Перша умова задає додатність економічного ефекту від експлуатації ЗЗІ: отриманий ефект не повинен бути меншим за вартість ЗЗІ та заходів щодо забезпечення ІБ.

Друга умова визначає цілепокладання підприємства, яке спрямоване на виконання його основної діяльності: реалізація функції забезпечення ІБ є допоміжною.

З функціональної точки зору, яка визначена загальним показником захищеності ІР, якість ЗЗІ визначають умови відповідності певному мінімальному порогу захисту для кожного ІР:

$$D_i \geq D_{i.min}, \forall i = \overline{1, z}. \quad (1.21)$$

Умови (1.20) та (1.21) суперечливі: підвищення УЗІР в ІС на певному етапі можливе лише при збільшенні інвестицій в ЗЗІ.

З цього випливає постановка задачі оптимізації:

$$D_{IP} \rightarrow \max$$

$$D_i \geq D_{i.min}, \forall i = \overline{1, z} \quad (1.22)$$

$$S_{33I} \leq \Delta R_{IP} + \Delta R_{3OI} + \Delta R_{33I}$$

$$S_{33I} \leq S_{IP} + S_{3OI}$$

Модель контролю показників якості ЗЗІ є загальною та відображає структуру взаємозв'язків параметрів ІС, а також порядок їх оцінки. Характер взаємозв'язків можна описати моделлю, представленою на рисунку 1.4.

Область загроз Т ІБ являє собою їх повний перелік для даної ІС; кожна загроза характеризується своєю частотою виникнення.

Множина вразливостей V – це набір вразливостей для даної ІС; основними характеристиками вразливостей є: значущість та доступність для зловмисника. В сукупності множина загроз і вразливостей, а також їх взаємозв'язки утворюють перелік способів досягнення мети зловмисником – заходів, що характеризуються на ІР.

ЗЗІ М – це наявний в організації набір важливих стандартів безпеки. Якість засобів та виконання вимог визначається при розгляді множини вразливостей V і

множини механізмів захисту M з їх взаємозв'язками, і характеризується можливостями подолання кожного бар'єра захисту, асоційованого з кожною [20]

уразливістю. Елемент (*) показує, що вразливість може бути взагалі не перекрита жодним бар'єром захисту. Область O представляє собою сукупність ІР, характеристики яких: цінність і вартість, визначаються виходячи з фінансових втрат організації, пов'язаних з відновленням ресурсів, або з упущеною вигодою, пов'язаними зі знищенням, тиражуванням, або блокуванням доступу до захищуваного ресурсу. Разом множини M , множини O та їх взаємозв'язки дають повний опис ЗЗІ організації (підприємства).

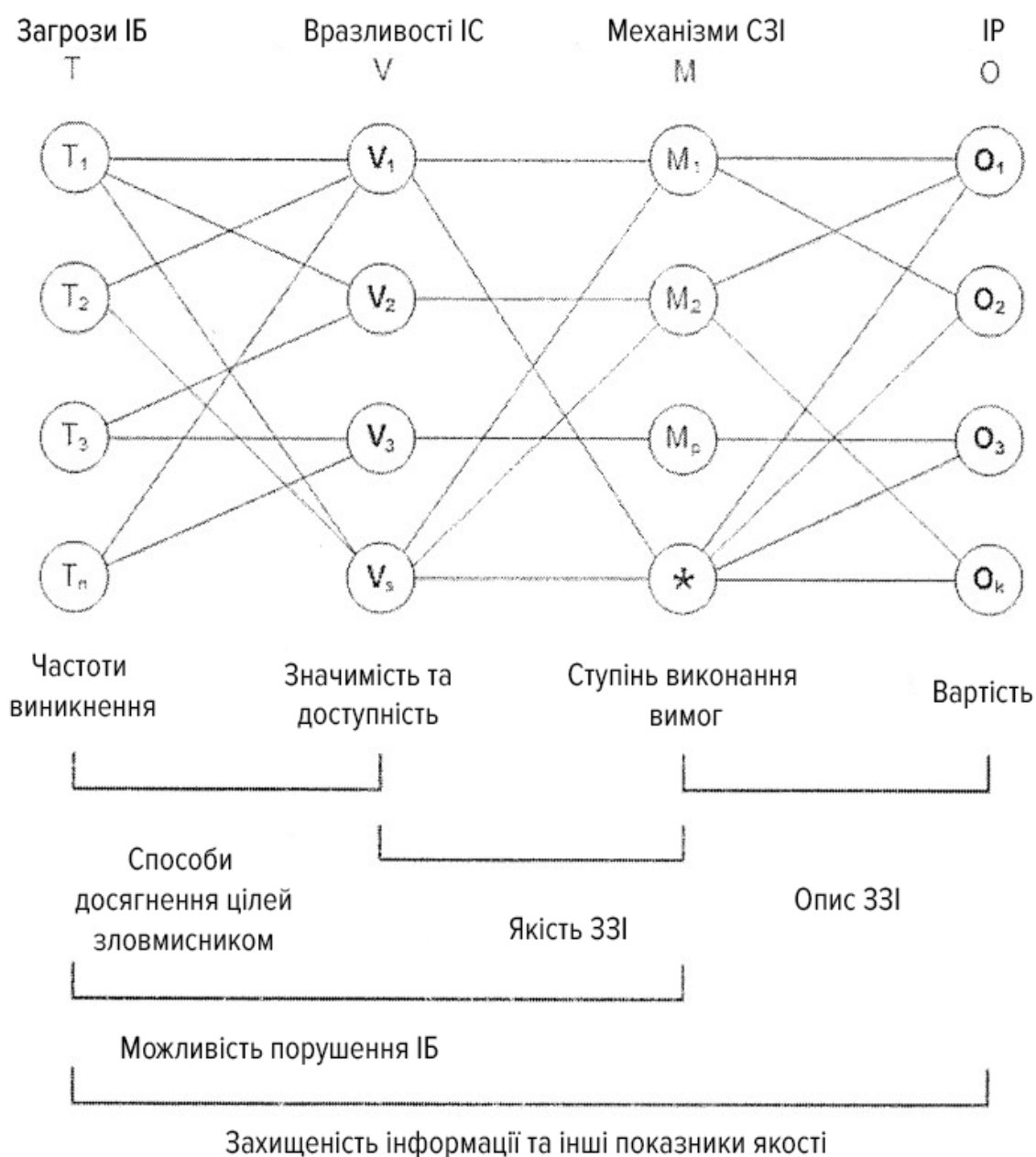


Рисунок 1.4 – Модель, що описує характер взаємозв'язку параметрів ІС та показників якості

Джерело: розроблено автором

Ймовірності реалізації загроз ІБ в ІС організації (підприємства) визначаються якістю ЗЗІ та заходами з забезпечення ІБ.

В цілому, УЗІР та інші показники якості визначаються всією сукупністю областей графа, при цьому ефективність характеризується співвідношенням ризиків від порушення захищуваних властивостей ІР в ІС організації за відсутності та за наявності ЗЗІ.

РОЗДІЛ 2

Системний аналіз важелів управління інформаційною безпекою підприємства

2.1 Аналіз уразливостей і загроз інформаційної системи підприємства

Уразливістю інформаційної системи (ІС) будемо називати деяку сутність, але не властивість об'єкту, який знаходиться під деструктивним впливом. Уразливість - це будь-яке відхилення в окремій частині ІС, що може стати причиною порушення інформаційної безпеки. До таких відхилень пропонується віднести:

- недоліки в організації захисту інформації,
- відхилення від політики інформаційної безпеки,
- невідповідність характеристики стандарту інформаційної безпеки,
- помилки в роботі системи обробки інформації.

Уразливості можна класифікувати за допомогою різноманітних ознак. З точки зору необхідності їх порівняння для виявлення найбільш значущих в класифікації необхідно розділяти уразливості на групи у відповідності до типу проявлення.

Порушник – це особа, яка зробила спробу виконання заборонених операцій (дій) помилково, або усвідомлено зі злим умислом (з корисливих інтересів) або без нього (заради гри або задоволення, з метою самоствердження і т.п.) і використовує для цього різні можливості, методи і засоби (Додаток А).

Система захисту ІС ТОВ «СТБ 2016» повинна будуватися виходячи з припущень про наступні можливі типи порушників у системі (з урахуванням категорії осіб, мотивації, кваліфікації, наявності спеціальних засобів тощо):

1) Недосвідчений (неуважний) користувач – співробітник ТОВ «СТБ 2016», який може робити спроби виконання заборонених операцій, доступу до ресурсів, що захищаються ІС з перевищенням своїх повноважень, введення некоректних

даних тощо, діє помилково, по некомпетентності або недбалості без злого наміру і використовує при цьому тільки штатні (доступні йому) апаратні і програмні засоби.

2) Аматаор – співробітник ТОВ «СТБ 2016», який намагається подолати систему захисту без корисливих цілей і злого умислу, для самоствердження або зі «спортивного інтересу». Для подолання системи захисту і здійснення заборонених дій він може використовувати різні методи отримання додаткових повноважень доступу до ресурсів (імен, паролів і т.п. інших користувачів), недоліки у побудові системи захисту і доступні йому штатні (встановлені на робочій станції) програми (несанкціоновані дії у вигляді перевищення своїх повноважень на використання дозволених засобів). Крім цього він може намагатися використовувати додатково нештатні інструментальні та технологічні програмні засоби (відладчики, службові утиліти), самостійно розроблені програми або стандартні додаткові технічні засоби [21].

3) Шахрай – співробітник ТОВ «СТБ 2016», який може робити спроби виконання незаконних технологічних операцій, введення підроблених даних і тому подібні дії в корисливих цілях, з примусу або зі злого умислу, але використовує при цьому тільки штатні (встановлені на робочій станції і доступні йому) апаратні і програмні засоби від свого імені або від імені іншого співробітника (знаючи його ім'я і пароль, використовуючи його короткочасна відсутність на робочому місці тощо) [22].

Внутрішній зловмисник – співробітник підрозділу ТОВ «СТБ 2016», зареєстрований як користувач системи, що діє цілеспрямовано з корисливих інтересів або помсти за нанесену образу, можливо в змові з особами, які не є співробітниками ТОВ «СТБ 2016». Він може використовувати весь набір методів і засобів злому системи захисту, включаючи агентурні методи отримання реквізитів доступу, пасивні засоби (технічні засоби перехоплення без модифікації компонентів системи), методи і засоби активного впливу (модифікація технічних засобів, підключення до каналів передачі даних, впровадження програмних закладок і використання спеціальних інструментальних і технологічних програм), а також комбінації впливів як зсередини, так і ззовні - з мереж загального користування [23].

Внутрішнім порушником може бути особа з наступних категорій персоналу ТОВ «СТБ 2016»:

- зареєстровані користувачі ІС ТОВ «СТБ 2016» (співробітники підрозділів ТОВ «СТБ 2016»);
- співробітники підрозділів ТОВ «СТБ 2016» не допущені до роботи з ІС ТОВ «СТБ 2016»;
- персонал, що обслуговує технічні засоби ІС ТОВ «СТБ 2016» (інженери, техніки);
- адміністратори ІС ТОВ «СТБ 2016»;
- співробітники відділів розробки і супроводу ПЗ (прикладні та системні програмісти);
- технічний персонал, що обслуговує будинки (прибиральниці, електрики, сантехніки та інші співробітники, що мають доступ в будівлі та приміщення, де розташовані компоненти ІС ТОВ «СТБ 2016»).

Користувачі та обслуговуючий персонал з числа співробітників ТОВ «СТБ 2016» мають найбільш широкі можливості щодо здійснення несанкціонованих дій, внаслідок наявності у них певних повноважень по доступу до ресурсів і гарного знання технології обробки інформації та захисних заходів. Дії цієї групи осіб безпосередньо пов'язане з порушенням чинних правил та інструкцій. Особливу небезпеку ця група порушників представляє при взаємодії з кримінальними структурами.

Зовнішній порушник (зловмисник) – стороння особа чи співробітник ТОВ «СТБ 2016», що діє цілеспрямовано з корисливих інтересів, з помсти або з цікавості, можливо в змові з іншими особами. Він може використовувати весь набір способів порушення безпеки інформації, методів і засобів злому систем захисту, характерних для мереж загального користування (особливо мереж на основі ІР-протоколу), включаючи віддалене впровадження програмних закладок і використання спеціальних інструментальних і технологічних програм, використовуючи наявні слабкості протоколів обміну та системи захисту вузлів мережі ІС ТОВ «СТБ 2016» [24].

Категорії осіб, які можуть бути зовнішніми порушниками:

- звільнені співробітники ТОВ «СТБ 2016»;
- представники організацій, що взаємодіють з питань забезпечення життєдіяльності організації (енерго-, водо-, теплопостачання тощо);
- відвідувачі (запрошені представники організацій, громадяни) представники фірм, що постачають техніку, програмне забезпечення, послуги тощо;
- члени злочинних організацій або особи, що діють за їх завданням;
- особи, які випадково чи навмисно проникли в мережі ІС ТОВ «СТБ 2016» із зовнішніх (по відношенню до ТОВ «СТБ 2016») мереж телекомунікації (зловмисники).

Звільнені співробітники можуть використовувати для досягнення цілей свої знання про технології роботи, захисні заходи та права доступу. Отримані в ТОВ «СТБ 2016» знання і досвід виділяють їх серед інших джерел зовнішніх загроз.

Кримінальні структури представляють найбільш агресивне джерело зовнішніх загроз. Для здійснення своїх задумів ці структури можуть йти на відкрите порушення закону та залучати до своєї діяльності співробітників ТОВ «СТБ 2016» всіма доступними їм силами і засобами.

Професійні зловмисники мають найбільш високу технічну кваліфікацію та знання про слабкості програмних засобів, які використовуються в ІС. Найбільшу загрозу становлять при взаємодії з працюючими і звільненими співробітниками ТОВ «СТБ 2016» і кримінальними структурами.

Співробітники ТОВ «СТБ 2016», які займаються розробкою, постачанням і ремонтом обладнання, інформаційних систем, представляють зовнішню загрозу в силу того, що епізодично мають безпосередній доступ до інформаційних ресурсів.

2.2 Аналіз можливих ризиків інформаційної безпеки підприємства

Ризик інформаційної безпеки являє собою можливість порушення ІБ з негативними наслідками.

Основними ризиками інформаційної безпеки є:

- ризик витоку конфіденційної інформації;
- ризик втрати або недоступності важливих даних;
- ризик використання неповної або викривленої інформації;
- ризик неправомочною прихованої експлуатації інформаційно-обчислювальних ресурсів (наприклад, при створенні бот-мережі);
- ризик поширення у зовнішньому середовищі інформації, загрозової репутації організації.

У ході оцінювання ризиків інформаційної безпеки, експерти враховують те, що ризики ІБ можуть мати різну ціну (див. табл.2.1)

Таблиця 2.1 – Ступінь негативного впливу настання події ризику

Вплив на репутацію Матеріа- льний збиток	Дуже низький	Низький	Середній	Високий
Незначний	Невеликий збиток	Невеликий збиток	Середній збиток	Великий збиток
Помірний	Невеликий збиток	Середній збиток	Середній збиток	Великий збиток
Великий	Середній збиток	Великий збиток	Великий збиток	Великий збиток
Дуже великий	Великий збиток	Великий збиток	Дуже великий збиток	Дуже великий збиток
Критичний	Дуже великий збиток	Критичний збиток	Критичний збиток	Критичний збиток

Джерело: розроблено автором

На основі інтегральних показників шкоди та показників ймовірності настання подій ризику розраховуються величини наявних інформаційних ризиків (табл. 2.2).

Наведемо найбільш небезпечні загрози, з яких складаються ризики, а також їх джерела, шляхи реалізації ненавмисних та навмисних дій, що реалізують загрози для ІС ТОВ «СТБ 2016».

Таблиця 2.2 – Величини наявних інформаційних ризиків

Імовірність настання події ризiku Збиток	Дуже низька	Низька	Середня	Висока
Незначний	Невеликий ризик	Невеликий ризик	Середній ризик	Великий ризик
Помірний	Невеликий ризик	Середній ризик	Середній ризик	Великий ризик
Великий	Середній ризик	Великий ризик	Великий ризик	Великий ризик
Дуже великий	Великий ризик	Великий ризик	Дуже великий ризик	Дуже великий ризик
Критичний	Дуже великий ризик	Критичний ризик	Критичний ризик	Критичний ризик

Джерело: розроблено автором

Наведемо найбільш небезпечні загрози, з яких складаються ризики, а також їх джерела, шляхи реалізації ненавмисних та навмисних дій, що реалізують загрози для ІС ТОВ «СТБ 2016».

Найбільш небезпечними загрозами безпеці інформаційним ресурсам (ІР) ІС ТОВ «СТБ 2016» (способами нанесення шкоди суб'єктам інформаційних відносин) є:

– порушення конфіденційності (розголошення, витік) відомостей, що становлять конфіденційну інформацію ТОВ «СТБ 2016», а також персональних даних;

- порушення працездатності ІС ТОВ «СТБ 2016», блокування інформації, порушення технологічних процесів, зрив своєчасного вирішення завдань, які вирішуються в ІС;

- порушення цілісності (спотворення, підміна, знищення) інформаційних, програмних і інших ресурсів ІС ТОВ «СТБ 2016», а також фальсифікація (підробка) електронних документів.

Основними джерелами загроз безпеки інформації ІС ТОВ «СТБ 2016» являються:

- ненавмисні (помилкові, випадкові, необдумані, без злого наміру і корисливих цілей) порушення встановлених регламентів збору, обробки і передачі інформації, а також вимог безпеки інформації та інші дії співробітників (в тому числі адміністраторів) структурних підрозділів ТОВ «СТБ 2016» при експлуатації ІС ТОВ «СТБ 2016», що призводять до непродуктивних витрат часу і ресурсів, розголошення відомостей обмеженого доступу, втрати цінної інформації або порушення працездатності окремих робочих станцій, підсистем або ІС ТОВ «СТБ 2016» в цілому;

- навмисні (в корисливих цілях, з примусу третіми особами, зі злим умислом і т.п.) дії співробітників підрозділів ТОВ «СТБ 2016», допущених до роботи з ІС ТОВ «СТБ 2016», а також співробітників підрозділів Укрзалізниці, що відповідають за обслуговування, адміністрування програмного і апаратного забезпечення, засобів захисту та забезпечення безпеки інформації;

- вплив з інших логічних і фізичних сегментів ІС ТОВ «СТБ 2016» з боку співробітників інших підрозділів ТОВ «СТБ 2016», в тому числі програмістів - розробників прикладних програм, а також дистанційне несанкціоноване втручання сторонніх осіб з телекомунікаційної мережі ТОВ «СТБ 2016» і зовнішніх мереж загального призначення (перш за все Internet) через легальні і несанкціоновані канали підключення мережі ТОВ «СТБ 2016» до таких мереж, використовуючи недоліки протоколів обміну, засобів захисту та розмежування віддаленого доступу до ресурсів ІС ТОВ «СТБ 2016»;

- діяльність міжнародних і вітчизняних злочинних груп та формувань, політичних і економічних структур, а також окремих осіб з добування інформації,

нав'язування неправдивої інформації, порушення працездатності системи в цілому і її окремих компонентів;

- помилки, допущені при проектуванні ІС ТОВ «СТБ 2016» та її системи захисту, помилки в програмному забезпеченні, відмови і збої технічних засобів (у тому числі засобів захисту інформації) ІС ТОВ «СТБ 2016»;

- аварії, стихійні лиха тощо.

Шляхи реалізації ненавмисних штучних (суб'єктивних) загроз безпеки ІР в ІС ТОВ «СТБ 2016»

Користувачі, оператори, системні адміністратори і співробітники ТОВ «СТБ 2016», які обслуговують ІС ТОВ «СТБ 2016», є внутрішніми джерелами випадкових впливів, так як мають безпосередній доступ до процесів обробки інформації і можуть здійснювати ненавмисні помилки і порушення діючих правил, інструкцій та процедур.

Основні шляхи реалізації ненавмисних штучних (суб'єктивних) загроз ІС ТОВ «СТБ 2016» (дії, чинені людьми випадково, через незнання, неухважність або недбалість, з цікавості, але без злого умислу) і заходи з нейтралізації відповідних загроз і зниження можливої нанесеної ними шкоди наведені в додатку А.

Умисні дії сторонніх осіб, зареєстрованих користувачів та обслуговуючого персоналу

Основні можливі шляхи навмисної порушення роботи, виведення ІС ТОВ «СТБ 2016» з ладу, проникнення в систему і несанкціонованого доступу до інформації (з корисливими цілями, з примусу, з бажання помститися і т.п.) і заходи з нейтралізації відповідних загроз і зниження можливої нанесеної шкоди наведено в додатку Б.

Аналіз найбільш поширених методів, способів і підходів оцінки ризиків інформаційної безпеки свідчить, що всі вони базуються на певній методологічній основі, встановлюваної нормативно-правовими актами країни, політиками і стандартами організації, запозиченими і прийнятими зарубіжними національними або міжнародними стандартами, що визначають вимоги інформаційної безпеки. Згідно з попереднім аналізом найбільш значущими є рекомендації міжнародних і зарубіжних національних організацій

стандартизації, таких як ISO, NIST та ін.

Кількісна оцінка інформаційних ризиків утруднена і часто виявляється неточною і ненадійною з кількох причин: є причини притаманні всім операційним ризикам, а є причини специфічні саме для окремого типу ризиків.

По-перше складно зібрати дані, необхідні для кількісної оцінки інформаційних ризиків, оскільки потрібна точність реєстрації, її безперервність і досить тривалий період, щоб дані були придатні для побудови робочої моделі.

По-друге, сучасне інформаційне середовище схильне до частих змін через постійне вдосконалення програмного і апаратного забезпечення. Таким чином, необхідно побудувати максимально гнучку модель інформаційного середовища підприємства, яку можна було б оперативно змінювати із зміною складових цього середовища.

І по-третє, витрати часу і людських ресурсів на аналіз уразливості до ризиків досить високі, що не дозволяє проводити його з необхідною періодичністю. Для бізнесу процес грамотного систематизованого збору даних, їх відстеження і перевірка, періодичний аналіз і налагодження звітності – поки невирішене завдання. Для того щоб реалізувати цей процес, необхідно спочатку провести ідентифікацію інформаційних ризиків.

2.3 Шляхи підвищення рівня інформаційної безпеки підприємства

Для підвищення рівня захисту інформаційних ресурсів ІС ТОВ «СТБ 2016» до необхідного рівня можна визначити наступні заходи та засоби забезпечення безпеки [25]:

- правові (законодавчі);
- організаційні (адміністративні);
- програмні та програмно-апаратні.

Правові (законодавчі) заходи захисту

До правових заходів захисту відносяться діючі в країні закони, укази, постанови та нормативні акти, а також нормативні відомчі документи ТОВ «СТБ 2016», які регламентують правила поводження з інформацією в ІС, закріплюють права та обов'язки учасників інформаційних відносин у процесі її обробки та використання в ІС, а також встановлюють відповідальність за порушення цих правил, перешкоджаючи тим самим неправомірному використанню інформації і є стримуючим фактором для потенційних порушників. Правові заходи захисту носять в основному попереджувачий, профілактичний характер і вимагають постійної роз'яснювальної роботи з користувачами і обслуговуючим персоналом системи.

Повинен бути визначений відповідальний керівник в ТОВ «СТБ 2016» з питань технічного захисту інформації, а також відповідальні керівники з питань технічного захисту інформації в структурних підрозділах ТОВ «СТБ 2016».

Відповідальні керівники повинні організувати виконання вимог нормативних та нормативно-правових документів, у тому числі відомчих документів ТОВ «СТБ 2016», які регламентують порядок обробки інформації з обмеженим доступом.

Співробітникам ТОВ «СТБ 2016» повинна бути роз'яснена відповідальність, у разі порушення визначених в документах правових норм.

Організаційні (адміністративні) заходи захисту – це заходи організаційного характеру, що регламентують процеси функціонування системи обробки даних, використання її ресурсів, діяльність обслуговуючого персоналу, а також порядок взаємодії користувачів з системою таким чином, щоб найбільшою мірою ускладнити або виключити можливість реалізації загроз безпеці або знизити розмір втрат у разі їх реалізації.

Головна мета адміністративних заходів, що вживаються на вищому управлінському рівні – сформувати політику в галузі забезпечення безпеки інформації (що відображає підходи до захисту інформації) та забезпечити її виконання, виділяючи необхідні ресурси і контролюючи стан справ.

З практичної точки зору політику в галузі забезпечення безпеки інформації в ІС ТОВ «СТБ 2016» доцільно розбити на два рівні. До верхнього рівня відносяться рішення керівництва, що зачіпають діяльність ТОВ «СТБ 2016» в цілому. Прикладом таких рішень можуть бути:

- ухвалення рішення про формування або перегляд комплексної програми забезпечення безпеки інформації, визначення відповідальних за її реалізацію;
- формулювання цілей, постановка завдань, визначення напрямів діяльності в галузі безпеки інформації;
- прийняття рішень з питань реалізації програми безпеки, що розглядаються на рівні ТОВ «СТБ 2016» в цілому;
- забезпечення нормативної (правової) бази питань безпеки і т.п.

Політика верхнього рівня повинна чітко окреслити сферу впливу і обмеження при визначенні цілей безпеки інформації, визначити які ресурси (матеріальні, персонал) будуть захищені і знайти розумний компроміс між прийнятним рівнем безпеки і функціональністю ІС.

Політика нижнього рівня визначає процедури та правила досягнення цілей і вирішення завдань безпеки інформації та деталізує (регламентує) ці правила:

- якою є область застосування політики безпеки інформації;
- які ролі і обов'язки посадових осіб, що відповідають за проведення політики безпеки інформації;
- хто має права доступу до інформації обмеженого поширення;
- хто і за яких умов може читати і модифікувати інформацію і т.д.

Політика нижнього рівня повинна:

- передбачати регламент інформаційних відносин, що виключають можливість довільних, випадкових або навмисних несанкціонованих дій щодо конфіденційних інформаційних ресурсів;
- визначати принципи і методи розмежування доступу до інформації з обмеженим доступом;
- вибирати програмні та прогамно-апаратні засоби захисту від НСД, шифрування, аутентифікації, авторизації, ідентифікації та інших захисних механізмів, що

забезпечують гарантії реалізації прав і відповідальності суб'єктів інформаційних відносин.

Регламентация доступу в приміщення ТОВ «СТБ 2016»

Експлуатація захищених АРМ і серверів ІС ТОВ «СТБ 2016» повинна здійснюватися в приміщеннях, обладнаних надійними автоматичними замками, засобами сигналізації і постійно перебувати під охороною або спостереженням, що виключає можливість безконтрольного проникнення в приміщення сторонніх осіб та забезпечує фізичну схоронність ресурсів, що захищаються (АРМ, серверів, електронних документів, реквізитів доступу тощо) [26].

Після закінчення робочого дня приміщення з критичними компонентами ІС повинні здаватися під охорону.

У разі оснащення приміщень засобами охоронної сигналізації, а також автоматизованою системою прийому і реєстрації сигналів від цих засобів, прийом-здача таких приміщень під охорону повинна здійснюватись на підставі інструкції, яка затверджується керівництвом ТОВ «СТБ 2016».

Регламентация допуску співробітників до використання ресурсів ІС ТОВ «СТБ 2016»

У рамках дозвільної системи допуску встановлюється: хто, кому, яку інформацію і для якого виду доступу може надати і за яких умов; система розмежування доступу, яка передбачає визначення для всіх користувачів автоматизованої системи інформаційних і програмних ресурсів, доступних їм для конкретних операцій (читання, запис, модифікація, видалення, виконання) за допомогою програмно-апаратних засобів захисту [27].

Допуск працівників підрозділів ТОВ «СТБ 2016» до роботи з автоматизованою системою і доступ до її ресурсів повинен бути строго регламентований. Будь-які зміни складу і повноважень користувачів повинні негайно впроваджуватися в правила розмежування доступу відповідальними особами.

Рівень повноважень кожного користувача визначається індивідуально, дотримуючись таких вимог:

- відкрита, конфіденційна інформація розміщуються за можливості на різних серверах (це спрощує забезпечення захисту);
- кожен співробітник користується тільки запропонованими йому правами по відношенню до інформації, з якою йому необхідна працювати у відповідності з посадовими обов'язками;
- начальник має права на перегляд інформації своїх підлеглих тільки у встановлених межах відповідно до своїх посадових обов'язків;
- найбільш відповідальні технологічні операції повинні проводитися за правилом "у дві руки" – правильність введеної інформації підтверджується іншою посадовою особою, яка не має права введення інформації.

Всі співробітники ТОВ «СТБ 2016», допущені до роботи (користувачі) і обслуговуючий персонал ІС ТОВ «СТБ 2016», повинні нести персональну відповідальність за порушення встановленого порядку автоматизованої обробки інформації, правил зберігання, використання та передачі носіїв інформації та інформаційних ресурсів ТОВ «СТБ 2016», які перебувають у їх розпорядженні. Кожен співробітник (при прийомі на роботу) повинен підписувати зобов'язання щодо дотримання та відповідальності за порушення встановлених вимог щодо збереження конфіденційної інформації Укрзалізниці, а також правил роботи з такою інформацією в ІС ТОВ «СТБ 2016».

Обробка інформації, що захищається в ІС ТОВ «СТБ 2016» повинна проводитися відповідно до затверджених технологічних інструкцій (технічними порядками).

Регламентація процесів ведення баз даних та здійснення модифікації інформаційних ресурсів

Всі операції з ведення баз даних ТОВ «СТБ 2016» і допуск співробітників підрозділів ТОВ «СТБ 2016» до роботи з цими базами даних повинні бути суворо регламентовані (повинні проводитися відповідно до затверджених технологічних інструкцій). Будь-які зміни складу і повноважень користувачів баз даних ІС ТОВ «СТБ 2016» повинні проводитися встановленим порядком.

Розподіл імен, генерація паролів, супровід правил розмежування доступу до баз даних повинно покладатися на спеціальних користувачів - адміністраторів

конкретних баз даних. При цьому можуть використовуватися як штатні, так і додаткові засоби захисту СКБД та операційних систем.

Регламентация процесів обслуговування та здійснення модифікації апаратних і програмних ресурсів ІС ТОВ «СТБ 2016»

Всі апаратні і програмні ресурси ІС ТОВ «СТБ 2016» повинні бути встановленим порядком категорійовані (для кожного ресурсу повинен бути визначений необхідний рівень обмеження доступу).

Апаратно-програмна конфігурація автоматизованих робочих місць, на яких обробляється інформація, що захищається (з яких можливий доступ до ресурсів, що захищаються), повинна відповідати колу покладених на користувачів даного АРМ функціональних обов'язків. Усі невикористовувані в роботі (зайві) пристрої введення-виведення інформації (COM, USB порти, дисководи, безпроводні інтерфейси тощо) на таких АРМ повинні бути відключені (вилучені), не потрібні для роботи програмні засоби та інформація з дисків АРМ також повинні бути видалені.

Для спрощення супроводу, обслуговування та організації захисту АРМ повинні оснащуватися програмними засобами і конфігуруватися уніфіковано (відповідно до встановлених правил) [28].

Введення в експлуатацію нових АРМ і всі зміни в конфігурації технічних і програмних засобів існуючих АРМ в ІС ТОВ «СТБ 2016» повинні здійснюватися тільки встановленим порядком.

Програмне забезпечення в ІС ТОВ «СТБ 2016» повинно встановлюватися і використовуватися лише, якщо воно отримане встановленим відомчими документами ТОВ «СТБ 2016» порядком. Використання в ІС несанкціонованого ПЗ повинно бути заборонено.

Забезпечення і контроль фізичної цілісності (незмінності конфігурації) апаратних ресурсів ІС ТОВ «СТБ 2016»

На всіх компонентах ІС, що підлягають фізичному захисту, мають бути встановлені необхідні обмежувальні технічні засоби захисту.

Вузли та блоки компонентів, до яких доступ обслуговуючого персоналу в процесі експлуатації не потрібен, після налагоджувальних, ремонтних і інших

робіт, пов'язаних з доступом до них повинні закриватися співробітниками служби технічного захисту інформації ТОВ «СТБ 2016».

Кадрова робота (підбір та підготовка персоналу, навчання користувачів)

До початку етапу експлуатації ІС її користувачі, а також необхідний керівний та обслуговуючий персонал повинні бути ознайомлені з переліком відомостей обмеженого доступу, в частині що їх стосується, і своїм рівнем повноважень, а також з організаційно-розпорядчій, нормативній, технічній та експлуатаційній документації, що визначає вимоги та порядок обробки інформації обмеженого поширення [29].

Всі співробітники ТОВ «СТБ 2016», що використовують при роботі ІС ТОВ «СТБ 2016», повинні бути ознайомлені з організаційно-розпорядчими документами захисту ІС ТОВ «СТБ 2016» в частині, що їх стосується, повинні знати і неухильно виконувати технологічні інструкції та загальні обов'язки щодо забезпечення безпеки інформації при використанні ІС. Доведення вимог зазначених документів до осіб, допущених до обробки інформації, що захищається, повинно здійснюватися начальниками підрозділів під розпис.

Підрозділи технічного захисту інформації

Для безпосередньої організації (побудови) і ефективного функціонування системи захисту інформації в ТОВ «СТБ 2016» повинна бути створена служба технічного захисту інформації.

Служба технічного захисту інформації повинна являти собою систему штатних або позаштатних підрозділів, призначених для організації кваліфікованої розробки (вдосконалення) системи захисту інформації та організаційного (адміністративного) забезпечення її функціонування в усіх підрозділах ТОВ «СТБ 2016».

На ці підрозділи доцільно покласти вирішення таких основних завдань:

- приведення в життя політики безпеки інформації, визначення вимог до системи захисту інформації;
- організація заходів та координація робіт всіх підрозділів ТОВ «СТБ 2016» з комплексного захисту інформації;
- аудит та контроль за діями користувачів ІС;

- контроль та оцінка ефективності вжитих заходів і застосовуваних засобів захисту інформації.

Основні функції підрозділу безпеки полягають в наступному:

- формування вимог до системи захисту в процесі створення (розвитку) ІС ТОВ «СТБ 2016»;
- участь у проектуванні системи захисту, її випробуваннях та прийнятті в експлуатацію;
- планування, організація та забезпечення функціонування системи захисту інформації в процесі функціонування ІС;
- розподіл між користувачами необхідних реквізитів та прав доступу;
- спостереження за функціонуванням системи захисту і її елементів;
- організація перевірок надійності функціонування системи захисту;
- навчання користувачів і персоналу ІС правилам безпечної обробки інформації;
- регламентація дій та контроль за користувачами, адміністраторами баз даних, серверів і мережевих пристроїв (у тому числі і за діями адміністраторів безпеки);
- взаємодія з відповідальними за безпеку інформації в підрозділах ТОВ «СТБ 2016»;
- контроль за дотриманням користувачами і персоналом ІС встановлених правил поведінки з інформацією, що захищається, в процесі її автоматизованої обробки;
- вживання заходів при спробах НСД до інформації і при порушеннях правил функціонування системи захисту.

Організаційно-правовий статус служби захисту визначається наступним чином:

- чисельність служби захисту повинна бути достатньою для виконання всіх перерахованих вище функцій;
- служба захисту повинна підкорятися особі, яка несе персональну відповідальність за дотримання правил поведінки з інформацією, що захищається;

- персонал служби захисту не повинен мати інших обов'язків, пов'язаних з функціонуванням ІС;
- співробітники служби захисту повинні мати право доступу до всіх приміщень, де встановлена апаратура ІС ТОВ «СТБ 2016» і право припиняти автоматизовану обробку інформації при наявності безпосередньої загрози для інформації, що захищається;
- керівнику служби захисту має бути надано право забороняти включення в число діючих нові елементи ІС ТОВ «СТБ 2016», якщо вони не відповідають вимогам захисту інформації і це може привести до серйозних наслідків у випадку реалізації значущих загроз безпеці інформації;
- службі захисту інформації повинні забезпечуватися всі умови, необхідні для виконання своїх функцій.

Для вирішення завдань, покладених на підрозділ захисту інформації, його співробітники повинні мати такі права:

- визначати необхідність і розробляти відомчі нормативні документи, які стосуються питань забезпечення безпеки інформації, включаючи документи, що регламентують діяльність співробітників підрозділів ТОВ «СТБ 2016»;
- отримувати інформацію від співробітників підрозділів ТОВ «СТБ 2016» з питань застосування інформаційних технологій та експлуатації ІС;
- брати участь в опрацюванні технічних рішень з питань забезпечення безпеки інформації при проектуванні і розробці комплексних систем захисту інформації;
- брати участь у випробуваннях розроблених комплексних систем захисту інформації з питань оцінки якості реалізації вимог щодо забезпечення безпеки інформації;
- контролювати діяльність співробітників підрозділів ТОВ «СТБ 2016» з питань безпеки інформації.

До складу підрозділу захисту інформації повинні входити такі спеціалісти:

- відповідальні за адміністрування засобів захисту від НСД (вибір, установка, настройка, зняття засобів захисту, перегляд журналів реєстрації подій,

- оперативний контроль за роботою користувачів та реагування на події НСД і т.п.);
- відповідальні за адміністрування криптографічних засобів захисту та засобів ЕЦП (установка, налаштування, зняття таких засобів, генерація і розподіл ключів і т.д.);
 - відповідальні за вирішення питань захисту інформації в розроблюваних програмістами і впроваджуваних прикладних програмах (участь у розробці технічних завдань з питань захисту інформації, вибір засобів і методів захисту, участь у випробуваннях нових прикладних програм з метою перевірки виконання вимог із захисту інформації і т.д.).

Відповідальність за порушення встановленого порядку використання ІС ТОВ «СТБ 2016». Розслідування порушень

Будь-яке грубе порушення порядку і правил роботи в ІС співробітниками структурних підрозділів ТОВ «СТБ 2016» має розслідуватися. До винних повинні застосовуватися адекватні заходи впливу. Міра відповідальності персоналу за дії, здійснені в порушення встановлених правил забезпечення безпечної автоматизованої обробки інформації, повинна визначатися завданими збитками, наявністю злого наміру і іншими факторами на розсуд керівництва ТОВ «СТБ 2016».

Фізичні заходи захисту засновані на застосуванні різного роду механічних, електро або електронно-механічних пристроїв і споруд, спеціально призначених для створення фізичних перешкод на можливих шляхах проникнення і доступу потенційних порушників до компонентів ІС та інформації, що захищається, а також технічних засобів візуального спостереження, зв'язку та охоронної сигналізації [30].

Фізичний захист будівель, приміщень, об'єктів і засобів інформатизації повинен здійснюватися шляхом встановлення відповідних постів охорони та фізичних засобів захисту, за допомогою технічних засобів охорони або будь-якими іншими способами, що запобігають або істотно ускладнюють проникнення в будинки, приміщення сторонніх осіб, несанкціонованого доступу до компонентів ІС та інформації з обмеженим доступом [30].

Програмні та програмно-апаратні засоби захисту входять до складу систем захисту ІС ТОВ «СТБ 2016» і виконують (самостійно або в комплексі з іншими засобами) функції захисту інформації (ідентифікацію та аутентифікацію користувачів, розмежування доступу до ресурсів, реєстрацію подій, криптографічне закриття інформації і т.д.).

За результатами аналізу структури ІС ТОВ «СТБ 2016», можна визначити наступні напрямки розвитку програмно-апаратної частини систем захисту ІС ТОВ «СТБ 2016»:

- засоби ідентифікації (розпізнавання) і аутентифікації (підтвердження достовірності) користувачів;
- засоби розмежування доступу зареєстрованих користувачів системи до ресурсів ІС;
- засоби забезпечення та контролю цілісності програмних та інформаційних ресурсів;
- засоби реєстрації та контролю подій в ІС;
- засоби реєстрації та контролю дій користувачів ІС;
- засоби криптографічного захисту інформації;
- засоби антивірусного захисту інформації;
- засоби захисту ІС ТОВ «СТБ 2016» від зовнішніх вторгнень.

Кожний засіб захисту інформації, база даних, сервер або мережевий пристрій чи програмне забезпечення із функціями захисту інформації представлені лінійкою засобів, які розраховані на різну завантаженість, кількість користувачів, пропускну здатність тощо. Тому, при виборі конкретної моделі чи версії необхідно враховувати конкретне призначення, функціональність та її місце в конкретній ІС ТОВ «СТБ 2016».

Засоби ідентифікації (розпізнавання) і аутентифікації (підтвердження достовірності) користувачів

З метою запобігання роботі з ІС ТОВ «СТБ 2016» сторонніх осіб необхідно забезпечити можливість розпізнавання системою кожного законного користувача (або обмежених груп користувачів). Для цього в системі (у захищеному місці) повинен зберігатися ряд ознак кожного користувача, за якими цього користувача

можна впізнати. Надалі при вході в систему, а при необхідності – і при виконанні певних дій у системі, користувач зобов'язаний себе ідентифікувати, тобто вказати ідентифікатор, присвоєний йому в системі. Крім того, для ідентифікації можуть застосовуватися різного роду пристрої: особисті ключі ЕЦП користувача, магнітні картки, засоби біометричної ідентифікації тощо.

Автентифікація (підтвердження достовірності) користувачів повинна здійснюватися на основі використання паролів (секретних слів) або перевірки унікальних характеристик (параметрів) користувачів за допомогою спеціальних біометричних засобів або ЕЦП.

Засоби розмежування доступу зареєстрованих користувачів системи до ресурсів ІС

Після розпізнавання користувача система повинна здійснювати авторизацію користувача, тобто визначати, які права надані користувачеві: які дані і як він може використовувати, які програми може виконувати, коли, як довго і з яких терміналів може працювати, які ресурси системи може використовувати і т. п. Авторизація користувача повинна здійснюється з використанням наступних механізмів реалізації розмежування доступу:

- механізмів виборчого управління доступом, заснованих на використанні атрибутних схем, списків дозволів тощо;
- механізмів повного управління доступом, заснованих на використанні міток конфіденційності ресурсів і рівнів допуску користувачів;
- механізмів забезпечення замкнутого середовища довіреного програмного забезпечення (індивідуальних для кожного користувача списків дозволених для запуску програм), підтримуваних механізмами ідентифікації (розпізнавання) і аутентифікації (підтвердження достовірності) користувачів при їх вході в систему.

Зони відповідальності і завдання конкретних технічних засобів захисту встановлюються виходячи з їх можливостей та експлуатаційних характеристик, описаних у документації на ці засоби.

Технічні засоби розмежування доступу повинні бути складовою частиною єдиної системи контролю доступу:

- на контрольовану територію;
- в окремі приміщення;
- до елементів ІС і елементів системи захисту інформації (фізичний доступ);
- до ресурсів ІС (програмно-апаратний доступ);
- до інформаційних сховищ (носіям інформації, томам, файлів, наборів даних, архівів, довідками, записам і т.д.);
- до активних ресурсів (прикладним програмам, завданням, формам запитів тощо);
- до операційної системи, системних програм та програм захисту інформації тощо.

Засоби забезпечення та контролю цілісності програмних та інформаційних ресурсів

Контроль цілісності програм, оброблюваної інформації і засобів захисту, з метою забезпечення незмінності програмного середовища, яке визначається передбаченою технологією обробки, і захисту від несанкціонованого коригування інформації повинен забезпечуватися:

- засобами електронного цифрового підпису;
- засобами підрахунку контрольних сум;
- засобами порівняння критичних ресурсів з їх еталонними копіями (і відновлення у разі порушення цілісності);
- засобами розмежування доступу (заборона доступу з правами модифікації чи видалення).

З метою захисту інформації і програм від несанкціонованого знищення чи спотворення необхідно забезпечити:

- дублювання системних даних та важливої інформації;
- дуплексування і дзеркальне відображення даних на дисках;
- відстеження транзакцій;
- періодичний контроль цілісності операційної системи і прикладних програм, а також файлів користувачів;
- антивірусний контроль;

- резервне копіювання даних за заздалегідь визначеною схемою;
- зберігання резервних копій поза приміщенням серверу;
- забезпечення безперервності електроживлення для серверів і критичних робочих станцій і кондиціонування електроживлення для решти станцій мережі.

Для захисту інформації та програм повинний бути встановлений:

- порядок здійснення процедур резервного копіювання, переміщення, обліку, зберігання й оновлення резервних копій, перелік інформаційних ресурсів, які резервуються, періодичність, а також відповідальність за дотриманням виконання цих процедур;
- порядок здійснення процедур відновлення інформації з резервних копій, а також відповідальність за дотриманням виконання цих процедур.

Програмно-апаратні засоби для забезпечення архівування мають забезпечувати можливість керування процедурою архівування з боку відповідних осіб ІС ТОВ «СТБ 2016» (за запитом, згідно графіку, архівування тільки змін тощо). Перелічені задачі можуть бути реалізовані як вбудованими засобами мережевих, серверних компонентів та засобами баз даних, так і окремими спеціалізованими засобами.

Забезпечення безперервності електроживлення повинно реалізовуватися шляхом встановлення засобів безперервного живлення для усіх критичних компонентів мережі. Засіб безперервного живлення встановлюється відповідно до потужності компоненти ІС плюс 30-40 % потужності запасу (на розвиток) і повинні бути розраховані на визначений час роботи, якого достатньо для відновлення основного живлення ІС або її коректного завершення роботи.

Засоби реєстрації та контролю подій в ІС

Засоби контролю і реєстрації повинні забезпечувати виявлення і реєстрацію всіх подій (дій користувачів, спроб НСД і т.п.), які можуть спричинити за собою порушення політики безпеки, яка прийнята в ТОВ «СТБ 2016» і привести до виникнення кризових ситуацій, а також контролю роботи користувача ІС в рамках його службових обов'язків. Засоби контролю та реєстрації повинні надавати можливості:

- ведення та аналізу журналів реєстрації подій безпеки та системних подій. Журнали реєстрації повинні обов'язково вестися активним мережевим обладнанням, серверами, базами даних та кожною робочою станцією користувача ІС;
- оперативного ознайомлення адміністратора безпеки з вмістом журналу реєстрації будь-якого компоненту мережі;
- можливість збору журналів реєстрації компонентів ІС в одне центра-лізоване сховище для зберігання та моніторингу відповідальною особою ІС;
- отримання твердої копії (роздруківки) журналу реєстрації;
- впорядкування журналів реєстрації по днях і місяцях, а також встановлення обмежень на термін їх зберігання;
- оперативного оповіщення адміністратора безпеки про порушення.

При реєстрації подій безпеки в журналі реєстрації повинна фіксуватися така інформація:

- дата і час події;
- ідентифікатор суб'єкта (користувача, програми), що здійснює реєстроване дію;
- дію (якщо реєструється запит на доступ, то зазначається об'єкт і тип доступу).

Повинні підтримуватись наступні основні способи реагування на виявлені факти НСД (можливо за участю адміністратора безпеки):

- сповіщення адміністратора адміністратора безпеки;
- відключення терміналу (робочої станції), з якого були здійснені спроби НСД до інформації;
- виключення порушника зі списку зареєстрованих користувачів;
- подача сигналу тривоги та ін.

Засоби реєстрації та контролю дій користувачів ІС

Сучасні світові дослідження вказують на те, що від 30 до 50% інформації підприємства розголошується внутрішніми співробітниками підприємства (інсайдерами). Тому, на цей час велике розповсюдження отримали засоби реєстрації та контролю дій користувачів ІС.

Засоби реєстрації та контролю дій користувачів ІС призначені для віддаленого системного контролю керівництвом підприємства або уповноваженою особою (адміністратором) дій співробітників підприємства на комп'ютерах у складі корпоративної мережі, для збору та аналізу статистики роботи користувачів.

Засоби реєстрації та контролю дій користувачів автоматично реєструють всі дії співробітників компанії в ІС. За допомогою великої кількості різноманітних критеріїв щодо звітів і різних модулів онлайн-спостереження можна точно знати на що, і наскільки оптимально, витрачають співробітники свій робочий час, а також керівники вчасно будуть сповіщені про шкідливі дії персоналу.

Засоби антивірусного захисту інформації впроваджуються з метою:

1. Запобігання проникненню в ІС ТОВ «СТБ 2016» комп'ютерних вірусів, троянів, хробаків, деструктивних програм тощо (далі – комп'ютерні віруси) з наступних джерел:

- знімних носіїв інформації, що використовуються ІС ТОВ «СТБ 2016» в технологічних процесах обробки інформації;
- запитів із зовнішніх телекомунікаційних мереж;
- внаслідок порушення окремими категоріями користувачів ІС політики безпеки інформації;

2. Своєчасного виявлення та знешкодження комп'ютерних вірусів у випадку їх проникнення в ІС ТОВ «СТБ 2016».

3. Реєстрації, збору та обробки даних, що мають відношення до антивірусного захисту, аналіз звітів антивірусного програмного забезпечення.

Антивірусний захист ІС ТОВ «СТБ 2016» повинен забезпечити:

- безперервний захист ІС ТОВ «СТБ 2016» від вірусів;
- безперервне управління підсистемою антивірусного захисту ІС ТОВ «СТБ 2016»;
- неперервну спостережність за підсистемою антивірусного захисту ІС ТОВ «СТБ 2016».

Заходи по запобіганню проникненню вірусів в ІС ТОВ «СТБ 2016» повинні впроваджуватись в усіх її складових частинах, для яких така загроза потенційно можлива.

РОЗДІЛ 3.

Механізми управління захистом інформаційних ресурсів підприємства

3.1 Концепція створення системи управління інформаційною безпекою компанії ТОВ «СТБ 2016»

Відповідно до міжнародного стандарту ISO/IEC 27002 для того, щоб створити ефективну СУІБ необхідно обрати відповідні захисні заходи (Рис. 3.1)[4].

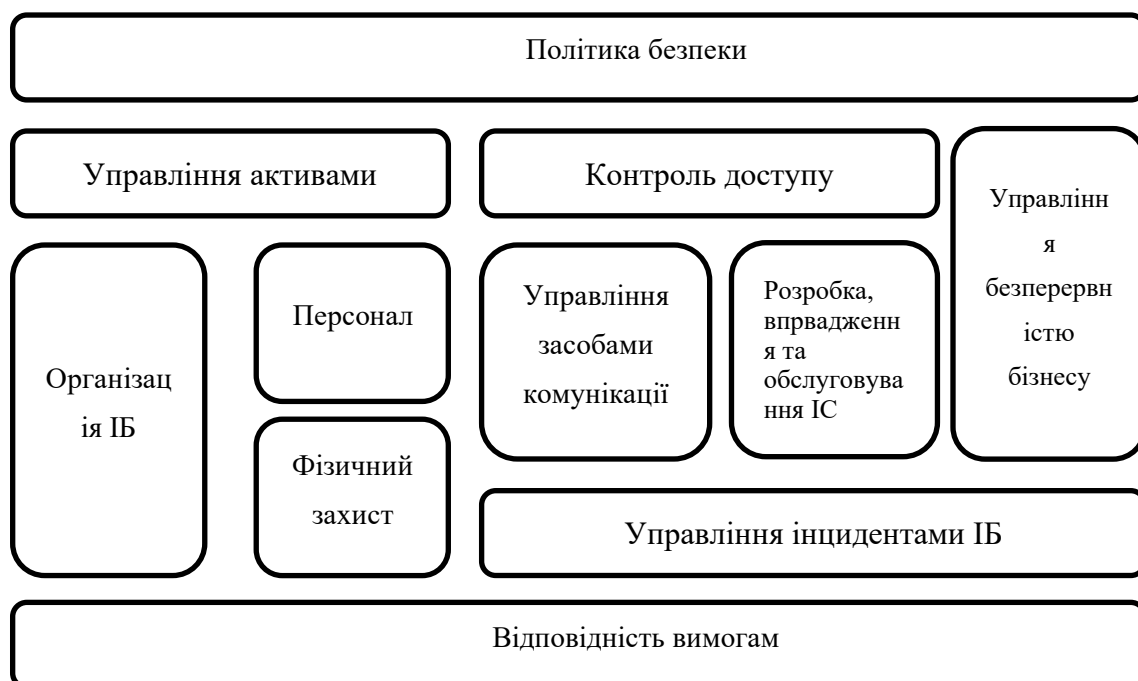


Рисунок 3.1 – Перелік захисних заходів

Джерело: розроблено автором

При створенні та вдосконаленні СУІБ в компанії необхідно залучати великі витрати, як людських ресурсів так і фінансових. У випадку інфраструктури корпоративної мережі компанії необхідно зробити багато кроків відповідно до незакритих загроз та вразливостей.

Відповідно до вимог стандарту 27001 А.11.2 «Менеджмент доступу користувачів» необхідно оформити документально процес надання користувачам

доступу до інформаційних систем, а також скасування прав доступу при звільненні співробітників. Процес надання прав доступу користувача на основі неформального прохання ускладнює перевірку того, чи були ці права дійсно надані з дозволу відповідальних посадових осіб компанії. В результаті виникає ризик того, що системний адміністратор може помилково або навмисно надати користувачам права, які вони не повинні мати. Такі випадки важко виявити.

Всі користувачі (внутрішні, зовнішні та тимчасові) та їхня діяльність в інформаційних системах (прикладні бізнес-пакети, функціонування системи, розробка та обслуговування) повинні ідентифікуватися за допомогою унікальних атрибутів. Права доступу користувачів до систем і даних повинні узгоджуватися з попередньо визначеними та документально оформленими вимогами бізнесу та посадовими обов'язками. Заявку на отримання прав доступу повинно подавати керівництво користувача, і вона повинна бути затверджена особою, відповідальною за систему, а права користування повинні надаватися особою, відповідальною за безпеку систем. Для цього необхідно запровадити офіційну процедуру подання форм заявки на отримання прав доступу. Такі форми повинні містити детальний опис прав та/або функцій, що надаються кожному користувачеві, і їх слід зберігати у централізованій базі даних. Облікові дані користувачів повинні бути деактивовані або вилучені негайно після припинення трудових відносин з користувачем.

Наступним кроком відповідно до вимог стандарту 27001 A.11.2 «Менеджмент доступу користувачів» необхідно запровадити процедуру регулярної зміни пароля в бухгалтерських програмах. Адміністратори надають користувачам пароль для початкового доступу до системи, однак система не передбачає обов'язкової зміни цього пароля при початковій реєстрації і не вимагає цього від користувача.

Відсутність регулярної зміни пароля створює ризик порушення конфіденційності та цілісності даних. Крім того, співробітники можуть розгадати пароль та отримати несанкціонований доступ до інформаційних систем. Якщо пароль для початкового доступу до системи не був змінений користувачем,

адміністратори можуть використовувати обліковий запис та пароль користувача для несанкціонованого доступу до системи.

А також паралельно запровадити процедуру звірки фактичних прав доступу користувачів до автоматизованої системи бухгалтерського обліку з тими, на які було надано запит.

Відсутність регулярного аналізу фактичних прав доступу користувачів до інформаційних систем збільшує ризик того, що фактичні права доступу будуть відрізнятися від тих, що були затверджені та надані згідно із запитом. Відсутність затверджених форм запиту на надання прав доступу та їх ведення у централізованому порядку може призвести до того, що робота засобів та систем контролю доступу до інформаційних систем буде неефективною.

Надалі для відповідності пунктам стандарту А.11.5 «Контроль доступу до операційної системи» та А.11.6 «Контроль доступу до за стосунків та інформації» необхідно розробити та прийняти посилені вимоги стосовно паролів. Параметри системи повинні використовуватися повною мірою для того, щоб посилити рівень за допомогою системи паролів. Рекомендовано встановити такі параметри:

- мінімальна довжина пароля: щонайменше вісім символів
- мінімальний строк дії пароля: щонайменше один день
- вимоги щодо складності пароля: активувати настройки, що відповідають за складність пароля
- необхідно забезпечити примусову зміну пароля після першої реєстрації в системі для того, щоб убезпечити систему від несанкціонованого доступу з боку користувачів
- строк дії пароля не повинен не повинен перевищувати шістдесят днів.

Вже тільки цими кроками компанія може підвищити свою безпеку на рівень, який дозволяє мати структуровану політику доступу та розмежування прав. Залишається тільки додати аналіз розмежування функцій в автоматизованій програмі бухгалтерського обліку відповідно до пункту А8 «Питання безпеки, пов'язані з персоналом» [4] [5]. Функції в автоматизованій системі бухгалтерського обліку об'єднані у дві категорії згідно з функціональними обов'язками працівників, по яких у подальшому розподіляються користувачі. Офіційний регулярний аналіз

розподілу функцій на рівні прикладних програм/бізнес-процесів не проводиться. Аналіз необхідний для того, щоб уникнути виконання користувачами системи несумісних функцій.

Результатом відсутності аналізу розподілу функцій в автоматизованій системі бухгалтерського обліку є ризик того, що працівник може мати у системі несумісні права, які, наприклад, дозволили б одній і тій самій особі і ініціювати, і санкціонувати критично важливі операції. Як приклад можна також навести ситуацію, коли один і той самий працівник має змогу вносити продавців до відповідної бази даних, видавати закупівельні ордери та авторизувати платежі віртуальним продавцям.

Тому необхідно розробити та впровадити офіційні процедури регулярного аналізу фактичних прав доступу користувача в автоматизованій системі бухгалтерського обліку та періодичного аналізу функціональних обов'язків, зокрема, з метою виявлення змін у процесах та потенційних конфліктів між функціями. Це дозволило б оцінювати нові процеси та функції в автоматизованій системі бухгалтерського обліку з точки зору розмежування функцій.

Якщо з логічним доступом вже все більш-менш ясно, то залишаються незакритими питання фізичного доступу та процесів безперервності бізнесу. Але і для цих аспектів інформаційної безпеки стандарт 27001 регламентує необхідні дії. Тому, відповідно до пункту А.9.1. «Зони безпеки» необхідно затвердити перелік персоналу, якому дозволено вхід до серверної кімнати та процедуру контролю доступу до серверної кімнати відвідувачів або персоналу компаній, що надають послуги з підтримки обладнання[4] [5]. Це можливо зробити відповідними засобами контролю доступу таким чином, щоб доступ до неї мав лише уповноважений персонал. Також Необхідно забезпечити фіксацію дати і часу входу та виходу третіх осіб, і при цьому дії всіх відвідувачів повинні контролюватися у випадках, якщо їх доступ не був попередньо затверджений. Доступ третім сторонам слід надавати тільки для конкретних, затверджених цілей, з наданням їм інструкцій щодо вимог до безпеки у зоні місцезнаходження серверів, а також інструкцій з питань дій у надзвичайних обставинах. Персоналу компаній, що надають послуги з підтримки обладнання, слід надавати обмежений доступ до зон дії системи

безпеки або засобів обробки конфіденційної інформації тільки згідно із запитом, і при цьому дії таких осіб повинні піддаватися моніторингу.

Повертаючись до процесів безперечності бізнесу варто зазначити, що найнеобхіднішими компонентами функціонування бізнесу безперервно є підтримка доступності та цілісності інформації. Відповідно до пунктів А.10.1.2 «Менеджмент змін» та А.10.5 «Резервування інформації» необхідно затвердити процедури управління внесенням змін до інформаційних систем та політику резервного копіювання [4] [5]. Відсутність цих документів може призвести до таких ризиків:

- ряд системних помилок можуть залишитися непоміченими, що збільшує ризик викривлення даних;
- у разі системних помилок можуть виникнути труднощі у вирішенні проблем;
- інсталювані модулі (форми, звіти тощо) можуть не повною мірою відповідати потребам користувачів або взагалі не використовуватися;
- можуть мати місце несанкціоновані зміни;
- може мати місце збільшення залежності від сторонніх розробників;
- компанія може понести додаткові витрати.

Існуюча практика резервування збільшує ризик втрати даних, створених після дати останнього резервного копіювання, внаслідок збою на жорсткому диску або через пошкодження серверу БД. За відсутності регулярного тестування резервних копій виникає ризик відсутності резервних копій для використання у разі виникнення надзвичайної ситуації.

Ці документи необхідні через те, що програмне забезпечення має інтегровану мову програмування, що дозволяє розширювати функціональні можливості системи. Персонал відділу ІТ проводить регулярні модифікації програмного забезпечення з метою забезпечення постійно зростаючих потреб Групи щодо організації бухгалтерського обліку та підготовки фінансової звітності. Запити на модифікації не завжди оформлюються документально, і при цьому немає підтверджень прийомки змін користувачами. Через відсутність реєстру змін, внесених до програмного забезпечення, відстеження таких змін по запитах з метою забезпечення їх належної авторизації стає неможливим.

Крім того, відсутнє розмежування функцій розробки та експлуатації, оскільки вбачається, що один і той самий працівник бере участь у розробці та адмініструванні системи бухгалтерського обліку.

І на останок треба додати регламент у разі виникнення інцидентів, пов'язаних з інформаційною безпекою. Необхідно впровадити офіційну процедуру реагування на інциденти з метою мінімізації шкоди в результаті порушень інформаційної безпеки, а також здійснення належного моніторингу та накопичення досвіду нейтралізації таких порушень. Вона повинна охоплювати такі питання, як доповідь про інциденти, пов'язані з інформаційною безпекою, та їхнє документування, аналіз причин виникнення таких інцидентів та вирішення пов'язаних з ними проблем, аналіз найбільш типових порушень правил інформаційної безпеки, а також процедури ескалації. Подібні інциденти мають бути:

- повідомлені контактній особі, наприклад, співробітникові служби технічної підтримки (helpdesk), співробітникові служби “гаряча лінія” або конкретному фахівцю IT;
- документально оформлені, як правило, використовуючи автоматизовану систему управління інцидентами;
- розподілені по категоріях (наприклад, порушення функціонування, зловмисні дії або порушення правил користування/неправильне використання систем);
- розподілені згідно з пріоритетом з урахуванням їх впливу та терміновості.

Вплив суттєвих інцидентів, пов'язаних з інформаційною безпекою, повинен бути оцінений фахівцем з IT, особою, відповідальною за програмний продукт з боку користувачів (“власником” системи), а також фахівцем у сфері інформаційної безпеки. Процедура реагування на інциденти повинна включати:

- аналіз першопричин;
- планування коригувальних заходів з метою недопущення впливу на безпеку
- обмеження доступу на час вживання коригувальних заходів
- документальне оформлення вжитих коригувальних заходів
- проведення аналізу з метою забезпечення того, щоб інцидент або заходи з його усунення не вплинули на інформаційну безпеку.

Необхідно проаналізувати найбільш типові порушення інформаційної безпеки з метою виявлення потенційної вразливості системи інформаційної безпеки та мінімізації можливості виникнення подібних інцидентів, що призводять до порушення роботи певних систем у майбутньому. Після виконання всіх рекомендованих дій можна говорити про підняття СУІБ на рівень, який функціонуватиме вже незалежно від того, хто керуватиме підрозділами, бо створена система – уніфікована.

3.2 Економічні та інші показники захищеності інформаційних ресурсів

У зв'язку з тим, що багато показників інформаційних систем, пов'язаних з аспектом інформаційної безпеки є якісними, а не кількісними, тоді в якості способу перевірки ступеня захищеності інформаційної системи використовується експертний метод.

Попередньо було проведено аудит інформаційної системи ТОВ «СТБ 2016», проаналізовано моделі загроз та модель порушника. Було виявлено загрози інформаційній безпеці та вразливості системи захисту інформаційної безпеки.

Виявлені загрози інформаційної безпеки:

Загрози, зумовлені порушеннями функціонування технічних засобів:

1. Дія потужного магнітного поля на магнітні носії інформації або обладнання, що призводить до руйнування інформації.
2. Відмови і збої компонент інформаційної інфраструктури (серверів, робочих станцій, комутаторів).

Загрози, зумовлені ненавмисними діями суб'єктів доступу:

1. Помилки системного адміністратора.
2. Помилки розробників у розробці ПЗ.
3. Помилки адміністратора безпеки при призначенні прав доступу.

Загрози, зумовлені зловмисними діями персоналу:

1. Модифікація, підміна чи спотворення технологічної інформації.

2. Фізичне руйнування автоматизованої системи або виведення з ладу важливих її елементів.

Загрози, зумовлені зловмисними діями суб'єктів з боку мережі загального користування:

1. НСД до сервісів передачі даних та до програмного забезпечення серверу.
2. Блокування сервісів передачі даних серверу СВ шляхом перевантаження його ресурсів.
3. Підміна даних IP- пакетів внаслідок використання вразливостей протоколів стеку TCP/IP, відповідних сервісів та застосувань (атаки типу "посередник").

Виявлені вразливості існуючої системи захисту інформації:

1. Недосконалість системи моніторингу подій інформаційної безпеки.
2. Відсутність процесу управління інцидентами інформаційної безпеки.
3. Відсутність процесу оцінки ризиків інформаційної безпеки.
4. Перевантаження працівників служби захисту інформації (Адміністратора інформаційної безпеки та Адміністратора системи).
5. Невиконання вимог політики інформаційної безпеки та правил інформаційної безпеки персоналом підприємства.

Забезпечення вімагаємого рівня захисту інформації в ІС підприємства в умовах впливу загроз ІБ потребує повної і достовірної оцінки усіх параметрів ІС і системи захисту інформації.

Нехай існує кінцева множина загроз ІБ, які характеризуються відносними частотами виникнення P_i^{B3} і збитком, що отримає підприємство u_i , де $i = \overline{1, n}$ номер загрози ІБ.

СЗІ виконує функцію протидії реалізації загроз. Основною характеристикою будь-якого засобу захисту є можливість зберігання кожного k -го ресурсу при впливу на нього i -й загрози P_{ki}^C , яка пов'язана з можливістю реалізації загрози P_i^{P3} через співвідношення $P_{ki}^C = 1 - P_{ki}^{P3}$.

Збитки ІС, якщо відсутня СЗІ, можуть бути представлені як додані за кожною загрозою $U = \sum_{i=1}^n u_i$.

В свою чергу, остаточний збиток, тобто збиток, який при будь-яких обставинах (і при існуванні СЗІ) буде нанесений ІС, також може представляти суму втрат від усіх загроз $W = \sum_{i=1}^n w_i$.

Тут зломисники можуть використовувати нові способи та засоби порушення властивостей інформації, що призведе до відповідної суми втрат від усіх загроз.

Ризик для ІС при відсутності СЗІ представляє собою функцію відносних частот виникнення загроз і збитку у випадку порушення класичних властивостей інформації $R^{ПЗ} = \sum_{i=1}^n P_i^{БЗ} \cdot u_i$,

а ризик для ІС при існуванні СЗІ залежить також від можливостей зберігання ІР $R^{ЗАХ} = \sum_{i=1}^n P_i^{БЗ} \cdot u_i (1 - P_i^C)$,

тут $R^{ПЗ}$ - ризик порушення захисту.

Враховуючи ймовірнісний характер загроз, можна замінити запобігання збитку $\Delta W = U - W$ на усунений ризик $\Delta R = R^{ПЗ} - R^{ЗАХ}$. Тоді економічна ефективність функціонування СЗІ може бути визначена як $Ef = \frac{R^{ПЗ} - R^{ЗАХ}}{S_{СЗІ}}$.

Для розрахунку економічної ефективності необхідно визначити перелік ІР та їх вартість, а також провести експертизу таких параметрів ІС як значимість уразливостей і ступень впливу кожної загрози на усі ІР ІС. Але достовірна експертиза параметрів ІС можлива тільки на основі визначення повного списку актуальних загроз і уразливостей, при умові адекватної оцінки ступеня виконання якісних і кількісних вимог до СЗІ.

Збиток, що наноситься i -ю загрозою u_i ІС при відсутності СЗІ, може бути визначений в абсолютних одиницях: економічних втратах, часових втратах, обсягах знищеної або пошкодженої інформації і т. п.

Тобто, збиток від порушення властивостей інформації, яка захищена – це функція двох параметрів: ступень впливу i -ї загрози на k -й ІР і вартість ресурсу - $S_{IP.k}$.

Ступень впливу повинна бути визначена експертним шляхом за лінгвістичною таблицею 3.1 і внесена в матрицю:

$$M_j^Q = \begin{bmatrix} q_{11}^j & q_{12}^j & \dots & q_{1z}^j \\ q_{21}^j & q_{22}^j & \dots & q_{2z}^j \\ \vdots & \vdots & \ddots & \vdots \\ q_{n1}^j & q_{n2}^j & \dots & q_{nz}^j \end{bmatrix},$$

де j – номер експерта,

n – кількість загроз ІБ,

z – кількість ІР,

$0 \leq q_{ik}^j \leq 1$ – ступень впливу i – ї загрози ІБ на k – й ІР.

Таблиця 3.1 – Цінність інформаційного ресурсу (за ранговою шкалою)

Лінгвістична оцінка цінності ресурсів на основі розрахунку витрат на поновлення	Значення рангу
Даний інформаційний ресурс є важливим для підприємства. Його втрата несе невиправлені наслідки для підприємства.	9
Витрати на ліквідацію наслідків втрати ресурсу співставлені з річними економічними показниками	8
Витрати на ліквідацію наслідків втрати ресурсу співставлені з квартальними економічними показниками	7
Витрати на ліквідацію наслідків втрати ресурсу співставлені з місячними економічними показниками	6
Витрати на ліквідацію наслідків втрати ресурсу співставлені з тижневими економічними показниками	4
Витрати на ліквідацію наслідків втрати ресурсу співставлені з економічними показниками за добу	3
Витрати на поновлення несуттєві, але потрібен додатковий час	2
Поновлення втрати ресурсу буде проведено в штатному режимі	1

Джерело: розроблено автором

Отже остання формула набуває такого вигляду:

$$S \cdot q_i^j = \sum_{k=1}^n q_{ik}^j, \forall k = \overline{1, z}, \forall j = \overline{1, m} \quad (3.1)$$

показує сумарний збиток для k -го ІР і не повинна бути більш ніж $S_{IP.k}$.

При достатньо великій кількості загроз ІБ та їх впливу на множину ресурсів така умова може бути порушена. Тоді стовчики матриці треба масштабувати.

ВИСНОВКИ

Визначено особливості та специфіку інформаційної безпеки підприємства ТОВ «СТБ 2016», як соціально-економічну систему, яка складається з певних складових та визначається станом захищеності підприємств, і залежить від внутрішніх і зовнішніх загроз (загрози інформаційної безпеки, точки уразливості інформаційної системи, основні інформаційні ресурси, склад елементів інформаційної системи, схильних до впливу загроз, складу елементів системи захисту інформації, переліку кількісних та якісних вимог до системи захисту інформації) та характеризується властивістю до адаптації щодо зміни умов функціонування та здатністю протистояти загрозам.

Доведено, що особливості інформаційної безпеки підприємства мають взаємозалежність та взаємозв'язок, пов'язаний з витратами і вартістю інформаційної системи, ризиків для незахищеної системи, ризиків для захищеної системи.

Сформовано методологічну платформу формування та управління інформаційною безпекою підприємства ТОВ «СТБ 2016», у межах якої виділено функції (основні та з'єднання - комунікації, прийняття рішень), завдання (цілепокладання, стабілізація, виконання розробленої програми, відстеження, оптимізація), закони й базові принципи управління інформаційною безпекою.

Визначено основні тенденції розвитку інформаційної безпеки підприємства, обумовлені впливом зовнішнього середовища. Для конкретизації впливу чинників зовнішнього середовища на інформаційну безпеку підприємства, запропоновано науково-методичний підхід оцінювання впливу на базі кількісних методів, який в межах трьох блоків (формування інформаційної системи оцінювання, аналітичний, результативний) дозволив визначити фактори впливу на інформаційну безпеку підприємства серед існуючої сукупності зовнішніх чинників, визначивши вагомість їх впливу та взаємозв'язок.

Обґрунтовано можливість застосування існуючих методичних підходів до оцінювання рівня підтримування інформаційної безпеки підприємства та

визначено доцільність використання методів математичного моделювання та доречність застосування загальних принципів економічного оцінювання визначення ціни і витрат на створення й експлуатацію комплексної системи захисту інформації, та зокрема, окремих її елементів;

Запропоновано науково-методичний підхід до вартісного оцінювання ІР й запобігання шкоди інформаційній безпеці підприємства ТОВ «СТБ 2016», який відповідає розробленій концепції управління інформаційною безпекою. Цей методичний підхід базується на загальних економічних законах і методах аналізу, і специфічних методичних підходах до аналізу ймовірностей виникнення загроз інформаційної безпеки, накопиченні специфічних статистичних даних оцінювання ймовірностей щодо усунення загроз безпеки, формуванні стійких уявлень про чинники, під впливом яких функціонують інформаційні системи та засоби захисту інформації.

Для забезпечення однозначності результатів оцінювання економічної доцільності системи захисту інформаційної безпеки підприємства, запропоновано формули, які дозволяють встановити рівень економічної ефективності захищеності інформаційної системи підприємства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Технології контролю та відстежуваність вразливостей інформаційної безпеки [Електронний ресурс] URL: http://www.infobezpeka.com/publications/SIEM_osobennosti_siem/
2. Бегун А. В., Осипова О.І., Урденко О.Г. Ситуаційний лог-менеджмент інформаційної безпеки підприємства // Моделювання та інформаційні системи в економіці. Міжвідомчий наук. збірник. Вип. №95. – К.: КНЕУ, 2018. – С.18- 29.
3. Впроваджувальні технології забезпечення інформаційної безпеки [Електронний ресурс] URL: <http://www.infobezpeka.com/products/>
4. НОРМАТИВНИЙ АСПЕКТ ПОБУДОВИ ТА ВПРОВАДЖЕННЯ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ/ М.Ю. Комаров, С.Ф. Гончар, А.В. Ониськова, Київ [Електронний ресурс] URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbisnbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/Mtit_2018_82_8.pdf
5. Урденко О.Г. Системний аналіз ризиків управління інформаційною безпекою видовищних заходів / Моделювання та інформаційні системи в економіці. Міжвідомчий наук. Збірник. Вип. №98. –К.: КНЕУ 2019.
6. ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements [Електронний ресурс] URL: <https://www.iso.org/standard/54534.html>
7. Sobchuk, V., Pichkur, V., Barabash, O., Laptiev, O., Kovalchuk, I., Zidan, A. (2020). Algorithm of control of functionally stable manufacturing processes of enterprises. 2020 IEEE 2nd International Conference on Advanced Trends in Information Theory (IEEE ATIT 2020) Conference Proceedings. Kyiv, 206–211.
8. Benson, V., Saridakis, G., Tennakoon, H., Ezingard, J. N. (2015). The role of security notices and online consumer behaviour: An empirical study of social

networking users. International Journal of Human-Computer Studies, 80, 36–44. doi: <http://doi.org/10.1016/j.ijhcs.2015.03.004>

9. Mvungi, B., Iwaihara, M. (2015). Associations between privacy, risk awareness, and interactive motivations of social networking service users, and motivation prediction from observable features. Computers in Human Behavior, 44, 20–34. doi: <http://doi.org/10.1016/j.chb.2014.11.023>

10. **Control** Objectives for Information and Related Technology. – Access mode : www.isaca.org/Knowledge-Center/cobit/Pages/Overview.

11. **Risk** Management Guide for Information Technology Systems. – Access mode : www.csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

12. URL: <https://www.minregion.gov.ua/press/news/ukrayinski-budivelniki-toruyut-shlyahi-integratsiyi-do-globalnogo-budivelnogo-prostoru/> (дата звернення 13.02.2023)(11)

13. URL: <https://www.ukrinform.ua/rubric-uarazom/3481537-v-op-nazvali-kraini-aki-gotovi-vzati-ucast-u-vidbudovi-ukraini.html> (дата звернення 05.09.2022)(37)

14. URL: https://dbn.co.ua/publ/osnovni_shljakhi_pidvishhennja_jakosti_budivnictva/2-1-0-170 (дата звернення 06.09.2022)(36)

15. Серьогіна Д.О., Т.А. Пушкар Т.А., Жовтяк Г.А. «Вплив будівельної галузі на соціально-економічний розвиток територій» НАУКОВИЙ ВІСНИК НАЦІОНАЛЬНОЇ АКАДЕМІЇ СТАТИСТИКИ, ОБЛІКУ ТА АУДИТУ, 2021, № 1-2 стор. 63.

16. URL: https://dbn.co.ua/publ/osnovni_shljakhi_pidvishhennja_jakosti_budivnictva/2-1-0-170 (дата звернення 06.09.2022)

17. URL: <https://www.ukrinform.ua/rubric-uarazom/3481537-v-op-nazvali-kraini-aki-gotovi-vzati-ucast-u-vidbudovi-ukraini.html> (дата звернення 05.09.2022)

Додатки

Додаток А

Таблиця А.1 – Основні шляхи реалізації ненавмисних штучних (суб'єктивних) загроз

Основні шляхи реалізації ненавмисних штучних (суб'єктивних) загроз ТОВ «СТБ 2016»	Заходи щодо нейтралізації загроз та зниження можливої шкоди
Дії співробітників ТОВ «СТБ 2016», що призводять до часткової або повної відмови системи або порушення працездатності апаратних чи програмних засобів; відключення обладнання або зміна режимів роботи пристроїв і програм; руйнування інформаційних ресурсів системи (ненавмисне псування обладнання, видалення, спотворення програм або файлів з важливою інформацією, системних програм, пошкодження каналів зв'язку, ненавмисне псування носіїв інформації тощо)	1. Організаційні заходи (регламентація дій, введення заборон). 2. Застосування фізичних засобів, що перешкоджають ненавмисному скоєнню порушення. 3. Застосування технічних (апаратно-програмних) засобів розмежування доступу до ресурсів. 4. Резервування критичних ресурсів.
Несанкціонований запуск технологічних програм, здатних при некомпетентному використанні викликати втрату працездатності системи (зависання або зациклення) або здійснити незворотні зміни в системі (форматування або реструктуризацію носіїв інформації, видалення даних і т.п.)	1. Організаційні заходи (видалення всіх потенційно небезпечних програм з АРМ). 2. Застосування технічних (апаратно-програмних) засобів розмежування доступу до технологічних і інструментальних програм з АРМ.
Несанкціоноване впровадження та використання неврахованих програм (ігрових, навчальних, технологічних та інших, які не є необхідними для виконання співробітниками своїх службових обов'язків) з подальшим необґрунтованим витрачанням ресурсів (процесорного часу, оперативній	1. Організаційні заходи (введення заборон). 2. Застосування технічних (апаратно-програмних) засобів, що перешкоджають несанкціонованому впровадженню та використанню неврахованих програм.

пам'яті, пам'яті на зовнішніх носіях і т.п.)	
Ненавмисне зараження комп'ютера вірусами	1. Організаційні заходи (регламентація дій, введення заборон). 2. Технологічні заходи (застосування спеціальних програм виявлення та знищення вірусів). 3. Застосування апаратно-програмних засобів, що перешкоджають зараженню комп'ютерів комп'ютерними вірусами.
Розголошення, передача або втрата атрибутів розмежування доступу (паролів, ключів шифрування або ЕЦП, ідентифікаційних карток, перепусток тощо)	1. Організаційні заходи (регламентація дій, введення заборон, посилення відповідальності). 2. Застосування фізичних засобів забезпечення збереження зазначених реквізитів.
Ігнорування організаційних обмежень (встановлених правил) при роботі в системі	1. Організаційні заходи (посилення відповідальності та контролю). 2. Використання додаткових фізичних і технічних засобів захисту.
Некомпетентне використання, налаштування або неправомірне вимкнення засобів захисту персоналом підрозділу безпеки	Організаційні заходи (навчання персоналу, посилення відповідальності та контролю).
Введення помилкових даних	1. Організаційні заходи (посилення відповідальності та контролю). 2. Технологічні заходи контролю за помилками операторів.

Таблиця Б.1 – Основні можливі шляхи навмисної дезорганізації роботи

Основні можливі шляхи навмисної дезорганізації роботи, виведення ІС ТОВ «СТБ 2016» з ладу, проникнення в систему і НСД до інформації (з корисливими цілями, з примусу, з бажання помститися і т.п.)	Заходи щодо нейтралізації загроз та зниження можливого завдається шкоди
Фізичне руйнування або виведення з ладу всіх або окремих найбільш важливих компонентів автоматизованої системи (пристроїв, носіїв важливої системної інформації, бази даних, мережеві пристрої, сервери та т.п.), відключення або виведення з ладу підсистем забезпечення функціонування обчислювальних систем (електроживлення, ліній зв'язку та т. п.)	1. Організаційні заходи (регламентація дій, введення заборон). 2. Застосування фізичних засобів, що перешкоджають ненавмисному скоєнню порушень. 3. Резервування критичних ресурсів. 4. Постійна автоматична або за запитом реєстрація дій персоналу.
Розкрадання носіїв інформації (роздруківок, носіїв інформації, запам'ятовуючих пристроїв і цілих ПК), розкрадання виробничих відходів (роздруківок, записів, списаних носіїв інформації тощо)	Організаційні заходи (організація та регламентація зберігання і використання носіїв інформації).
Несанкціоноване копіювання носіїв інформації, читання залишкової інформації з оперативної пам'яті і з зовнішніх запам'ятовуючих пристроїв	1. Організаційні заходи (організація зберігання і використання носіїв з захищається). 2. Застосування технічних засобів розмежування доступу до ресурсів, що захищаються і автоматичної реєстрації отримання твердих копій документів. 3. Постійна автоматична або за запитом реєстрація дій персоналу.
Незаконне отримання паролів та інших реквізитів розмежування доступу (агентурним шляхом, використовуючи халатність користувачів, шляхом підбору, шляхом імітації інтерфейсу системи програмними закладками і т.д.) з подальшою маскуванням під зареєстрованого користувача.	1. Організаційні заходи (регламентація дій, введення заборон, робота з кадрами). 2. Застосування технічних засобів, що перешкоджають впровадженню програм перехоплення паролів, ключів та інших реквізитів. 3. Постійна автоматична або за запитом реєстрація дій персоналу.

Несанкціоноване використання АРМ користувачів, що мають унікальні фізичні характеристики, такі як номер та адресу робочої станції в мережі, фізичну адресу, адресу в системі зв'язку і т.п.	1. Організаційні заходи (сувора регламентація доступу в приміщення та допуску до робіт на даних АРМ). 2. Застосування фізичних і технічних засобів розмежування доступу. 3. Постійна автоматична або за запитом реєстрація дій персоналу.
Несанкціонована модифікація програмного забезпечення - впровадження програмних "закладок" і "вірусів" ("троянських коней" і "жучків"), тобто таких програм, які не потрібні для здійснення заявлених функцій, але дозволяють долати систему захисту, таємно і незаконно здійснювати доступ до системних ресурсів з метою реєстрації та передачі інформації, що захищається чи порушення функціонування ІС.	1. Організаційні заходи (сувора регламентація допуску до робіт). 2. Застосування фізичних і технічних засобів розмежування доступу та програм, що перешкоджають несанкціонованій модифікації апаратно-програмної конфігурації АРМ. 3. Застосування засобів контролю цілісності програм. 4. Постійна автоматична або за запитом реєстрація дій персоналу.
Порушення цілісності (спотворення, підміна, знищення) інформаційних ресурсів ІС ТОВ «СТБ 2016», у тому числі електронних документів.	1. Організаційні заходи (сувора регламентація допуску до робіт). 2. Застосування інфраструктури електронного цифрового підпису.
Відмова від авторства відправника та отримувача електронного документу.	1. Організаційні заходи (сувора регламентація допуску до робіт). 2. Застосування інфраструктури електронного цифрового підпису.
Перехоплення даних, переданих по телекомунікаційних каналах, та їх аналіз з метою отримання конфіденційної інформації та з'ясування протоколів обміну, правил входження в зв'язок і авторизації користувачів і подальших спроб їх імітації для проникнення в систему	1. Фізичний захист телекомунікаційних каналів. 2. Застосування засобів криптографічного захисту переданої інформації.

Втручання в процес функціонування ІС ТОВ «СТБ 2016» з мереж загального користування з метою несанкціонованої модифікації даних, доступу до конфіденційної інформації, порушення роботи АС і т.п.	1. Організаційні заходи (регламентація підключення та роботи в мережах загального користування). 2. Застосування спеціальних технічних засобів захисту (міжмережевих екранів, засобів контролю захищеності і виявлення атак на ресурси системи і т.п.). 3. Постійна автоматична або за запитом реєстрація дій персоналу.
---	--

Ім'я користувача:
Комп'ютерної математики та інформаційної безпеки...

ID перевірки:
1016335442

Дата перевірки:
08.06.2024 16:33:07 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
08.06.2024 16:36:01 EEST

ID користувача:
100005746

Назва документа: Диплом_РУДУХА

Кількість сторінок: 76 Кількість слів: 15921 Кількість символів: 123820 Розмір файлу: 548.83 KB ID файлу: 1016136079

Виявлено модифікації тексту (можуть впливати на відсоток схожості)

29.5%
Схожість

Найбільша схожість: 13.2% з джерелом з Бібліотеки (ID файлу: 1014880043)

13.7% Джерела з Інтернету 431 Сторінка 78

23.5% Джерела з Бібліотеки 292 Сторінка 82

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи 690

Підозріле форматування 1
сторінка