

Центральноукраїнський національний технічний університет

(повне найменування вищого навчального закладу)

Факультет економіки та менеджменту

(повне найменування інституту, назва факультету (відділення))

Кафедра „Економіка, менеджмент та комерційна діяльність”

(повна назва кафедри (предметної, циклової комісії))

*Допущена до захисту:*

Завідувач кафедри економіки,  
менеджменту та комерційної  
діяльності

д.е.н., професор

\_\_\_\_\_ О.М. Левченко

(протокол засідання кафедри ЕМ та КД

№ \_\_\_\_\_ від „\_\_” \_\_\_\_\_ 20\_\_ р.)

# Випускна кваліфікаційна робота

за другим (магістерським) рівнем вищої освіти

на тему: «Управління інформаційною безпекою торговельного підприємства»

Виконала: студентка 2 курсу, групи УФЕБ-19М-1,4  
спеціальності 073 «Менеджмент (Управління фінансово-  
економічною безпекою)»

(шифр і назва спеціальності)

Житня Валерія Андріївна

(прізвище, ініціали, підпис)

Керівник к.е.н., проф, Левченко А.О. \_

(наук.ст., вч.звання, прізвище, ініціали, підпис)

Рецензент Бугенко В.В., директор

ТОВ ТД «Гранд-Трейд»

(прізвище, ініціали, посада)

Рецензент д.е.н., проф, Шалімова Н.С, декан ФОФ

(прізвище, ініціали, посада)

м. Кропивницький – 2020 рік

## ЗМІСТ

|                                                                                                                       |    |
|-----------------------------------------------------------------------------------------------------------------------|----|
| ВСТУП                                                                                                                 | 4  |
| РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ВИВЧЕННЯ ПОНЯТТЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТОРГОВЕЛЬНОГО ПІДПРИЄМСТВА                         | 9  |
| 1.1. Основні підходи до визначення поняття інформаційної безпеки підприємства                                         | 9  |
| 1.2. Ключові ризики інформаційної безпеки сучасних підприємств сфери торгівлі                                         | 18 |
| 1.3. Вітчизняний і зарубіжний досвід використання сучасних засобів захисту інформації                                 | 22 |
| РОЗДІЛ 2. ОЦІНКА РІВНЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТОРГОВЕЛЬНОГО ПІДПРИЄМСТВА                                               | 29 |
| 2.1. Загальна характеристика підприємства ТОВ ТОРГОВИЙ ДІМ «Гранд-Трейд»                                              | 29 |
| 2.2. Аналіз основних показників торгового підприємства та результатів його діяльності                                 | 33 |
| 2.3. Ідентифікація та оцінка інформаційних активів досліджуваного підприємства                                        | 37 |
| РОЗДІЛ 3. УДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТОРГОВЕЛЬНОГО ПІДПРИЄМСТВА                                              | 53 |
| 3.1. Доцільність розробки структури VPN мережі на досліджуваному підприємстві                                         | 53 |
| 3.2. Впровадження стратегії спрямованості захисних заходів у ТОВ ТОРГОВИЙ ДІМ «Гранд-Трейд» та інформаційної політики | 56 |
| 3.3. Обґрунтування економічної доцільності запропонованого проекту                                                    |    |
| ВИСНОВКИ                                                                                                              | 81 |
| СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ                                                                                            | 83 |
| ДОДАТКИ                                                                                                               | 86 |

## ВСТУП

Актуальність теми. На сучасній стадії еволюції нашого суспільства деякі традиційні ресурси людського розвитку потроху втрачають своє первісне призначення. На зміну їм приходять нові ресурси, єдині продукти не убувають, а зростають з часом. Вони носять назву інформаційних ресурсів. Інформація стала в даний час основним ресурсом науково-технічного і соціально-економічного прогресу у світовому співтоваристві. Чим більшою мірою і з більшою швидкістю впроваджують якісну інформацію в економіку і спеціальні галузі господарства, тим вище стає життєвий рівень населення, а також економічні, військові та політичні можливості держави.

На даний момент налагоджена і широко розподілена мережа інформаційних і обчислювальних комплексів відіграє таку ж важливу роль в житті, яку в минулому мали електрифікація, телефонізація, радіо і телебачення, взяті разом. Яскравий приклад цього твердження стала поява розвитку глобальної інформаційної мережі Internet. В даний час говорять про новий виток спіралі розвитку суспільних формацій - інформаційне суспільство.

Будь-яка діяльність в області підприємництва є тісно пов'язаною з прийманням, накопиченням, збереженням, обробкою і застосуванням різних інформаційних потоків. Цілісність існуючого світоустрою як єдиного глобального співтовариства забезпечує, в основному, інтенсивний інформаційний обмін. Зупинка глобальних інформаційно-комунікаційних потоків навіть на зовсім короткий проміжок часу здатна приводити до такою ж криз, ніж розриви міждержавних економічних зв'язків. Тому, в нових ринково-конкурентних умовах з'являється велика кількість нових проблем, які пов'язані не тільки із забезпеченням цілісності і конфіденційності комерційних, фінансових або підприємницьких даних як видів інтелектуальної власності, але також і фізичних і юридичних осіб, їх майнової власності і особистої безпеки.

Актуальність вирішення цих проблем і зумовила проведення дослідження питань теорії, методики і практики забезпечення інформаційної безпеки на підприємстві, застосовуючи сучасні засоби захисту інформації від несанкціонованого доступу.

Проблема удосконалення управління інформаційною безпекою підприємствами досить багатогранна. Цьому питанню присвячені дослідження таких вчених як: І. Близнюк, О. Братель, В. Бондаренко, О. Горбатюк, М. Гуцалюк, М. Камлик, Г. Козаченко, О. Ляшенко, С. Норкатт, В. Остроухов, В. Пономарьов, С. Рамазанов, А. Стрельцов, В. Цимбалюк, В. Щербина та багато інших.

Інформаційною безпекою називається комплекс заходів щодо захисту даних від несанкціонованого доступу, руйнувань, модифікацій, розкриттів або затримки при доступі. В інформаційну безпеку включаються заходи щодо захисту процесу створення інформації, її введення, обробки і виведення. Мета інформаційної безпеки полягає в тому, щоб убезпечити цінність систем, захищати і гарантувати точність і цілісність даних, а також мінімізувати наслідки, які можуть виникнути в тому випадку, коли дані будуть модифіковані або зруйновані. В рамках інформаційної безпеки потрібно облік всіх дій, в ході яких інформація створюється, піддається модифікації, коли до неї здійснюється доступ або вона поширюється по мережі.

Мета дослідження. Метою написання випускної кваліфікаційна роботи є вивчення теоретичних аспектів забезпечення фінансово-економічної безпеки, застосовуючи сучасні засоби захисту інформації від несанкціонованого доступу, розрахунок основних показників і коефіцієнтів фінансово-економічної та інформаційної безпеки, а також розробка заходів щодо поліпшення фінансово-економічної безпеки підприємства в цілому, використовуючи сучасні засоби захисту інформації.

Завдання дослідження. Досягнення поставленої мети зумовило необхідність постановки та розв'язання наступних задач:

- визначити суть поняття «інформаційна безпека підприємства»;

- охарактеризувати ключові ризики інформаційної безпеки сучасних підприємств сфери торгівлі;
- вивчити вітчизняний і зарубіжний досвід використання сучасних засобів захисту інформації;
- розглянути характеристику досліджуваного підприємства та здійснити оцінку основних показників діяльності торговельного підприємства;
- здійснити ідентифікацію та оцінку інформаційних активів досліджуваного підприємства;
- розробити напрями удосконалення інформаційної безпеки торговельного підприємства шляхом обґрунтування доцільності розробки структури VPN мережі на досліджуваному підприємстві, впровадження стратегії спрямованості захисних заходів та інформаційної політики, а також здійснення оцінки економічної доцільності запропонованого проєкту.

Об'єкт і предмет дослідження. Об'єктом дослідження є процес управління інформацією безпекою на вітчизняних торговельних підприємствах. Предметом дослідження є удосконалення управління інформаційною безпекою торговельного підприємства. Конкретні дослідження проводилися з використанням матеріалів Товариства з обмеженою відповідальністю ТОРГОВИЙ ДІМ «Гранд-трейд».

При проведенні дослідження використовувалися наступні загальні та спеціальні методи: аналізу і синтезу, індукції та дедукції, аналітичний, групування, порівняння, класифікації, коефіцієнтний, методи фінансового та економічного аналізу.

Інформаційна база дослідження. Інформаційною основою дослідження слугують наукові праці вітчизняних та зарубіжних вчених з досліджуваного напрямку, збірників тез науково-практичних конференцій і семінарів, періодичні та монографічні фахові видання, довідково-інформаційні видання, законодавчі та нормативні документи України, опубліковані статистичні дані, інтернет-ресурси, а також фінансова звітність досліджуваного

підприємства.

Наукове та практичне значення одержаних результатів. Наукове значення одержаних результатів полягає у розробці покрокової процедури виявлення проблем у сфері забезпечення інформаційної безпеки торговельних підприємств, встановлено, що однією із найбільш значущих виступає проблема забезпечення надійного збереження та встановлення статусу застосування інформації, яка циркулює і обробляється в розподіленій інформаційній системі.

Результати досліджень можуть бути використані при розробці практичних рекомендацій щодо підвищення рівня інформаційної безпеки на торговельних підприємствах шляхом впровадження ними структури VPN мережі, яка дозволяє забезпечити централізоване управління, високу пропускну здатність, високу надійність та відмовостійкість, простоту впровадження та експлуатації, віддалене оновлення та, що є вкрай важливим, оптимізувати штат співробітників.

Апробація результатів дослідження та їх публікація. Результати дослідження оприлюднені на VII Обласній науково-практичній конференції учнів та здобувачів вищої освіти «Сучасний стан економіки України: проблеми та перспективи розвитку» (2020 року, доповідь «Управління інформаційною безпекою торговельного підприємства»).

Структура і обсяг роботи. Випускна кваліфікаційна робота складається зі вступу, трьох основних розділів, висновків, списку використаних джерел, додатків.

В першому розділі «Теоретичні засади вивчення поняття інформаційної безпеки торговельного підприємства» викладено сутність поняття «інформаційної безпеки», досліджено ключові ризики інформаційної безпеки сучасних підприємств сфери торгівлі, вивчено вітчизняний і зарубіжний досвід використання сучасних засобів захисту інформації.

В другому розділі «Оцінка рівня інформаційної безпеки торговельного підприємства» проведено аналіз фінансового стану підприємства та

проведено ідентифікацію та оцінку інформаційних активів досліджуваного підприємства.

В третьому розділі «Удосконалення інформаційної безпеки торговельного підприємства» розкрито доцільність розробки структури VPN мережі на досліджуваному підприємстві, запропоновано впровадження стратегії спрямованості захисних заходів у ТОВ ТОРГОВИЙ ДІМ «Гранд-Трейд» та інформаційної політики, а також обґрунтовано економічну доцільність запропонованого проєкту.

Основний зміст викладено на 86 сторінок друкованого тексту. Робота містить 5 рисунків та 18 таблиць. Список використаних джерел налічує 39 найменування на 4 сторінках.

## РОЗДІЛ 1

### ТЕОРЕТИЧНІ ЗАСАДИ ВИВЧЕННЯ ПОНЯТТЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТОРГОВЕЛЬНОГО ПІДПРИЄМСТВА

#### **1.1. Основні підходи до визначення поняття інформаційної безпеки підприємства**

Сучасний етап розвитку суспільства характеризується зростаючою роллю інформаційної сфери, що представляє собою сукупність інформації, інформаційної інфраструктури, суб'єктів, які здійснюють збір, створення, надання, поширення і використання інформації, а також системи регулювання виникаючих при цьому суспільних відносин.

При цьому проблема злочинності в глобальних інформаційних мережах має два компоненти. По-перше, з'являються нові злочини, такі як порушення цілісності, доступності та конфіденційності електронних даних, об'єктом яких є нові охоронювані законом інтереси, що виникли в зв'язку з розвитком інформаційних технологій. По-друге, глобальні інформаційні мережі використовуються для здійснення діянь, вже криміналізованих в законодавстві багатьох держав, таких як розкрадання майна, порушення таємниці приватного життя тощо [9].

З ростом інформаційних технологій в Україні, як і за весь світ, з'явилася не тільки можливість для швидкого розвитку та ефективного застосування інформаційних мереж в підприємницькій діяльності, але і нові загрози. Інформаційно-комунікаційні технології впроваджуються і розвиваються набагато швидше, ніж законодавці та правоохоронні органи можуть реагувати на це зростання [5].

Згідно з даними Securelist на початку 2019 року відбулася різке збільшення кібератак:

1. 29% комп'ютерів (майже кожен третій комп'ютер в бізнес-середовищі), зазнали хоча б однієї атаки через інтернет;

2. На 58% корпоративних комп'ютерів була відображена хоча б одна атака шкідливого ПО, що на 3 пункти більше, ніж у 2018 році;

3. При атаках на бізнес експлойти до офісних додатків використовуються в три рази частіше, ніж в атаках на домашніх користувачів;

4. Файловий антивірус спрацював на 41% комп'ютерів корпоративних користувачів (виявляти об'єкти, виявлені на комп'ютерах або на знімних носіях, підключених до комп'ютерів, - флеш-картах, картах пам'яті, телефонах, зовнішніх жорстких дисках, мережевих дисках) [37].

В сучасних умовах функціонування підприємств і розвитку інформаційного суспільства все складніше здійснювати захист від недобросовісних конкурентів. Стає очевидною залежність загального рівня фінансово-економічної безпеки підприємства від її інформаційно функціональної складової. Як показує практика, будь-яка цілеспрямована дія проти інтересів господарюючого суб'єкта починається зі збору або викрадення, а в подальшому вивчення необхідної інформації, яка може бути використана для розкрадання патентів або винаходів, поглинання компанії, рейдерських захоплень, виведення активів і т.д.

Діяльність будь-якої компанії в даний час пов'язана з операційною діяльністю, управлінням фінансами та кадрами, бухгалтерським обліком, в яких суттєва роль належить інформаційних ресурсів і технологій, таким як засобу зв'язку, програми, інформаційні системи. Від безперервності і працездатності інформаційної складової залежить весь економічний і технологічний процес фірми [25].

Незважаючи на те, що застосування інформаційних технологій є однією зі складових забезпечення фінансово-економічної безпеки компанії, не варто забувати, що необхідний грамотний підхід до їх створення, організації та впровадження, так як наявність інформаційних ресурсів на підприємстві дає не тільки переваги, а й певні ризики, такі як: передумови для витоку важливої інформації, розкрадання, втрати, підробки, спотворення,

копіювання або знищення, що в свою чергу може привести до серйозних згубних наслідків для підприємства [2].

Термін «безпека інформації» описує ситуацію, яка виключає доступ для перегляду, модерації і знищення даних суб'єктами без наявності відповідних прав. Це поняття включає забезпечення захисту від витоку і крадіжки інформації за допомогою сучасних технологій та інноваційних пристроїв [12].

Захист інформації включає повний комплекс заходів по забезпеченню цілісності та конфіденційності інформації за умови її доступності для користувачів, що мають відповідні права.

Цілісність - поняття, що визначає збереження якості інформації та її властивостей.

Конфіденційність передбачає забезпечення секретності даних і доступу до певної інформації окремим користувачам.

Доступність - якість інформації, що визначає її швидке і точне знаходження конкретними користувачами.

Мета захисту інформації - мінімізація шкоди внаслідок порушення вимог цілісності, конфіденційності та доступності.

Таким чином, під захистом інформації буде розумітися комплекс правових, адміністративних, організаційних і технічних заходів, спрямованих на запобігання реальних або передбачуваних ІБ-загроз, а також на усунення наслідків інцидентів.

Безперервність процесу захисту інформації повинна гарантувати боротьбу з погрозами на всіх етапах інформаційного циклу: в процесі збору, зберігання, обробки, використання і передачі інформації.

Інформаційна безпека в цьому розумінні стає однією з характеристик працездатності системи.

У кожен момент часу система повинна володіти вимірюваним рівнем захищеності, і забезпечення безпеки системи має бути безперервним процесом, які здійснюється на всіх часових відрізках в період життя системи.

В теорії інформаційної безпеки під суб'єктами інформаційної безпеки розуміють власників і користувачів інформації, причому користувачів не тільки на постійній основі (співробітники), але і користувачів, які звертаються до баз даних в одиничних випадках, наприклад, державні органи, що запитують інформацію. У ряді випадків, наприклад, в банківських ІБ-стандартах до власників інформації зараховують акціонерів - юридичних осіб, яким належать певні дані

Підтримуюча інфраструктура, з точки зору основ інформаційної безпеки, включає комп'ютери, мережі, телекомунікаційне обладнання, приміщення, системи життєзабезпечення, персонал. При аналізі безпеки необхідно вивчити всі елементи систем, особливу увагу приділивши персоналу як носія більшості внутрішніх загроз.

Метою реалізації інформаційної безпеки підприємства є побудова системи забезпечення інформаційної безпеки даного об'єкту [4].

Для побудови та ефективної експлуатації системи забезпечення інформаційної безпеки необхідно:

1. Виявити вимоги захисту інформації, специфічні для даного об'єкта захисту;
2. Врахувати вимоги національного та міжнародного законодавства;
3. Використовувати напрацьовані практики (стандарти, методології) побудови подібних систем забезпечення інформаційної безпеки;
4. Визначити підрозділи, відповідальні за реалізацію та підтримку системи забезпечення інформаційної безпеки;
5. Розподілити між підрозділами області відповідальності в здійсненні вимог системи забезпечення інформаційної безпеки;
6. На базі управління ризиками інформаційної безпеки визначити загальні положення, технічні та організаційні вимоги, складові політики інформаційної безпеки об'єкта захисту;
7. Реалізувати вимоги політики інформаційної безпеки, впровадивши відповідні програмно-технічні засоби і способи захисту інформації;

8. Реалізувати систему менеджменту (управління) інформаційної безпеки;

9. Використовуючи систему менеджменту інформаційної безпеки організувати регулярний контроль ефективності системи менеджменту інформаційної безпеки і при необхідності перегляд і коригування [5].

Процес реалізації системи забезпечення інформаційної безпеки безперервний і циклічний, так як повертається до першого етапу, повторюючи послідовно всі інші. Так система забезпечення інформаційної безпеки коригується для ефективного виконання своїх завдань захисту інформації та відповідності новим вимогам, що постійно оновлюється інформаційної системи [19].

До завдань систем інформаційної безпеки на підприємстві можна віднести:

1. Забезпечення захищеного зберігання інформації на носіях;
2. Захист даних, що передаються по каналах зв'язку;
3. Створення резервних копій, після аварійного відновлення;
4. Забезпечення доступності інформації, що має можливість за прийнятний час отримати необхідну інформаційну послугу, а також запобігання несанкціонованим відмова в отриманні інформації;
5. Забезпечення цілісності інформації, що передбачає запобігання несанкціоновані модифікації або руйнування інформації;
6. Забезпечення конфіденційності інформації, що пов'язано із запобіганням несанкціонованого ознайомлення з інформацією.

Питання, пов'язані із забезпеченням фінансово-економічної безпеки за допомогою налагодження функціонування інформаційної безпеки підприємства, давно є одними з найбільш пріоритетних практично всіх великих компаній.

У певних ситуаціях нехтування забезпечення інформаційного захисту може привести до серйозних проблем або зовсім втрати бізнесу [8].

Такі інформаційні параметри, як конфіденційність, цілісність, доступність, достовірність і т.д. в разі погіршення, можуть привести до серйозних наслідків, таких як, втрати лідируючого місця на ринку або втрата оригінальності продукту, збоїв в системі управління технологічними процесами і іншим критичним системам [13].

Організація і функціонування системи безпеки підприємства повинні здійснюватися на основі наступних принципах:

1. Комплексність - передбачає забезпечення безпеки персоналу, матеріальних і фінансових ресурсів, інформації від всіх можливих загроз усіма доступними законними засобами і методами, протягом всього життєвого циклу і у всіх режимах функціонування, а також здатністю системи до розвитку і вдосконалення в процесі функціонування;

2. Надійність - різні зони безпеки повинні бути однаково надійними з точки зору ймовірності реалізації загрози;

3. Своєчасність - здатність системи носити упереджувальний характер на основі аналізу та прогнозування загроз безпеці і розробці ефективних заходів протидії їм;

4. Безперервність - відсутність перерв у роботі систем безпеки, викликаних ремонтом, заміною, профілактикою і т. д;

5. Законність - розробка систем безпеки на основі існуючого законодавства;

6. Розумна достатність - встановлення прийнятного рівня безпеки, при якому ймовірність і розмір можливих збитків будуть поєднуватися з гранично допустимістю функціонування системи безпеки з витратами на розробку і функціонуванням системи безпеки;

7. Централізація управління - самостійне функціонування системи безпеки за єдиними організаційним, функціональним і методологічним принципам;

8. Компетентність - система безпеки повинна створюватися і управлятися особами, які мають професійну підготовку, достатню для

коректної оцінки обставин і адекватного прийняття рішення, в тому числі в умовах підвищеного ризику [22].

При розголошенні відомостей, що становлять комерційну таємницю, порушення достовірності фінансової документації, несанкціонований доступ до персональних даних співробітників компанії, а так само при розголошенні відомостей, що мають інформацію про стан матеріальних і фінансових потоків, договірної діяльності, дані фінансового і управлінського обліку, результатами можуть стати: погіршення або припинення ділових відносин з партнерами, втрата вигідних контрактів, відмова від рішень, що стали неефективними через розкриття інформації, як наслідок нові втрати, пов'язані з розробками, зниження цін або обсягів реалізації, втрата ділової репутації підприємства та ін. [23].

Будь-який господарюючий суб'єкт має право застосовувати певні заходи щодо захисту інформації, що становлять комерційну таємницю, під якою є технологічна, науково-технічна, виробнича і фінансово-економічна або інша інформація, яка має комерційну цінність в силу не відомості третім особам.

Таким чином, сучасна корпоративна система інформаційної безпеки покликана забезпечувати захист конфіденційної інформації від несанкціонованого доступу, запобігати зловмисні або випадкові зміни (контролювати цілісність) і надавати необхідний рівень доступності [18].

Виявлення, оцінка та запобігання загрозам інформаційним системам і інформаційних ресурсів компанії, є одним з найважливіших видів діяльності щодо забезпечення інформаційної безпеки підприємства [24].

Загрози умовно можна розділити на наступні групи:

1. Програмні - впровадження «вірусів», апаратних і програмних зламів; знищення і модифікація даних в інформаційних системах;
2. Технічні, а також радіоелектронні - перехоплення інформації в лініях зв'язку; радіоелектронне придушення сигналу в лініях зв'язку і системах управління;

3. Фізичні - знищення засобів обробки і носіїв інформації;

4. Режимні - порушення регламентів інформаційного обміну; незаконні збір і використання інформації; несанкціонований доступ до інформаційних ресурсів; незаконне копіювання даних в інформаційних системах; розкрадання носіїв, а також апаратних або програмних пральних ключів; дезінформація, приховування або перекручення інформації система розкрадання інформації з баз даних [14].

При побудові ефективної системи захисту інформації, питання аналізу загроз і ризиків є вирішальними. За оцінками фахівців лише 11% компаній використовують власно розроблені методи для виявлення ризиків і загроз, які дозволяють виконувати не тільки кількісний аналіз, але й оптимізацію підсистем інформаційної безпеки [2].

Найбільш частими загрозами інформаційній безпеці являються вірусні епідемії, хакерські атаки і спам. Крім того, не варто забувати, що існують внутрішні загрози, які виходять від співробітників компанії, наприклад, недбалість, крадіжка інформаційних ресурсів, шахрайство, а також використанням корпоративних інформаційних систем і так далі. Результати досліджень показують, що більшість компаній не вживає достатніх заходів щодо захисту від дій інсайдерів. Наприклад, тільки 1% опитаних Infowatch компаній впроваджує засоби захисту від витоків інформації. Ці дані підтверджуються і компанією КРОК на основі проведення аудиту систем інформаційної безпеки. Крім того, згідно зі статистичними даними, близько 80% зловмисників проти підприємства є його співробітники [1].

У більшості випадків, керівництво підприємств не усвідомлюють взаємозв'язок між фінансовими втратами і незахищеністю інформаційних систем господарюючого суб'єкта. Відділ з питань фінансово-економічної безпеки повинен виявляти і запобігати всі можливі загрози в інформаційній сфері з боку зловмисників, а також створювати і впроваджувати ефективні засоби захисту комерційної інформації [10].

Щодо основної ідеї ефективної системи забезпечення інформаційної безпеки підприємства представляється виправдана позиція, сформульована Я. Волковим: будучи частиною процесів управління організацією і спираючись на технічну інфраструктуру, дана система повинна максимально скорочувати величину ризиків, пов'язаних з інформаційними технологіями, мінімізувати витрати на це і мати великий запас гнучкості для самостійної адаптації до мінливих умов [15].

При створенні систем захисту необхідно враховувати наступне:

1. Для повноцінного захисту інформаційних ресурсів і систем потрібна реалізація комплексу заходів (юридичних, технологічних, організаційно-економічних);
2. Залучення вузькопрофільних фахівців для більш точної розробки способів і методів щодо захисту інформації. Їх системний підхід до реалізації механізму захисту [4].

Існує чотири напрямки функції служби інформаційної безпеки:

1. Розробка методології і методики аналізу загроз, становить оцінки рівня інформаційної безпеки підприємства і корпоративних стандартів системи її забезпечення;
2. Організація і здійснення конкретних видів діяльності по захисту інформації;
3. Експлуатація технічних засобів захисту інформації;
4. Аудит і контроль функціонування системи інформаційної безпеки підприємства.

Застосування деяких функцій має здійснюватися спільно один з одним. До основних засобів забезпечення інформаційної безпеки підприємства відносяться:

1. Засоби захисту від несанкціонованого доступу;
2. Системи аналізу та моделювання інформаційних потоків (CASE-системи);
3. Системи моніторингу мереж;

4. Аналізатори протоколів;
5. Антивірусні засоби;
6. Між мережеві екрани;
7. Криптографічні засоби (шифрування і цифровий підпис);
8. Системи резервного копіювання;
9. Системи безперебійного живлення (джерела безперебійного живлення, резервування навантаження, генератори напруги);
10. Системи аутентифікації, пароль, ключ доступу (фізичний або електронний), сертифікат, біометрія;
11. Засоби запобігання злому корпусів і крадіжки обладнання.
12. Засоби контролю доступу в приміщення;
13. Інструментальні засоби аналізу систем захисту (антивірус) [5].

В сучасних умовах інформаційна безпека є невід'ємною складовою системи фінансово-економічної безпеки господарюючого суб'єкта. У свою чергу, надійне забезпечення фінансово-економічної безпеки є неодмінною умовою переходу на модель сталого розвитку не тільки окремого підприємства, а й національної економіки в цілому [13].

## **1.2. Ключові ризики інформаційної безпеки сучасних підприємств сфери торгівлі**

Сучасні підприємства стикаються з самими серйозними ризиками для інформаційної безпеки.

Ці ризики мають як внутрішні, так і зовнішні джерела. Інформаційної безпеки підприємств загрожують:

- проникаючі ззовні хакери і шкідливі програми
- власні зловмисні співробітники - інсайдери
- власні співробітники - незловмисні порушники
- стихійні лиха (пожежі, повені, аварії в енергосистемах тощо).

Головні цілі атак на інформаційні системи підприємств:

- отримання контролю над цінними ресурсами, наприклад, крадіжка фінансової інформації або експлуатація обчислювальних ресурсів корпоративної мережі

- обмеження діяльності підприємства на замовлення недобросовісних конкурентів або політичних опонентів, наприклад, шляхом виведення з ладу інформаційної системи, руйнування зв'язків з партнерами тощо [4].

Ризики для інформаційної безпеки можуть бути реалізовані в самому різному вигляді: шкідливих програм, апаратних і програмних закладок, спам-розсилок, пристроїв для перехоплення сигналів зв'язку, регламентів, що допускають несанкціонований доступ інсайдерів та ін.

Різні методи для нанесення шкоди інформаційної безпеки стають все більш таргетованими (націленими на конкретну галузь і навіть підприємство). Так, в 2010 році була виявлена спеціалізована шкідлива програма, атакуюча автоматизовані системи оперативного диспетчерського управління виробництвом, - комп'ютерний черв'як Stuxnet. Існують цілі класи шкідливих програм, специфічних для окремих галузей економіки, наприклад, троянці-Банкер.

Успішна комп'ютерна атака на підприємство може вести до самих неприємних наслідків - фінансових збитків, зниження репутації і переслідуванню регуляторних органів.

Найбільш поширені види загроз:

1. Несприятлива для підприємства економічна політика держави. Регулювання економіки державою за допомогою маніпуляцій (визначення валютного курсу, облікова ставка, митні тарифи і податки) є причиною багатьох протиріч на підприємствах в сфері виробництва, фінансів і комерції.

Велику небезпеку для забезпечення безпеки інформації підприємства несуть адміністративні зобов'язання виходу на ринок, що призводить до насильницького звуження товарно-грошових відносин, порушення законів з боку держави і обмеження діяльності підприємства. Часто держава перебільшує свою компетентність у фінансовій і комерційній сфері

діяльності підприємства і необґрунтовано втручається в простір інформації цих сфер, а також зазіхає на власність підприємства в різних формах.

Серйозну загрозу для забезпечення безпеки інформації підприємства несуть політичні дії, спрямовані на обмеження або припинення економічних зв'язків. Санкції в економіці викликають у обох сторін недовіру до подальшої діяльності і підривають комерційні взаємини. Все це веде до дестабілізації економічних відносин, і не тільки на рівні держави.

2. Дії інших господарюючих суб'єктів. В даному випадку ризик забезпечення безпеки інформації несе нездорова конкуренція. Нездорова або недобросовісна конкуренція має кілька понять і за нормами міжнародного права поділяється на три види:

- Коли діяльність однієї комерційної структури намагаються представити споживачеві під виглядом іншого;
- дискредитування репутації комерційного підприємства шляхом поширення неправдивої інформації;
- Неправомірне і некоректне використання торгових позначень, що вводять споживача в оману.

У західних країнах існують законодавчі акти щодо ведення недобросовісної конкуренції, фірмових найменувань, товарних позначень і перешкоджання забезпеченню безпеки інформації, порушення яких веде до певної юридичної відповідальності. Також до відповідальності наводять такі неправомірні дії:

- Підкуп або переманювання споживачів з боку конкурента;
- Порядок забезпечення інформаційної безпеки організації порушується шляхом розголошення комерційних таємниць, а також з'ясування інформації за допомогою шпигунства, підкупу;
- Навмисне зниження цін для придушення конкуренції;
- Копіювання товарів, реклами, послуг і інших форм комерційної діяльності та інформації конкурента.

Наступною формою недобросовісної конкуренції, спрямованої на перешкоджання забезпеченню безпеки інформації, вважається фізичне придушення у вигляді посягання на життя і здоров'я службовця компанії. У цю категорію входить:

- Організація розбійних нападів на виробничі, складські приміщення і офіси з метою пограбування;
- Знищення, псування майна і матеріальних цінностей шляхом вибуху, підпалу або руйнування;
- Захоплення співробітників в заручники або фізичне усунення.

3. Кризові явища в світовій економіці. Кризи мають особливість перетікати з однієї країни в іншу, використовуючи канали зовнішніх економічних зв'язків. Вони також завдають шкоди забезпеченню безпеки інформації. Це слід врахувати, визначаючи методи і засоби забезпечення інформаційної безпеки організації.

Поетапне інтегрування України в міжнародну економіку сприяє залежності комерційних підприємств країни від різних процесів, що відбуваються в світовій економіці (падіння і зростання цін на енергоносії, структурна перебудова і інші фактори).

За ступенем впровадження національної економіки в світову економічну структуру посилюється її схильність до зовнішніх факторів. Тому, сучасне виробництво в прагненні до збільшення прибутку, поліпшення діяльності шляхом модернізації, підвищення рівня забезпечення безпеки інформації, стабільності обов'язково має звертати увагу на динаміку споживчого попиту, політику держави і центральних банків, розвиток науково-технічного прогресу, на ставлення конкурентів, світову політику і господарську діяльність.

Таким чином, комп'ютеризація економіки і поширення електронних фінансових транзакцій призводять до зростання загроз інформаційній безпеці підприємств. Для забезпечення прийнятного рівня інформаційної безпеки, питань захисту необхідно приділяти достатню увагу. Корпоративні

комп'ютерні системи - це складні інформаційні структури, і тому для виконання проектів щодо забезпечення їх безпеки у багатьох випадках залучаються сторонні спеціалізовані компанії.

### **1.3. Вітчизняний і зарубіжний досвід використання сучасних засобів захисту інформації**

Сучасний вітчизняний ринок засобів захисту інформації від несанкціонованого доступу представлений різними комплексами і системами, які за своїм виконанням можна розділити на програмні і програмно-апаратні, а по сфері застосування - на кошти для захисту персональних даних і конфіденційної інформації (класи захищеності 1Г, 1Д, 2Б, 3Б) і засоби для захисту державної таємниці та конфіденційної інформації високого рівня (класи захищеності 1А, 1Б, 1В, 2А, 3А) [28].

В даний час вітчизняні розробники пропонують ряд програмних засобів, сертифікованих відповідним чином, в яких прикладні програми та основні функції захисту довірені звичним елементам, що знаходяться на материнській платі ПЕОМ, а також зовнішньому носію інформації, на якому зберігається програма захисту інформації від несанкціонованого доступу.

До програмних засобів захисту можна віднести:

1. Страж NT 4.0. Продукт компанії ПрАТ НВЦ «Модуль», володіє ліцензіями і сертифікатами.

Система захисту інформації від несанкціонованого доступу Страж NT (версія 4.0) являє собою програмний комплекс засобів захисту інформації з використанням апаратних ідентифікаторів.

Засіб захисту Страж NT (версія 4.0) призначене для комплексного захисту інформаційних ресурсів від несанкціонованого доступу. Страж NT (версія 4.0) може застосовуватися при розробці систем захисту інформації для одно- і багатокористувацьких автоматизованих систем та інформаційних систем обробки персональних даних відповідно до вимог законодавства.

2. Dallasrrvese Lock 8.0. Продукт компанії ЦЗІ ТОВ «Конфідент», володіє ліцензіями.

Dallas Lock 8.0 - сертифікована система захисту інформації накладного типу для автономних і мережевих АРМ (застосовна для складних мережевих інфраструктур).

Призначена для захисту конфіденційної інформації, в тому числі міститься в автоматизованих системах до класу захищеності 1Г включно, в державних інформаційних системах до 1 класу захищеності включно, в інформаційних системах персональних даних для забезпечення 1 рівня захищеності персональних даних, в автоматизованих системах управління виробничими і технологічними процесами до 1 класу захищеності включно, а також для захисту інформації, що містить відомості, які є державною таємницею, рівня «цілком таємно» включно [37].

Відмінність програмно-апаратних засобів від виключно програмних полягає в тому, що захисні функції реалізуються технічними засобами, що знаходяться повністю на окремій платі. Цей варіант максимально розділяє технічні засоби обробки, що підлягають захисту даних і технічних засобів, що реалізують функції захисту інформації від несанкціонованого доступу.

При цьому програма захисту інформації від несанкціонованого доступу зберігається в пам'яті мікропроцесора, технологія запису програми в довготривалу пам'ять виключає її вірусне зараження, оперативна пам'ять і пам'ять програм розділені.

До програмно-апаратних засобів захисту від несанкціонованого доступу можна віднести:

#### 1. Акорд-АМДЗ. Продукт виготовлений ТОВ «ОКБ САПР».

Являє собою апаратний модуль довіреної завантаження для IBM-сумісних ПК - серверів і робочих станцій локальної мережі, що забезпечує захист пристроїв і інформаційних ресурсів від несанкціонованого доступу.

«Довірена завантаження» - це завантаження різних операційних систем тільки з заздалегідь визначених постійних носіїв (наприклад, тільки з

жорсткого диска) після успішного завершення спеціальних процедур: перевірки цілісності технічних і програмних засобів ПК (з використанням механізму покрокового контролю цілісності) і ідентифікації / аутентифікації користувача [38].

2. Secret Net 7 + Secret Net Card. Продукт виробництва ТОВ «КодБезпеки».

Можливості Secret Net:

- Аутентифікація користувачів;
- Розмежування доступу користувачів до інформації та ресурсів автоматизованої системи;
- Довірена інформаційне середовище;
- Контроль витоків і каналів поширення конфіденційної інформації;
- Контроль пристроїв комп'ютера і відчужуваних носіїв інформації на основі централізованих політик, що виключають виток конфіденційної інформації;
- Затирання залишкової інформації при звільненні та видаленні областей пам'яті комп'ютера і запам'ятовуючих пристроїв;
- Централізоване управління системою захисту, оперативний моніторинг і аудит безпеки;
- Масштабована, система захисту, можливість використання Secret Net (мережевий варіант) в організації з великою кількістю філій;
- Захист термінальної інфраструктури і підтримка технологій віртуалізації робочих столів (VDI) [38].

3. Соболь 3.0.9. Продукт компанії ТОВ «1 Безпеки».

Програмно-апаратний комплекс «Соболь» - засіб захисту комп'ютера від несанкціонованого доступу, що забезпечує довірену завантаження. «Соболь» може застосовуватися для захисту автономного комп'ютера, а також робочої станції або сервера, що входять в склад локальної обчислювальної мережі.

Програмно-апаратний комплекс "Соболь" версія 3.0.9. Наявність даних сертифікатів дозволяє використовувати «Соболь» для захисту інформації, що становить комерційну або державну таємницю в автоматизованих системах з класом захищеності до 1Б включно. Основними можливостями є:

- Ідентифікація і аутентифікація. Використовуються персональні електронні ідентифікатори. Загрузка операційної системи з жорсткого диска здійснюється тільки після пред'явлення зареєстрованого ідентифікатора;
- Реєстрація спроб доступу до комп'ютера. Електронний замок «Соболь» здійснює ведення системного журналу, записи якого зберігаються в спеціальній енерго-незалежній пам'яті: факт входу користувача і ім'я користувача; пред'явлення незареєстрованого ідентифікатора; введення неправильного пароля; перевищення числа спроб входу в систему; дата і час реєстрації подій несанкціонованого доступу;
- Сторожовий таймер. Механізм сторожового таймера забезпечує блокування доступу до комп'ютера за умови, що після включення комп'ютера і через встановлений період часу управління не передано розширенню BIOS комплексу «Соболь»;
- Датчик випадкових чисел. Електронний замок «Соболь» містить датчик випадкових чисел, який відповідає вимогам служби безпеки;
- Контроль цілісності програмного середовища.

При виборі найбільш оптимального засобу захисту інформації від несанкціонованого доступу слід звернути увагу на: виконання вимог чинного законодавства; сумісність з оперативною системою комп'ютера, який буде атестований; слабкий вплив на комп'ютер в процесі роботи; стабільність програмного забезпечення; відсутність додаткових засобів, ускладнюючих експлуатацію; оптимальна вартість [17].

США використовують платформу Dynamic Threat Protection компанії ISS, яка забезпечує швидку і надійну багаторівневий захист мереж, серверів і робочих станцій від Інтернет-загроз. При цьому за рахунок використання системи централізованого управління і кореляції RealSecureSiteProtector (tm)

досягається максимальна простота управління засобами захисту. Платформа Dynamic Threat Protection включає в себе наступні компоненти:

1. Internet Scanner 7.0, будучи ключовим компонентом платформи Dynamic Threat Protection, взаємодіє з іншими системами безпеки для того, щоб точно визначити вразливі вузли і вчасно попередити атаки.

Основні можливості Internet Scanner 7.0:

- Механізм необмеженої інвентаризації - він дозволяє користувачеві сканувати всю його мережу, а не тільки ту кількість вузлів, на яке ви придбали ліцензію, потім класифікувати сервери, робочі станції, маршрутизатори і точки бездротового доступу за ступенем захищеності та виділити найбільш важливі пристрої, що вимагають постійного контролю їх захищеності, відповідно до числа, зазначеним в ліцензії;

- Покращена точність - точніша ідентифікація операційної системи за допомогою механізму опитування стека TCP / IP віддаленого вузла, використовуюваного в сканері NMAP;

- Розподілене виявлення вразливостей - за допомогою системи Site Protector можна розміщувати в мережі велику кількість сканерів уразливості і ефективно управляти ними;

- Віртуальні латки - можна, визначивши критичні уразливості, оновити політики безпеки і автоматично застосовувати ці оновлення до уразливих систем;

2. Система Real Secure Server 7.0 є частиною платформи Dynamic Threat Protection. Вона захищає сервера, запобігаючи виявлену на них шкідливу і неавторизовану активність. дія системи засноване на контролі поведінки Real Secure Server 7.0 активно блокує переповнення буфера, передачу "неправильних" пакетів, доступ до кореневих тек і інші способи атак, часто використовувані зловмисниками [29].

Основні можливості Real Secure Server 7.0:

- Запобігання вторгнень - застосування різних методів інтелектуального аналізу більш ніж 95 мережевих протоколів і баз відомих

атак, що нараховує понад 1700 унікальних сигнатур, забезпечує максимально точне виявлення атаки;

- Блокування, заснована на аналізі поведінки, - дозволяє зупинити переповнення буфера, передачу "неправильних" пакетів, доступ до кореневих тек і інші види атак;

- Кореляція подій і аналіз атак - можливість миттєво порівнювати зразки атак і реальні атаки, знаходити відповідність між ними . Інтеграція Real Secure Server 7.0 з іншими засобами захисту дозволяє виявляти зв'язок між атаками на вузли і мережевими атаками;

- Зниження ймовірності помилкового виявлення атаки і не виявлення реальної атаки, можливість виявити підозрілу поведінку до того, як атака встигне завдати шкоди;

- Підтримка великої кількості платформ - Windows 2000 і HP-UX, Windows 2003 AIX, Linux and Solaris. 3. Система Real Secure Desktop 7.0 - компонент платформи Dynamі Threat Protection. Вона в режимі реального часу забезпечує захист від атак за рахунок аналізу поведінки додатоківі мереж (включаючи VPN) на робочих станціях і мобільних комп'ютерах.

3. Система Real Secure Desktop 7.0 також запобігає атаки і забезпечує координацію реагування на них. 7.0;

Основні можливості Real Secure Desktop 7.0:

- Запобігання вторгнень - як і в системі Real Secure Server - Блокування вихідного та вхідного трафіку - дозволяє закривати вхідний трафік в мережу і вихід з неї трафіку для певних портів, мережесих протоколів і діапазонів IP-адрес;

- Інтеграція з VPN - це означає можливість перевірити відповідність роботи клієнта корпоративній політиці перш, ніж дати йому доступ до мережі через VPN;

- Узгодженість з антивірусним ПЗ - заборона віддаленим користувачам доступу в мережу через VPN в разі, якщо антивірусне програмне

забезпечення не запущено або без оновлення, а також своєчасне оповіщення таких користувачів через централізовану систему управління;

- Удосконалена захист додатків - запобігає запуск троянських програм, дозволяючи використання тільки авторизованих програм (певних адміністратором або локальним користувачем і перевірених на контрольну суму MD5), і дає адміністратору можливість конфігурувати рівень прав локальних користувачів.

Таким чином, слід зауважити, що вітчизняний і зарубіжний досвід використання сучасних засобів захисту інформації досить різноманітний. Вітчизняні програми для захисту інформації адаптовані під українське законодавство, а так само схвалені службами безпеки України. У свою чергу, інші зарубіжні сучасні засоби захисту інформації від несанкціонованого доступу підходять лише для використання на зарубіжних підприємствах.

## РОЗДІЛ 2

### ОЦІНКА РІВНЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТОРГОВЕЛЬНОГО ПІДПРИЄМСТВА

#### 2.1. Загальна характеристика підприємства ТОВ ТОРГОВИЙ ДІМ "Гранд-трейд"

Товариство з обмеженою відповідальністю ТОВ ТОРГОВИЙ ДІМ "Гранд-трейд", яке здійснює оптовий продаж широкого спектру товарів відповідно до документів, які регламентують діяльність досліджуваного підприємства (Додаток А).

Відповідно до Статуту підприємства основна мета організації, як комерційного підприємства, полягає в отриманні прибутку від діяльності і продовжувати протягом максимально тривалого терміну залишатися на ринку, при цьому розширюючи свій асортимент і ринки збуту (Додаток Б).

Видами діяльності Товариства є:

- організація оптової та роздрібної торгівлі;
- торгово-закупівельна та торгово-посередницька діяльність, в тому числі на зовнішньому ринку, а також на внутрішньому ринку;
- інвестиційна діяльність;
- діяльність на ринку цінних паперів;
- надання маркетингових, консалтингових, посередницьких та інших платних послуг та практичної допомоги підприємствам, фірмам, фізичним особам;
- транспортне обслуговування, в тому числі доставка вантажів різними видами транспорту і перевезення туристів, а також міжнародні перевезення;
- рекламна діяльність;
- здійснення операція з експорту та імпорту товарів, виробничо-технічних знань і послуг;
- роботи і послуги, пов'язані з розвитком наукових, ділових, спортивних і культурних зв'язків, в тому числі з зарубіжними організаціями

та громадянами, консалтингових, орендних, лізингових, інжинірингових, правових, посередницьких (в тому числі з зарубіжними партнерами), транспортних, сервісних, соціально-побутових;

- підготовка до продажу, купівлі та продаж власного нерухомого майна;

- покупка і продаж власних нежитлових будівель та приміщень;

- дослідження кон'юнктури ринку;

- роздрібна торгівля алкоголем та іншими напоями;

- роздрібна торгівля тютюновими виробами;

- оптова та роздрібна торгівля алкогольної, слабоалкогольної та безалкогольної продукцією та тютюновими виробами;

- будівництво та ремонт будівель і споруд;

- організація і виробництво будівельних і будівельно-монтажних робіт, проектування;

- випуск і реалізація будівельно-монтажної продукції;

- виробництво товарів легкої промисловості;

- виробництво, переробка, зберігання і реалізація нафтопродуктів;

- виробництво та реалізація металів і сплавів з них;

- виробництво товарів народного споживання;

- виробництво, переробка і реалізація сільськогосподарської продукції;

- торгово-закупівельні, маркетингові, рекламно-сервісні, посередницькі та консультаційні послуги, надання представницьких послуг, в тому числі закордонним фірмам на території країни;

- придбання і комплектування технічними засобами;

- розробка і виробництво зразків нової техніки, приладів та інструментів;

- здійснення товарообмінних операцій і посередницької діяльності;

- консалтингова діяльність;

- здійснення всіх видів транспортно-експедиційних та складських послуг;

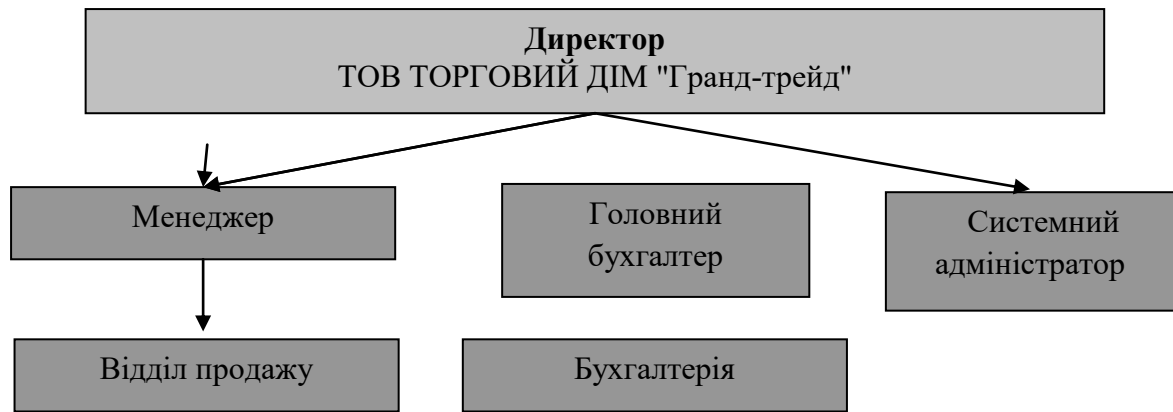
- здійснення маркетингової діяльності та реклама продукції підприємств, що входять в суспільство;
- проведення маркетингових досліджень;
- створення власних філій, дослідно-експериментальних, виробничих, торгово-збутових баз, комерційних центрів і відповідних підрозділів, що забезпечують їх роботу;
- надання послуг громадянам та організаціям у придбанні та збуті товарів і технологій;
- надання комерційних, інформаційних, посередницьких та інших видів послуг замовникам у здійсненні їх ринкової діяльності як на території України, так і за кордоном;
- розвиток і впровадження інформаційних проектів, технологій, засобів обчислювальної техніки і програмних засобів, інжиніринг, лізинг, маркетинг в різних сферах господарської та громадської діяльності (на основі розвитку власних виробництв і залучення партнерів на конкурсній основі);
- діяльність у сфері права;
- інші види діяльності, не заборонені чинним законодавством України.

ТОВ ТОРГОВИЙ ДІМ "Гранд-трейд" співпрацює з великою кількістю різних постачальників (Додаток В). Замовлення товарів здійснюються по телефону.

Оплату товару постачальникам здійснюють за допомогою безготівкових розрахунків платіжними дорученнями.

Ключовим елементом організаційного механізму Товариства виступає структура управління.

Далі розглянемо організаційну структуру ТОВ ТОРГОВИЙ ДІМ "Гранд-трейд" (рис. 2.1).



**Рис. 2.1. Організаційна структура ТОВ ТОРГОВИЙ ДІМ "Гранд-трейд"**

Джерело: сформовано автором

Як спостерігаємо, на рис. 2.1 ТОВ ТОРГОВИЙ ДІМ "Гранд-трейд" має лінійно-функціональну структуру управління.

До переваг такої структури управління слід віднести: однозначність впливу суб'єкта на об'єкт управління; відсутність проміжних зв'язків між керівником і підлеглим; можливість отримання несуперечливих, пов'язаних між собою завдань; висока відповідальність керівника за результати роботи.

Загалом, персонал підприємства включає в себе:

- директора, який проводить безпосереднє управління процесами фірми, проводить безготівкові розрахунки з постачальниками і покупцями, здійснює аналізи більш ранніх продажів і здійснює прийом заявок від менеджерів на замовлення товару, на основі аналізів та заявки здійснює замовлення необхідних товарів у постачальника, знаходить можливість для збільшення асортименту ;
- менеджера, який передає директору заявку на замовлення товару у постачальника;
- продавців. Вони здійснюють реалізацію в роздріб в торгових залах. Після продажу товару вони роблять позначку в базі даних про кількість реалізованих одиниць товару, несуть відповідальність за зберігання;

- системного адміністратора, який проводить настройку і установку устаткування, займається усуненням неполадок програмного забезпечення (ПО) і комп'ютерного обладнання. Здійснює спостереження за працездатністю ЕОМ і периферійних пристроїв. Так само на нього покладаються обов'язки адміністратора з інформаційної безпеки (ІБ);
- бухгалтерію.

Бухгалтера ТОВ ТОРГОВИЙ ДІМ "Гранд-трейд" здійснюють суцільне, безперервне, взаємопов'язане, документальне відображення господарського функціонування підприємства.

Функції даного відділу організації накладені на відповідних посадових осіб (бухгалтерів), які здійснюють облік, необхідний для характеристик окремої сторони діяльності фірми.

Зазначена посадова особа несе відповідальність за правильне і своєчасне оформлення господарської операції, а також забезпечують збереження і облік грошових коштів, які циркулюють в процесі здійснення господарської діяльності.

З бухгалтерами укладені договори про повну матеріальну відповідальність відповідно до чинного законодавства України.

## **2.2. Аналіз основних показників торгового підприємства та результатів його діяльності**

Далі, вважаємо за доцільне, здійснити оцінку фінансового стану підприємства.

Аналіз основних фінансово-економічних показників ТОВ ТОРГОВИЙ ДІМ «Гранд-Трейд» наведені в табл. 2.1.

На основі даних таблиці 2.1 можна зробити наступні висновки: чистий дохід від реалізації продукції, робіт, послуг досліджуваного підприємства має тенденцію до збільшення.

Таблиця 2.1

**Основні показники фінансово-господарської діяльності ТОВ ТОРГОВИЙ  
ДІМ «Гранд-Трейд» за період 2015-2019 рр.**

| Показники                                               | Значення показника за рік, тис. грн. |         |         |       |       | Відхилення (+,-) 2019р. до: |         |       |
|---------------------------------------------------------|--------------------------------------|---------|---------|-------|-------|-----------------------------|---------|-------|
|                                                         | 2015                                 | 2016    | 2017    | 2018  | 2019  | 2016                        | 2017    | 2018  |
| 1. Чистий дохід від реалізації продукції, робіт, послуг | 13207,8                              | 20631,2 | 25993,1 | 45117 | 61744 | 41112,8                     | 35750,9 | 16627 |
| 2. Собівартість реалізованої продукції                  | 12923,0                              | 20255,7 | 25212,1 | 42749 | 57495 | 37239,3                     | 32282,9 | 14746 |
| 3. Валовий прибуток                                     | 284,8                                | 375,5   | 781,0   | 2368  | 4249  | 3873,5                      | 3468    | 1881  |
| 4. Чистий прибуток підприємства                         | 0,0                                  | 10,0    | 120,4   | 215,0 | 107,0 | 97                          | -13,4   | -108  |
| 5. Основні засоби (залишкова вартість)                  | 6218,3                               | 6217,7  | 7679,9  | 10588 | 12872 | 6654,3                      | 5192,1  | 2284  |
| 6. Середньорічна вартість осн. засобів                  | 6365,5                               | 6218,0  | 6948,8  | 13073 | 17837 | 11619                       | 10888,2 | 4764  |
| 7. Статутний капітал                                    | 1570,5                               | 1570,5  | 1570,5  | 2600  | 2600  | 1029,5                      | 1029,5  | 0     |
| 8. Дебіторська заборгованість                           | 749,5                                | 932,3   | 1499,5  | 1153  | 3754  | 2821,7                      | 2254,5  | 2601  |
| 9. Середня кількість працівників                        | 71                                   | 71      | 79      | 129   | 129   | 58                          | 50      | 0     |
| 10. Фондоозброєність (р.6/р.10)                         | 89,65                                | 87,58   | 87,96   | 101,3 | 138,3 | 50,72                       | 50,34   | 37    |
| 11. Фондовіддача основних фондів(р.1/р.5)               | 2,12                                 | 3,32    | 3,38    | 4,3   | 4,8   | 1,48                        | 1,42    | 0,5   |

Джерело: розраховано автором на основі даних Додатку Г

Різке збільшення всіх показників у 2018-2019 роках порівняно з попередніми роками пов'язано із зміною структури підприємства (до його складу увійшли ще 2 підприємства). У 2019 році чистий дохід складав 61744,0 тис. грн., що на 16627,0 тис. грн. більше, ніж у попередньому, 2018 р. тобто на 35% більше.

Собівартість реалізованої продукції також має чітку тенденцію зростання до 2019 року включно. У 2019 році собівартість склала 57495 тис. грн., що на 36% більше порівняно з 2018 р. і є наслідком росту обсягів виконаних робіт. Ріст собівартості відбувався, насамперед, через зростання матеріальних затрат, адміністративних та інших операційних витрат. Збільшення чистого доходу від реалізації продукції вплинуло на збільшення

валових фінансових результатів, у 2019 році підприємство отримало валовий прибуток у розмірі 4249,0 тис. грн., що на 1881,0 тис. грн. більше ніж у 2018 році.

Відзначається різка тенденція зростання дебіторської заборгованості у 2019 році в порівнянні з 2015 роком, що негативно впливає на платоспроможність підприємства (рис. 2.2).

Фінансово-економічний аналіз результатів ТОВ ТОРГОВИЙ ДІМ «Гранд-Трейд» свідчить про те, що собівартість реалізованої продукції має чітку тенденцію до зростання.



**Рис. 2.2. Динаміка дебіторської заборгованості ТОВ ТОРГОВИЙ ДІМ «Гранд-Трейд» (тис.грн)**

Джерело: розраховано автором на основі даних Додатку Г

Чистий дохід від реалізації продукції, який визначається шляхом віднімання з валового доходу (виручки) від реалізації продукції (товарів, робіт, послуг) відповідних податків, збільшився. Збільшення чистого доходу від реалізації продукції вплинуло на збільшення валових фінансових результатів.

Загалом економічні показники ТОВ ТОРГОВИЙ ДІМ «Гранд-Трейд» за аналізований період свідчать про задовільне функціонування та прибуткову діяльність підприємства.

Суттєво зросли нематеріальні активи досліджуваного підприємства

(право власності на результати інтелектуальної діяльності, право користування майном та майновими правами платника податку).

Динаміка вартості основних засобів ТОВ ТОРГОВИЙ ДІМ «Гранд-Трейд» за період 2015-2019 рр. показує, що відбулося збільшення вартості основних засобів підприємства (рис. 2.3.) на 6654 тис. грн. у 2019 р. порівняно з 2015 р. Це відбулося за рахунок капіталовкладень (придбання устаткування і приєднання до структури підприємства додатково двох підприємств).

Слід відмітити, що сума зносу основних засобів лише за аналізований період 2015-2019 рр. збільшилася на 43,1%, що досить-таки суттєво.

У структурі активів протягом 2015-2019 років найбільшу питому вагу займають необоротні активи, в середньому 75%, що є нормальною ситуацією – допустимим співвідношенням між оборотними та необоротними активами для підприємства, яке роздрібною торгівлею, оскільки у власності підприємства знаходиться широка мережа складських приміщень та автопарку для забезпечення логістичних перевезень товару.



**Рис. 2.3. Динаміка вартості основних засобів ТОВ ТОРГОВИЙ ДІМ «Гранд-Трейд» за період 2015-2019 рр. (тис. грн)**

Джерело: розраховано автором на основі даних Додатку Г

Власний капітал підприємства суттєво зменшився протягом аналізованого періоду і у 2019 році склав 8001,0 тис. грн., що на 26,8%

менше показника 2016 року. При цьому його питома вага також значно зменшилась із 56,6% у 2016 році до 36,2% у 2018 році, що свідчить про підвищення залежності підприємства від зовнішніх джерел фінансування. У підтвердження цього факту свідчить динаміка обсягів довгострокових забезпечень та поточних зобов'язань, розмір яких підприємство у 2018 році збільшило в порівнянні з 2016 роком на 5756,6 тис. грн., або у 1,7 рази.

Значна питома вага поточних зобов'язань говорить про те, що підприємство не є залежним від довгострокових кредитів і надає перевагу короткостроковим позикам, що негативно впливає на рівень ліквідності активів.

До того ж сучасний рівень розвитку економіки не стимулює банківські установи видавати довгострокові кредити.

Зростання показника довгострокових забезпечень у 2018 році до значення 2986,0 тис.грн. пов'язане з переходом до міжнародних стандартів фінансової звітності (МСФЗ) з 01.01.2018 р.

Далі, здійснюємо аналіз стану інформаційних активів ТОВ ТОРГОВИЙ ДІМ «Гранд-Трейд».

### **2.3. Ідентифікація та оцінка інформаційних активів досліджуваного підприємства**

Одним із етапів аналізу ризиків є ідентифікація всіх об'єктів, які потребують захисту зловмисників. Необхідно брати до уваги всі фактори, що може бути порушено при порушенні режимів безпеки.

ТОВ ТОРГОВИЙ ДІМ «Гранд-Трейд» є організацією, яка не виробляє свій товар, а набуває його у великих, брендових фірм, які знаходяться на ринку довгий час, і їх продукція вже за багато років асоціюється у покупців з надійністю і якістю. Придбання товару можна описати наступним логічним ланцюжком:

1. аналізується потреби ринку;

2. здійснюється закупівля товару в потрібній кількості, як правило, за оптовими цінами;
3. товар надходить на склад;
4. зі складу товар направляється контрагентам або відразу в руки покупцеві.

Звідси можна зробити висновки, що одним з основних активів в організації, куди вкладаються гроші, є товар, в покупці і перепродажі якого ТОВ ТОРГОВИЙ ДІМ «Гранд-Трейд» отримує прибуток.

Інший половиною вкладення грошових коштів є створення і забезпечення безпеки документообігу на підприємстві. Володіння цінною інформацією і її вміле, практичне застосування багато в чому обумовлює успішність сучасної людини, що відноситься і до діяльності на ринку продажів. На сучасному підприємстві в обороті знаходиться величезна кількість інформації, що зачіпає всю організаційну структуру, починаючи від директора і закінчуючи продавцями, і ретельно взаємодіє між собою. Взаємодія відбувається шляхом об'єднання всієї організаційної структури в локальну обчислювальну мережу.

Комерційною таємницею називають такий режим конфіденційності інформації, який дозволяє її власникам при наявних або можливих обставинах збільшувати дохід, уникати невиправданих витрат, зберігати присутність на ринках товарів, робіт, послуг або витягувати інші комерційні переваги.

Організація правильного конфіденційного діловодства в організаціях становить основну частину комплексного забезпечення безпеки даних і набуло більшої значущості при досягненні цілей їх захисту.

Як відомо фахівцям, в області інформаційної безпеки, що близько 80% конфіденційних даних знаходиться в документах, які відносяться до діловодства. Тому питання конфіденційного документообігу в організаціях, очевидно, грає одну з головних ролей при досягненні ними комерційних успіхів.

Попадання конфіденційної інформації в руки зловмисників і конкурентів може призводити до різних негативних наслідків для фірми, таким як шкоди матеріальним активам, діяльності та престижу фірми, втрати стратегічно важливих замовників.

Інформація про оцінку активів ТОВ ТОРГОВИЙ ДІМ «Гранд-Трейд» представимо в табл. 2.2 (Додаток Д).

На даний момент налічують понад 30 різних видів конфіденційної інформації. Це при цілому розгляді не може створювати сприятливу атмосферу в сенсах забезпечення їх інформаційної безпеки.

Користувачі інформаційних засобів організації повинні підписувати відповідні зобов'язання по відношенню до конфіденційності (угода про нерозголошення).

Службовцями зазвичай підписуються такі зобов'язання як частина основних умов приймання на роботу.

Договір про дотримання конфіденційності інформації повинен переглядатися при зміні умов прийому на роботу або контрактних умов, особливо в тому випадку, коли службовець збирається звільнитися або при закінченні терміну дії контракту.

ІТ-ресурси ТОВ ТОРГОВИЙ ДІМ «Гранд-Трейд» діляться на три групи:

1. Інформацію, яка є комерційною таємницею;
2. конфіденційну інформацію;
3. сувору конфіденційну інформацію.

Відомості, які відносяться до цих груп, наведемо в табл. 2.3.

Після оцінки інформаційних активів підприємства, необхідно провести їх ранжування, щоб в подальшому виявити актуальні і неактуальні загрози, і в залежності від рангу, проводити побудова технічних заходів для забезпечення захисту.

Таблиця 2.3

**Перелік відомостей конфіденційного характеру  
ТОВ ТОРГОВИЙ ДІМ «Гранд-Трейд»**

| <b>Найменування відомостей</b>                                                                                                        | <b>Гриф конфіденційності</b> |
|---------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| Відомості про структуру виробництва, виробничих потужностях, тип і розміщення устаткування, запасах комплектуючих і готової продукції | суворо конфіденційно         |
| Відомості про плани інвестицій, закупівель, продажів                                                                                  | комерційна таємниця          |
| Відомості про стан банківських рахунків підприємства і вироблених операціях                                                           | суворо конфіденційно         |
| Відомості про стан програмного та комп'ютерного забезпечення                                                                          | конфіденційно                |
| Відомості про особливості використовуваних і розроблюваних технологій і специфіку їх застосування                                     | конфіденційно                |

Джерело: сформовано автором

Результати ранжування активів ТОВ ТОРГОВИЙ ДІМ «Гранд-Трейд» представимо в табл. 2.4.

Таблиця 2.4

**Результати ранжирування активів  
ТОВ ТОРГОВИЙ ДІМ «Гранд-Трейд»**

| <b>Найменування активу</b>                                   | <b>Цінність активу (ранг)</b> |
|--------------------------------------------------------------|-------------------------------|
| Відомості ділового характеру                                 | 4                             |
| Інформаційний актив з торговельно-економічних питань         | 4                             |
| Інформаційний актив про надані послуги                       | 5                             |
| Інформаційний актив з питань забезпечення безпеки            | 5                             |
| Інформаційний актив з організаційно-управлінської діяльності | 2                             |
| Товар організації                                            | 3                             |
| Устаткування                                                 | 3                             |

Джерело: сформовано автором

Активи, які мають найбільшу цінність:

1. Інформаційні активи про наданих послугах;
2. Інформаційні активи з питань забезпечення безпеки;
3. Відомості ділового характеру;

4. Інформаційні активи з торгово-економічних питань;
5. Товари торговельного підприємства;
6. Обладнання;
7. Інформаційний актив з організаційно-управлінської діяльності.

Вищим керівництвом організації ТОВ ТОРГОВИЙ ДІМ “Гранд-трейд”, в особі директора, було вироблено чітке положення про інформаційну політики безпеки для всіх підрозділів організації. Політика безпеки є результатом спільної діяльності технічного персоналу, покладеного на системного адміністратора, здатного зрозуміти всі аспекти політики і її реалізації, а також директора, здатного впливати на проведення політики в житті.

В одному з пунктів даного положення йдеться, що для забезпечення підтримки інформаційної безпеки на високому рівні, один раз на рік буде проводитися перевірка внутрішнім аудитом, яка побудована на повній відповідності правових і законодавчих документах про аудиторську діяльність в Україні. В ході перевірки буде застосовуватися детальний аналіз ризику, який включає в себе оцінку вразливості активів.

Вразливістю інформації називається можливість виникнення таких станів, при яких з'являються умови для реалізації загрози безпеці даними. Сама по собі наявність уразливості не завдає шкоди, так як для цього необхідним є наявність відповідних загроз. Наявність вразливостей за відсутності таких загроз не вимагає використання захисних заходів, але уразливості повинні бути зафіксовані і в подальшому перевірені на випадки змін ситуації.

Такі види оцінок припускають ідентифікацію уразливості в навколишньому середовищі, організаціях, процедурах, персоналі, менеджменті, адміністрації, апаратних засобах, програмному забезпеченні або апаратурі зв'язку, які можуть бути використані джерелами загроз для нанесення шкоди активу і діловому функціонуванню організації, які здійснюються з їх застосуванням. Варто відзначити, що некоректно

застосовуються, а також неправильно працюють захисні заходи можуть самі по собі бути джерелом появи уразливості. Поняття «уразливості» може бути віднесено до властивостей або атрибутів активів, які використовуються іншою чином або для іншої мети, ніж та, для якої купувалися або виготовлялися дані активи. Початкові дані для оцінки вразливостей повинні виходити від власника або користувача активів, фахівця з обслуговуючим пристроїв, експерта по програмних і апаратних засобів систем інформаційних технологій.

Результат оцінювання вразливості активів ТОВ ТОРГОВИЙ ДІМ «Гранд-Трейд» представлено в табл. 2.5 (Додаток Ж).

Користувач інформаційних послуг зобов'язаний чітко фіксувати і повідомляти про всі помічені або передбачуваних вразливих місцях засобів захисту по відношенню до систем або послуг, а так само повідомити про це безпосереднім керівникам, і як можна швидше. Користувач повинен знати, що ні при якому обставині він не повинен вживати самостійних спроб перевіряти слабе місце, що викликає підозру. Це потрібно з метою його ж захисту, оскільки його дія по перевірці слабого місця може бути інтерпретовано як потенціальне зловживання.

В ході перевірок будуть надані висновки в письмовій формі, з переліком всіх знайдених та оцінених вразливостей, для визначення сумарних оцінок ризиків, які має на увазі надалі вибір комплексу заходів щодо захисту даних.

Оцінка загроз активів є наступним кроком услід за оцінкою вразливості цих же активів в детальному аналізі ризику. Загрози будуть виявлені в ході внутрішнього аудиту, який затверджений в письмовому положенні про інформаційну безпеку в особі вищого керівної ланки організації ТОВ ТОРГОВИЙ ДІМ «Гранд-Трейд» - директора, і покладені обов'язки з проведення внутрішнього аудиту на системного адміністратора.

Загрози (потенційні можливості несприятливих впливів) мають здатність нанесення шкоди системам інформаційних технологій і їх активів. Якщо ці загрози

реалізуються, вони можуть взаємодіяти з системами і викликати небажані інциденти, які нададуть несприятливий вплив на систему.

В основі загрози можуть лежати як природні, так і людські фактори; вони можуть бути реалізовані випадковим або навмисним чином.

Джерела як випадкової, так і навмисної загрози повинні ідентифікуватися, а ймовірності їх реалізації - оцінені.

Важливо не випускати з уваги жодної з можливих загроз, так як в результаті можливе порушення функціонування або поява уразливості систем забезпечення безпеки. Вихідні дані для оцінки загрози необхідно отримати від власника або користувача активу, службовців відділу кадрів, фахівця з розробки обладнання та інформаційних технологій, а також особи, яка відповідає за реалізацію захисних заходів в організації.

Класифікація можливості реалізації загрози (атаки), являє собою сукупності можливих варіантів дії джерел загрози певними методами реалізації з застосуванням вразливостей, які приведуть до реалізації мети атак.

Мета атак може і не співпасти з цілями реалізації загрози і може направлятися на отримання проміжних результатів, необхідних для досягнення в майбутньому реалізації загроз. У разі таких розбіжностей атаку розглядають як «підготовку до вчинення» протиправних дій.

Результатами атак є наслідки, які стануть реалізацією загроз або сприятимуть таким реалізаціям.

Існує досить велика кількість різнопланових загроз безпеки інформації різного генезису. Застосовується багато різноманітних видів класифікацій, де в якості критерію розподілу застосовують види породжується небезпеки, ступінь злого умислу, джерела появи загрози тощо.

Далі опишемо найбільш просту систему класифікації загроз:

1. Природна загроза. Викликана впливом на елемент об'єктивними фізичними процесом або стихійним, природним явищем, незалежних від людини;
2. Штучна загроза. Викликана діяльністю людей. Серед штучних загроз, виходячи з мотивацій дії, можуть бути виділені:

2.1. ненавмисна (ненавмисна, випадкова) загроза, викликана помилкою в проектуванні захищається елемента, помилкою в програмному забезпеченні, помилкою в дії персоналу тощо;

2.2. навмисна (умисна) загроза, пов'язана з корисливим мотивом людини (злоумишленнікам).

В ході перевірки буде надано висновок у письмовій формі, з переліком всіх знайдених та оцінених загроз, для визначення сумарної оцінки ризику, який має на увазі надалі вибір комплекс заходів щодо захисту інформації.

Результат оцінки загрози активам ТОВ ТОРГОВИЙ ДІМ «Гранд-Трейд» представимо в табл. 2.6 (Додаток 3).

Так як ТОВ ТОРГОВИЙ ДІМ «Гранд-Трейд» є невеликим комерційним підприємством, як за штатом співробітників, так і по займаному обсягу продажів на ринку, положення про інформаційну безпеку було сформовано всередині організації, вищому керуючим особою - директором.

У цьому письмовому положенні завдання по забезпеченню інформаційної безпеки покладаються на посаду системного адміністратора.

Перевірка має на увазі проведення внутрішнього аудиту, після закінчення якого видається висновок в письмовій формі і передається директору, за яким стоїть остаточне рішення щодо впровадження або вдосконалення, того чи іншого модуля.

Інформаційна система, що розглядається нами організації, представляє собою сукупність робочих станцій і серверів, об'єднаних в єдину локальну мережу. Дані зберігаються і обробляються як на робочих станціях, так і на файловому сервері.

Локальну обчислювальну мережу створюють з урахуванням єдиних концептуальних положень, які лежать в основі побудови сучасних обчислювальних мереж зв'язку організації.

Основою такого положення, в першу чергу, є застосування загальних принципів побудови і однорідного активного мережного обладнання.

В мережевій структурі компанії є кілька досить виражених рівнів ієрархії. ЛВС створюється на базі стандарту Ethernet 10/100 Base-T. Даний стандарт підходить для використання з різними операційними системами і мережевим обладнанням.

Використання цього стандарту дає можливість простим методом добиватися стабільного функціонування мережі.

Для побудови мереж слід вибирати кабелю, від якості і характеристик яких багато в чому залежить якість роботи мереж.

У нашому випадку використовуємо неекрановану виту пару категорії 5. Конфігурацію мережі представимо в табл. 2.7.

Таблиця 2.7

**Конфігурація мережі підприємства  
ТОВ ТОРГОВИЙ ДІМ «Гранд-Трейд»**

| <b>Компоненти/характеристики</b>            | <b>Реалізація мережі</b>                                                                                                                                                |
|---------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Типологія                                   | зірка                                                                                                                                                                   |
| Лінія зв'язку                               | Неекрановані кручені пари категорії 5                                                                                                                                   |
| Мережеві адаптери                           | Ethernet 10/100 Base-T                                                                                                                                                  |
| Комунікаційне обладнання                    | Комутатори Ethernet 10/100 Base-T                                                                                                                                       |
| Спільне використання периферійних пристроїв | Підключення мережевого принтера і БФП через комп'ютер до мережевого кабелю. Управління чергою до принтера здійснюють за допомогою програмного забезпечення комп'ютерів. |
| Підтримувані додатки                        | Організація колективної роботи в середовищі електронного документообігу, робота з базами даних.                                                                         |
| Мережеві адаптери                           | Ethernet 10/100 Base-T                                                                                                                                                  |

Джерело: сформовано автором на основі даних підприємства

При виборі компонентів мережі слід виконувати наступні загальні вимоги:

- комп'ютери мережі повинні мати гарну швидкодію, щоб забезпечувати роботу всіх служб і додатків в реальному часі мережі без помітних затримок в роботі;

- жорсткий диск комп'ютера повинен бути максимально надійним для того, щоб забезпечувати безпеку і цілісність інформації, що зберігається інформації;
- мережевий принтер повинні встановлюватися в залежності від місця розташування користувача, який активно його використовує;
- комутатори, які є центральними пристроями даної мережі, повинні бути розташовані в легкодоступних місцях, щоб можна було без проблем підключити кабель і стежити за індикаціями.

Перераховані вище вимоги визначають таку конфігурацію мережевої структури: комп'ютери в мережі мають базу процесорів Intel Core 2 Duo, як мережевих принтерів вибираємо багатофункціональний пристрій (лазерний), так як вони мають найбільші ресурси та малі витрати на расходний матеріал.

Конфігурацію робочих станцій наведемо в табл. 2.8.

Таблиця 2.8

### Конфігурація робочої станції підприємства ТОВ ТОРГОВИЙ ДІМ «Гранд-Трейд»

| Найменування                                                                                    | Кількість, шт. |
|-------------------------------------------------------------------------------------------------|----------------|
| Мат. плати Asus P5q-Vm (Intel G45); Lga775 <G41> PCI-E; Lan; Svs Sata Matx 2xDDR-II <Pc3-10600> | 12             |
| Процесор Core 2 Duo E7500, 2.93 GHz                                                             | 12             |
| Оперативна пам'ять Kingston DIMM 1Gb DDRII-533                                                  | 12             |
| Жорсткі диски Seagate Barracuda 7200.9 ST3120814A 120,0Gb (U-ATA, 7200 rpm)                     | 12             |
| Корпуси InWin S523T (MidiTower, ATX, USB, 350Вт, Чорний)                                        | 12             |
| Монітори NEC (LCD) AccuSync 73V (17", 1280x1024, 500: 1)                                        | 12             |
| Миші Genius NetScroll Eye Mouse (оптика, PS / 2)                                                | 12             |
| Клавіатури Logitech Value Keyboard (PS / 2)                                                     | 12             |

Джерело: сформовано автором на основі даних підприємства

Конфігурація мережевого обладнання приведена в табл. 9.

Таблиця 2.9

**Конфігурація мережевого обладнання підприємства  
ТОВ ТОРГОВИЙ ДІМ «Гранд-Трейд»**

| Найменування товару                      | Кількість, шт. |
|------------------------------------------|----------------|
| Комутатори CISCO 3825 (UTP, 16 x 10/100) | 1 шт.          |
| Кабелю UTP (Alcatel, категорії 5)        | 300 м.         |
| Коннектори RJ-45 (категорії 5)           | 30 шт.         |

Джерело: сформовано автором на основі даних підприємства

Конфігурацію периферійного обладнання наведемо в табл. 2.10.

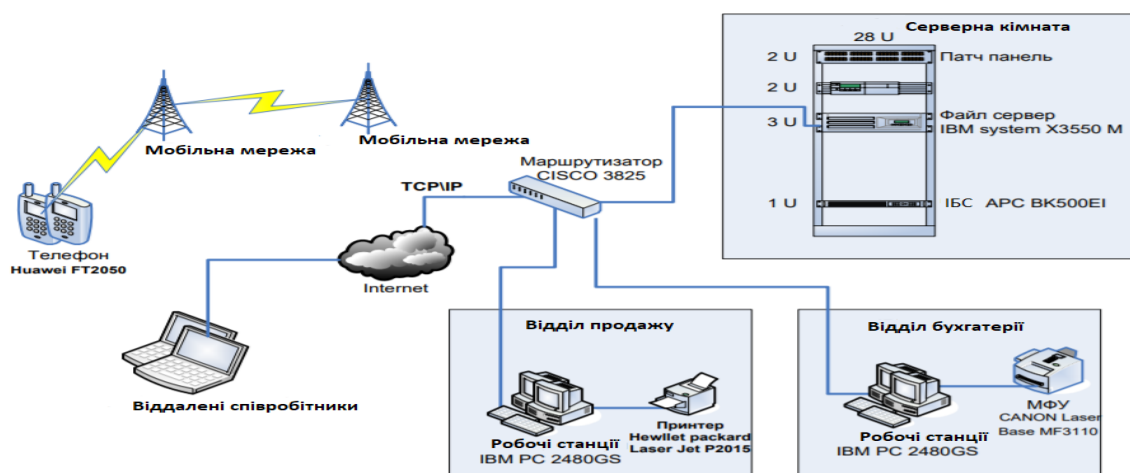
Таблиця 2.10

**Конфігурація периферійних пристроїв підприємства  
ТОВ ТОРГОВИЙ ДІМ «Гранд-Трейд»**

| Найменування                                                                 | Кількість, шт. |
|------------------------------------------------------------------------------|----------------|
| Принтери Hewlett Packard LaserJet P2015 (A4, 1200dpi, 26 ppm, 32Mb, USB 2.0) | 1              |
| МФУ Canon LaserBase MF3110 (A4; 1200x600 dpi; 250 лист., 64mb)               | 1              |
| Стационарний багатофункціональний телефон Huawei FT2050                      | 3              |

Джерело: сформовано автором на основі даних підприємства

Технічну архітектуру представимо на рис. 2.4.



**Рис. 2.4. Технічна архітектура ТОВ ТОРГОВИЙ ДІМ «Гранд-Трейд»**

Джерело: сформовано автором на основі даних підприємства

Конфігурацію програмного забезпечення наведемо в табл. 2.11.

Таблиця 2.11

**Конфігурація програмних засобів підприємства  
ТОВ ТОРГОВИЙ ДІМ «Гранд-Трейд»**

| <b>Найменування</b>                                        | <b>Кількість, шт.</b> |
|------------------------------------------------------------|-----------------------|
| Windows Server 2003 Std Russian R2                         | 1                     |
| Windows XP Professional Russian SP2                        | 12                    |
| Office 2007 Standart Edition Russian SP2                   | 3                     |
| 1С: Бухгалтерія 7.7                                        | 1                     |
| Ліцензія на 5 дод. робочих місць для «1С: Бухгалтерія 7.7» | 1                     |
| Ліцензія на сервер для «1С: Бухгалтерія 7.7»               | 1                     |
| ВО «Облік і продаж»                                        | 5                     |
| Ліцензійний ключ Kaspersky Internet Security               | 1                     |

Джерело: сформовано автором на основі даних підприємства

По периметру всієї території, де знаходиться головне приміщення ТОВ ТОРГОВИЙ ДІМ «Гранд-Трейд», яке включає в себе: торговий зал, склад, офіс директора, бухгалтерію, ІТ відділ, серверну, розташовані 7 камер відеоспостереження фірми Germikom (модель D-250). Завдяки постійному відеоспостереження фізичне розкрадання матеріального об'єкта стає майже неможливим. Так само при розробці загальних заходів політики безпеки на підприємстві було прийнято рішення про впровадження антивірусного ПО продукції Касперського на всі робочі станції і сервери.

Аналіз виконання основних завдань щодо забезпечення інформаційної безпеки ТОВ ТОРГОВИЙ ДІМ «Гранд-Трейд» представимо в табл. 2.12.

Значить, з використанням програмних і апаратних засобів в ТОВ ТОРГОВИЙ ДІМ «Гранд-Трейд» повинні вирішуватися наступні завдання:

1. Створення загальнодоступних баз даних;
2. Спільна робота над інформацією користувачами фірми;
3. Проведення централізованого резервного копіювання всієї інформації;
4. Здійснення контролю над доступом до даних;
5. Спільне застосування апаратних засобів і програмного забезпечення.

У затвердженому положенні, директором ТОВ ТОРГОВИЙ ДІМ «Гранд-Трейд» про інформаційну безпеку, встановлено, що в ході перевірки внутрішнім аудитом, покладеним на посаду системного адміністратора, на заключному етапі буде представлено висновок у письмовій формі про сумарною оцінкою ризику, із застосуванням детального аналізу ризику, для подальшого вибору комплексу заходів щодо захисту інформації.

Таблиця 2.12

**Виконання основних завдань ІБ ТОВ ТОРГОВИЙ ДІМ  
«Гранд-Трейд»**

| <b>Завдання щодо забезпечення інформаційної безпеки даних</b>                                                                                                                                         | <b>Ступінь виконання</b>                                                                  |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| забезпечити безпеку торговельної діяльності, захист інформації та відомостей, що є комерційною таємницею                                                                                              | Чи не в повних обсягах, наявність захисту тільки від фізичного доступу                    |
| організувати роботу з правової, організаційної та інженерно-технічної (фізичної, апаратної, програмної і математичної) захисту комерційних таємниць                                                   | Чи не в повних обсягах, виконана стандартними вбудованими засобами апаратури і програми   |
| організувати спеціальне діловодство, яке виключає несанкціоноване отримання даних, що є комерційною таємницею                                                                                         | У повних обсягах                                                                          |
| запобігти необґрунтованому допуску і відкритому доступу до відомостей і робіт, що становлять комерційну таємницю                                                                                      | Чи не в повних обсягах, наявність захисту тільки від фізичного доступу                    |
| виявити і локалізувати можливі канали витоку конфіденційних даних в процесах повсякденному виробничої діяльності та в екстремальних (аварії, пожежі та ін) ситуаціях                                  | Чи не в повних обсягах, виконується стандартними вбудованими засобами апаратури і програм |
| забезпечити режим безпеки при здійсненні таких видів роботи, як різні зустрічі, переговори, наради, засідання та інші заходи, які пов'язані з діловою співпрацею на національних і міжнародних рівнях | У повних обсягах                                                                          |
| забезпечити охорону територій, будівель приміщень, з захищеними даними                                                                                                                                | У повних обсягах                                                                          |

Джерело: сформовано автором на основі даних підприємства

Раніше всі дані про активи організації були зібрані з власників цих активів, оцінені, виявлені вразливості і загрози.

На заключних етапах аналізу ризиків проводять сумарну оцінку.

Оцінки ризиків є оцінки співвідношення потенційних негативних факторів на ділову діяльність у випадках небажаного інциденту і рівнів оціненої загрози і вразливих місць. Ризики фактично є заходами незахищеності систем і пов'язаними з ними організаціями. Величини ризиків залежать від наступних факторів: цінність активу; загрози і пов'язана з ними ймовірність виникнення небезпечних для активу подій; легкість реалізації загрози в уразливому місці з наданням небажаних впливів; існуючого або планованого засоби захисту, що знижує ступінь вразливостей, загрози і небажаного впливу.

Варто зазначити, що вибір методики оцінки ризику, лежить повністю на розсуд особи, яка проводить цей аналіз, в нашому випадку це посаду системного адміністратора. Головним визначальним фактором вибору є те, що б для самої організації обраний спосіб був зручний і вселяв довіру.

В даному випадку був обраний метод використовує матрицю у вигляді таблиці із заздалегідь визначеними значеннями.

Суть таких підходів полягає у визначенні найбільш критичного активу в організаціях з точки зору ризиків ІБ по «штрафному балу».

Оцінювання ризику виробляють експертним шляхом на основі аналізів цінності активу, можливостей реалізації загрози і використання уразливості, визначеної в попередньому пункті. Для оцінювання використовуються таблиці, із заздалегідь визначеними «штрафними балами» для кожної комбінації цінності активу, рівня загрози та вразливості. В кінці, після оцінювання активу усіма виявленими уразливими і погрозами, штрафні бали підсумовуються. Кінцева сума і буде підсумковою мірою ризику, в залежності від якої буде проводитися ранжування ризиків в організації.

Сама оцінка відбувається наступним чином: ідентифікують відповідні ряди матриць по цінності активів, а відповідну колонку - за ступенем загроз і вразливостей. Наприклад, якщо цінність активів дорівнює «4», загроза характеризується як «висока», а уразливість - як «низька», міра ризику дорівнює 5.

Якщо існує вразливе місце без відповідних загроз або загроза без відповідних вразливих місць, то вважають, що в даний час ризики відсутні.

Показник ризику в застосовуваній таблиці вимірюється в шкалах від 0 до 8 з такими визначеннями рівня ризиків:

1 - ризики практично відсутні; теоретично можлива ситуація, при якій подія настане, але на практиці це відбувається рідко, а потенційний збиток порівняно невеликий;

2 - ризики дуже малі; подія подібного роду трапляється досить нечасто, крім того, негативні наслідки невеликі;

8 - ризики дуже великі; події швидше за все наступлять, і наслідки будуть дуже важкими тощо.

Використовувана для оцінки шкала представлена в рис. 2.5.

|                  | РІВНІ ЗАГРОЗ      | НИЗЬКИЙ |   |   | СЕРЕДНІЙ |   |   | ВИСОКИЙ |   |   |
|------------------|-------------------|---------|---|---|----------|---|---|---------|---|---|
|                  | РІВНІ ВРАЗЛИВОСТІ | Н       | С | В | Н        | С | В | Н       | С | В |
| ЦІННІСТЬ АКТИВІВ | 1                 | 0       | 1 | 2 | 1        | 2 | 3 | 2       | 3 | 4 |
|                  | 2                 | 1       | 2 | 3 | 2        | 3 | 4 | 3       | 4 | 5 |
|                  | 3                 | 2       | 3 | 4 | 3        | 4 | 5 | 4       | 5 | 6 |
|                  | 4                 | 3       | 4 | 5 | 4        | 5 | 6 | 5       | 6 | 7 |
|                  | 5                 | 4       | 5 | 6 | 5        | 6 | 7 | 6       | 7 | 8 |

**Рис. 2.5. Оцінка ризиків ТОВ ТОРГОВИЙ ДІМ «Гранд-Трейд»**

Джерело: сформовано автором на основі даних підприємства

Результат проведення оцінок ризиків ТОВ ТОРГОВИЙ ДІМ «Гранд-Трейд» представимо в табл. 2.13.

Таблиця 2.13

**Результати оцінки ризиків ТОВ ТОРГОВИЙ ДІМ  
«Гранд-Трейд»**

| <b>Ризик</b><br>(в штрафні бали) | <b>Актив</b>                                                 | <b>Ранг ризику</b> |
|----------------------------------|--------------------------------------------------------------|--------------------|
| 61                               | Інформаційний актив про надані послуги                       | 1                  |
| 60                               | Інформаційний актив з питань забезпечення безпеки            | 2                  |
| 47                               | Відомості ділового характеру                                 | 3                  |
| 46                               | Інформаційний актив з торговельно-економічних питань         | 4                  |
| 27                               | Устаткування                                                 | 5                  |
| 22                               | Інформаційний актив з організаційно-управлінської діяльності | 6                  |
| 6                                | Товар організації                                            | 7                  |

Джерело: сформовано автором на основі даних підприємства

Виходячи з аналізу ризиків в ТОВ ТОРГОВИЙ ДІМ «Гранд-Трейд» існують такі види загроз безпеки інформації, як загрози порушення конфіденційності даних.

Саме цьому аспекту буде приділено увагу у наступному розділі.

## РОЗДІЛ 3

### УДОСКОНАЛЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТОРГОВЕЛЬНОГО ПІДПРИЄМСТВА

#### 3.1. Доцільність розробки структури VPN мережі на досліджуваному підприємстві

Виходячи з результатів аналізу нами було встановлено наявність загрози порушення конфіденційності даних, тому саме для вирішення цієї проблеми буде розроблятися система захисту.

Конфіденційністю називається характеристика інформації, яка полягає в тому, що інформацію можна отримати повчитися неавторизованого користувачеві, тобто користувачеві, який не володіє привілеями на отримання даної інформації.

Зберігання та перегляд цінної інформації допустимо тільки для тих людей, які за своїми службовими обов'язками і повноваженнями призначається для цього.

Конфіденційність призивається для забезпечення захисту інформації, що передається від пасивної атаки, тобто захисту потоків даних від можливостей його аналітичних досліджень. Це забезпечує неможливість для порушників виявляти як джерела інформації, так і їх вміст.

Основний спосіб забезпечення конфіденційності полягає в шифруванні інформації з використанням ключів користувача. При цьому дізнатися зміст інформації може тільки власник ключа, на якому зашифровані дані.

Забезпечення цієї характеристики є, звичайно, однією з важливих задач, тому що при порушенні цілісності і доступності даних в результаті псування або крадіжки вона може бути відновлена з архіву, а при порушенні конфіденційності інформація стає загальнодоступною, що може привести до величезних збитків.

Загрози порушення цілісності даних.

Цілісністю називають характеристику інформації, яка полягає в тому, що інформацію не може модифікувати неавторизований користувач. Підтримка цілісності цінних і секретних даних означає, що вони захищені від неправомірних модифікацій. Є безліч видів інформації, які мають цінність тільки в тому випадку, коли можна гарантувати, що ця інформація правильна.

Основні завдання заходів щодо забезпечення цілісності інформації полягають в можливості виявлення фактів модифікації, факту, що дана інформація не була пошкоджена, зруйнована або змінена іншим іншим способом.

Спотворенням інформації обумовлюється повний контроль над інформаційними потоками між усіма об'єктами системи або можливості передачі повідомлень від імені інших користувачів.

Для реалізації цілісності інформації використовують різні види цифрових підписів, або односпрямовану функцію хешування.

Загрози порушення доступності.

Доступність називають властивості ресурсів системи, які полягають в тому, що користувачі і/або процеси, що володіють відповідними повноваженнями, можуть використовувати ресурси відповідно до правил, які встановлені політиками безпеки, без очікування часу, більшого заданого проміжку часу.

Тобто забезпечення того, щоб інформація та інформаційна система були доступні і готові до застосування завжди, як тільки вони потрібні.

У цьому випадку повинні існувати гарантії, що дані завжди будуть доступні і підтримуються в придатному для використання стані.

Загрози порушення спостережливості даних.

Спостере називають властивості інформаційних систем, які роблять можливими фіксування діяльності користувача і процесу, застосування пасивного об'єкта, а так само однозначне встановлення ідентифікаторів причетних до конкретної події користувача і процесу з метою порушення

політик безпеки або приховування фактів відповідальності за певну подію, яка мала місце.

Загрози порушення автентичності інформації.

Автентичність інформації повинна бути забезпечена за допомогою процедур аутентифікації. Аутентифікація називають процедури перевірки відповідності пред'явлених ідентифікаторів об'єктів на предмет належності їх цим об'єктам.

Загроза порушення автентичності полягає в тому, що в результаті проведення деякого дії користувачі і(або) процеси видають себе за інших користувачів і мають можливості скористатися чужими правами і привілеями.

Для кожної з наведених вище загроз ставляться у відповідність відповідні послуги, що надаються захищених систем, тобто, послуги конфіденційності, цілісності, доступності, спостережливості і автентичності. Системи при цьому вважаються захищеними або безпечними, якщо забезпечуються всі перераховані вище послуги.

Відштовхуючись від аналізу ризиків проведених раніше, а так само маючи на увазі актуальні загрози і вразливості, місцем, де будуть розроблятися комплексні організаційні та інженерно-технічні заходи щодо забезпечення інформаційної безпеки, стане локальна обчислювальна мережа компанії ТОВ ТОРГОВИЙ ДІМ «Гранд-Трейд».

Одна з основних завдань для нормального функціонування локальної обчислювальної мережі та можливостей з її допомогою успішного проведення бізнес-процесів є безпека інформаційних потоків, які циркулюють в ній.

На даний момент існуючі засоби інформаційної безпеки в організації обмежуються вбудованими засобами використовуваного ПО, наприклад захисними механізмами операційної системи, що в даний час не забезпечить надійного захисту.

Для локальної обчислювальної мережі будуть обрані такі засоби забезпечення захисту, що шанс виникнення загроз, вразливостей і ризиків будуть зведений до мінімуму, тобто мережу, яка в компанії існує на даний момент, стане захищеною.

Вся обов'язок по виконанню покладено на посаду системного адміністратора, які відповідають за діяльність адміністратора з інформаційної безпеки.

### **3.2. Впровадження стратегії спрямованості захисних заходів у ТОВ ТОРГОВИЙ ДІМ «Гранд-Трейд» та інформаційної політики**

Організація повинна визначитися, який із трьох стратегій спрямованості захисту інформації, а саме оборонної, наступальної, упереджуючої слідувати.

Під стратегією розуміється загальна спрямованість в організації відповідної діяльності, що розробляється з урахуванням об'єктивних потреб в даному виді діяльності, потенційно можливих умов її здійснення і можливостей організації.

Проаналізувавши характеристики всіх трьох стратегій і зміст етапів побудови засобів захисту інформації, в ТОВ ТОРГОВИЙ ДІМ «Гранд-Трейд» вибір був зроблений на користь наступальної стратегії захисту інформації.

На вибір вплинули наступні характеристики:

- Забезпечуваний рівень захисту;

Може бути дуже високим, але тільки в межах існуючих уявлень про природу загроз інформації та можливості їх прояву.

- Умови, необхідні для реалізації;

1. Наявність переліку та характеристик повного безлічі потенційно можливих загроз інформації;

2. Можливість використовувати різні методи і засоби захисту;

3. Наявність можливостей впливу на архітектуру локальної вимірювальної мережі технологію обробки інформації.

- ресурсомісткість;

Значна, причому з підвищенням вимог до захисту зростає по експоненті.

- Рекомендації по застосуванню;

При порушенні захищеності інформації, виникає загроза значних фінансових та інших втрат.

На вибір вплинуло такий зміст етапів побудови засобів захисту:

Формування середовища захисту;

1. структурована архітектура локальної вимірювальної мережі;
2. структурована технологія обробки інформації, що захищається, чітка організація обробки інформації, що захищається інформації.

Аналіз засобів захисту;

1. Подання організаційно структурної побудови локальної вимірювальної мережі у вигляді упорядкованого графа: вузли - типові структурні компоненти, дуги - взаємозв'язку між компонентами;

2. Подання технології обробки інформації, що захищається в вигляді суворо визначеній схеми;

3. Визначення параметрів, що захищається і умов її обробки.

Оцінки уразливості інформації;

1. Визначення значень ймовірностей порушення захищається в тих умовах, в яких вона буде оброблятися;

2. Оцінки розмірів можливого збитку при порушеннях захищеності інформації.

Визначення вимог до захисту;

Визначення ймовірності надійного захисту інформації, яка повинна бути забезпечена при обробці інформації, що захищається інформації.

Побудова системи захисту;

Вибір типового варіанту або проектування індивідуальної системи захисту.

Організація функціонування систем захисту;

Розробка технології функціонування системи захисту.

Вимоги до середовища захисту визначається в залежності від вимог до захисту інформації.

Організаційні заходи відіграють істотну роль при реалізації надійних механізмів захисту даних, тому що можливість несанкціонованого використання конфіденційних відомостей в значній мірі обумовлені як технічним аспектом, так і злочинними діями або недбалістю користувача.

Організаційні заходи захисту засновані на законодавчих і нормативних документах щодо забезпечення безпеки даних. Вони повинні охопити всі основні способи збереження ресурсів. Слід провести такі заходи:

- обмежити фізичний доступ до об'єктів ІС ;
- обмежити можливість для перехоплення даних внаслідок наявності фізичних полів;
- обмежити доступ до інформаційного ресурсу і інших елементів ІС, встановивши правила розмежування доступів, а також криптографічне закриття каналу передачі даних;
- створити тверді копії важливого з точки зору втрати масиву інформації;
- провести профілактичні та інші заходи від впровадження вірусів.

До необхідних організаційно-правових заходів захисту, необхідними для організації в ТОВ ТОРГОВИЙ ДІМ “Гранд-трейд” віднесемо:

- організувати і підтримувати надійний пропускний режим і контроль відвідувачів фірми;
- організувати надійну охорону приміщень компанії і території;
- організувати захист інформації, тобто призначити відповідального за захист інформації, здійснити систематичний контроль над роботою персоналу, порядком обліку, зберігання і знищення документів.

Організаційні заходи по роботі з персоналом торговельного підприємства передбачають:

- провести бесіди при прийомі;
- ознайомити з правилами і процедурами роботи з інформаційними системами в організації;
- навчити правилам роботи з інформаційними системами для забезпечення схоронності її цілісності і коректності;

Навчання співробітників передбачається не тільки для придбання та систематичного підтримання на високому рівні виробничих навичок, а й для психологічного виховання необхідності виконання вимог промислової або виробничої секретності, інформаційної безпеки.

Систематичне навчання сприятиме збільшенню рівнів компетентності адміністрації та співробітників в вопросах захисту комерційних інтересів підприємства.

Для забезпечення адміністративного рівня в організації були прийняті наступні види документів:

1. Керівництво для користувача;
2. Документація на програмні і апаратні засоби, яка включає в себе короткий посібник для користувача з описом основних функцій.

3. Керівництво по комплексним засобам захисту; Даний документ адресований системному адміністратору відповідального за захист та повинен містити: опис контрольованих функцій; посібник з впровадження засобів захисту; опису старту програмних і апаратних коштів, процедур перевірки правильності старту, процедур роботи із засобами реєстрації.

4. Загальна політика безпеки;

У документі описані цілі, область застосування, сама політика, прийнята в організації ТОВ ТОРГОВИЙ ДІМ "Гранд-трейд".

Тестова документація.

У цьому документі представлено опис тестів і випробувань, яких зазнали кошти обчислювальної техніки і результатів тестування.

Побудова системи захисту інформації з точки зору способу реалізації, буде проводитися шляхом модернізації існуючої системи. На підприємствах робота по інженерно-технічному захисту інформації включає в себе 2 етапи: модернізація (в нашому випадку) системи захисту та підтримку захисту на необхідному рівні.

Так само модернізація системи захисту інформації та підтримання її на необхідному рівні передбачає проведення наступних основних робіт:

- уточнення переліку захищаються джерел інформації і носіїв інформації, виявлення і оцінка загроз безпеці інформації;
- визначення заходів щодо захисту інформації, викликаних зміною цілей і завдань захисту, загроз безпеки інформації;
- контроль ефективності заходів щодо інженерно-технічного захисту інформації в організації.

Перед вибором конкретних програмно-технічних засобів, проведемо аналіз основних технологій, які застосовуються в сучасний час для забезпечення захищеної ЛОМ:

Virtual Personal Network (VPN) рішення.

Поширення глобальної мережі передачі даних дає величезні можливості для об'єднання територіально розкиданих локальних мереж організацій і створення так званих приватних віртуальних мереж (VPN). Глобальні мережі в такому випадку виконують роль транспортного компонента, що об'єднує локальні мережі в єдину інформаційно-обчислювальну систему.

VPN створювалися і до стрімкого зростання глобальних мереж, однак для їх об'єднання були виділені канали передачі даних, що призводило до наступного: висока вартість оренди виділених каналів зв'язку; жорстка прихильність до місця розташування.

Наприклад, в разі переїзду офісу компанії, що має розгорнутий сегмент локальної мережі, який пов'язаний виділеним каналом із загальною мережею

підприємства, виникали додаткові проблеми з подальшим підключенням локальної і загальної мереж.

При використанні комутованих каналів глобальних мереж передачі даних можна домогтися гнучкості, масштабованості і універсальності при побудові VPN. Також розширення Internet дало можливість багатьом компаніям переводити частину персоналу на домашній режим роботи. У таких випадках співробітники мають постійний зв'язок з фірмою в рамках, наприклад, системи електронного документообігу, при цьому проблема зв'язку його з мережею офісу вирішують за допомогою провайдерів.

Потреби в забезпеченні безпеки мереж на основі протоколу IP постійно зростають. У сучасному світі бізнесу, сильно пов'язаному з допомогою Інтернету, интрасетей, дочірніх відділень і віддаленого доступу, дуже важливу інформацію постійно переміщують через кордони мереж. Завдання мережевих адміністраторів і інших фахівців інформаційних служб слід бачити в тому, щоб цей трафік не допускав:

- модифікацію даних під час їх передачі по каналах;
- перехоплення, перегляд або копіювання;
- доступ до даних з боку неавторизованих користувачів.

Зазначені проблеми можна позначити як забезпечення цілісності даних, конфіденційності та аутентифікації. Також необхідно захищати від відтворення інформації.

При вирішенні проблем передачі інформації через відкриті канали інтернет використовуються VPN рішення. VPN - це об'єднання декількох локальних мереж, які підключені до мережі загального призначення, в єдину віртуальну (логічно виділену) мережу. VPN кошти утворюють захищений тунель між двома точками за допомогою криптографії. Крім того, вони надають широкі можливості для вибору алгоритмів аутентифікації, шифрування і перевірки цілісності потоку даних.

При застосуванні VPN ресурси компанії можна легко консолідувати і вживати з більшою ефективністю. Через того, що VPN працює по мережі

інтернет, у компанії не виникає значних витрат, пов'язаних з купівлею додаткового обладнання та орендою ліній зв'язку. Використання виділених (орендованих) ліній зв'язку може збільшити витрати до сотень тисяч доларів, а такі витрати досить складно виправдати.

Головне достоїнство VPN - це можливість забезпечення безпеки багатьох комунікаційних потоків за допомогою одного механізму. VPN-з'єднання захищає web, e-mail, ftp, інтернет-відеоконференції і будь-які інші потоки даних, які використовують протокол Тср / ІР. Більш конкретно - потоки інформації захищені від небажаних одержувачів з використанням криптографічних методів.

Завдяки VPN можливо уникнути багатьох загроз.

VPN зберігає цілісність і конфіденційність даних за допомогою шифрування а також їх аутентифікацію шляхом застосування спеціальних протоколів і схем аутентифікації.

Також кошти VPN через збереження інформації, що відноситься до транспорту ІР пакетів захищені від ряду мережевих атак, таких як ІР-spoofing і hijacking, також вони захищені від атак типу man-in-the-middle.

В процесі реалізації ПО при створенні VPN або його апаратної реалізації можуть бути уразливості, але, як правило, на практиці використовують перевірені часом відомі розробки, для яких випускаються постійні оновлення та заплатки.

Основні вимоги, які повинні виконувати рішення VPN, такі:

- аутентифікація користувача. Засіб має аутентифіцировать віддаленого VPN-клієнта і допускати тільки авторизованих користувачів. Воно також має забезпечувати політику аудиту для перегляду активності користувачів: хто, коли і на який час підключався;
- управління ІР адресами. Засіб VPN має видавати адреси з підмережі і давати гарантію, що ці адреси не розкриваються;
- шифрування даних. Дані, що передаються по публічних мереж, повинні бути нечитабельним;

- управління ключовою інформацією. VPN-засіб повинен генерувати ключі для шифрування і оновлювати їх з певною періодичністю.

Технологія екранування мережі.

Основні засоби захисту локальної обчислювальної мережі - це міжмережеві екрани. У літературі зустрічаються їх синоніми, такі як: брандмауер, firewall, фільтруючий маршрутизатор тощо.

Під усіма цими термінами мається на увазі одне і те ж, є одне функціональне призначення, але може міститися різний набір інструментів захисту.

Мережеві екрани є лише інструментами системи безпеки. Мережеві екрани - це засіб реалізації політики безпеки на мережевому рівні, вони дають певний рівень захисту. Рівень безпеки, що надається мережевим екраном, може варіюватися в залежності від вимог безпеки. Досягається традиційний компроміс між безпекою, простотою використання, вартістю, складністю тощо

Мережевий екран - один з декількох механізмів, які використовують для управління і спостереження за доступом до мережі з метою її захисту.

Системою firewall замінюється маршрутизатор або зовнішній шлюз мережі. Захищену частину мережі розміщують за ним. Пакети, адресовані Firewall, обробляють локально, а не просто переадресовують. Пакети ж, адресовані об'єктам, розташованим за Firewall, не доставляються. З цієї причини хакеру доводиться мати справу з системою захисту Firewall.

Така схема є більш простою і надійною, так як слід дбати про захист однієї машини, а не багатьох. Зазвичай мережевий екран - це мережева станція з двома і більше мережевими інтерфейсами. При цьому один інтерфейс здійснює зв'язок з Інтернет, а другий - з захищеною мережею. Мережевий екран поєднує функції маршрутизатора-шлюзу, екрану і управління екраном.

Недоліки FireWall впливають з її переваг: ускладнюючи доступ ззовні, система ускладнює і доступ назовні.

Для більшості програм, працюючих на нестандартних портах і не підтримують проксі-сервера, для установки з'єднання необхідно або відкрити порти, або відмовитися від їх використання. Служби FTP в системі може і не бути, але якщо вона присутній, доступ можливий тільки через сервер FireWall. Внутрішні ПК не можуть встановити пряму FTP-зв'язок ні з якою ЕОМ з зовнішнього світу.

Отже, з метою безпеки захищена мережа не повинна мати вихід у зовнішній світ крім системи МЕ, в тому числі і через модем. Екрани конфігурують так, щоб маршрут за замовчуванням було вказано на захищену мережу.

Для користувачів захищеної мережі створюють спеціальний вхід для FTP та інших послуг. При цьому можна не вводити будь-які обмеження щодо транспортування файлів в захищену мережу і блокувати передачу будь-яких файлів з цієї мережі, навіть в разі, коли ініціатором FTP-сесії є клієнт захищеної мережі. У зовнішніх клієнтів Інтернет немає доступу ні до однієї з захисних ЕОМ ні через один з протоколів.

У більшості випадків до МЕ екрану висувають такі вимоги:

- фільтрацію пакетів на мережевому рівні;
- фільтрацію пакетів на прикладному рівні;
- налаштування правила фільтрації та адміністрування;
- використання стійкого протоколу для аутентифікації по мережі;
- проведення журналу аудиту.

Системи Intrusion Detection System (IDS);

Системи визначення атаки IDS займаються моніторингом інформаційної системи на мережевому і прикладному рівнях з метою виявлення порушень безпеки і оперативного реагування на них. Мережеві IDS є джерелами даних для аналізу мережевих пакетів, а IDS прикладного рівня аналізуються записи журналів аудиту безпеки ОС і додатків. При цьому методи аналізу (виявлення атак) загальні для всіх класів IDS.

Були запропоновані різні підходи до вирішення завдань виявлення атак. У загальному випадку розглядається навмисна активність, що включає, крім атаки, дії, що виконуються в рамках наданих повноважень, але порушують встановлені правила політики безпеки. Однак всі існуючі IDS поділяють на два основні класи: одні застосовують статистичний аналіз, інші - сигнатурний аналіз.

Статистичні методи передбачають, що активність зловмисника завжди пов'язана з якимись аномаліями, зміною профілю поведінки користувачів, програм і апаратури.

Основний метод виявлення атак - це, прийнятий в більшості сучасних комерційних продуктів, сигнатурний аналіз. Через відносну простоту даний метод можна з успіхом впроваджувати в практику. IDS, які використовують сигнатурний аналіз, зазвичай нічого «не знають» про правила політики безпеки, що реалізуються мережевим екраном, тому в даному випадку мова йде не про навмисну активності, а тільки про атаки.

Основний принцип їх функціонування полягає в порівнянні відбуваються в системі / мережі подій з сигнатурами відомих атак - той же, що використовується в антивірусному ПЗ.

Є два що не виключають один одного підходу для виявлення мережевих атак: аналіз мережевого трафіку і аналіз контенту. У першому випадку вивчаються лише заголовки мережевих пакетів, у другому - їх вміст. Але найбільш повний контроль інформаційних взаємодій відбувається тільки за допомогою аналізу вмісту всіх мережевих пакетів, включаючи їх заголовки і області даних.

Однак з практичної точки зору таке завдання важко виконати через величезний обсяг даних, які довелося б обробляти.

У сучасних IDS починаються серйозні проблеми з продуктивністю вже при швидкості 100 Мб/с в мережах. Тому найчастіше вдаються для виявлення атак до аналізу мережевого трафіку, в окремих випадках поєднуючи його з аналізом контенту.

Як вже зазначалося вище, відповідні продукти діляться на системи IDS на базі мережі і на базі хоста. Обидві системи намагаються виявити вторгнення, але обробляються абсолютно різні дані.

Система IDS на базі мережі для розпізнання атаки читає потік даних, подібно до аналізатору. Вона складається, головним чином, з реєструючих всі мережеві пакети сенсорів, інтерфейс яких підключений до призначеному для аналізу або копіювання порту комутатора. Як альтернатива для підключення в мережу такої системи можуть застосовуватися концентратори.

Системою IDS на базі хоста використовуються агенти. Вони функціонують в якості невеликого додаткового програмного забезпечення на контрольованих серверах або робочих місцях і проводять аналіз активності на підставі даних журналів реєстрацій та аудиту для пошуку ознак небезпечних подій.

Найстарішим і найпоширенішим методом виявлення атак є так зване зіставлення з шаблоном. Як і в разі сканування вірусів, він спирається на список шаблонів або сигнатур, на підставі яких робиться висновок про атаку. Таким чином, подібними системами порівнюються всі пакети даних з усіма шаблонами, і при збігу з одним з них вважається, що виявлено вторгнення. Недоліки методу - великі витрати, а крім того - погана масштабованість. Набагато ефективнішим є метод аналізу протоколів, в процесі якого не проводиться послідовного порівняння з шаблоном, а спочатку декодуються використовувані при взаємодії протоколи. Відхилення від дозволеного стандарту вже служить першим вірогідним ознакою атаки. Додатково можуть бути використані різні шаблони, але трафік даних буде порівнюватися тільки з відносяться до відповідного протоколу шаблонами, через що значно підвищується продуктивність. Однак на практиці межа між аналізом протоколу і оптимізованим з урахуванням протоколів зіставленням з шаблонами залишається нечіткою.

Як і у системи захисту від вірусів, ефективність системи IDS на базі мережі багато в чому залежить від актуальності шаблонів. Так як нові

уразливості виявляють кожен день і зловмисник не упустить можливості скористатися багатьма з них, системи IDS повинні бути завжди актуальні. Якщо шаблони оновлювати раз на місяць, то слід врахувати, що в проміжку між оновленнями з'являться нові, не розпізнані системою атаки. Проблема існуючої системи визначення атак укладена в високих витратах через значної кількості хибних сигналів тривоги. Вони виникнуть, якщо шаблони зі списку зустрічаються в звичайних потоках даних, навіть при відсутності атак, або коли звичайна програма буде використовувати незначну модифікації стандартного протоколу, що в кінцевому рахунку призведе до подачі системи IDS сигналу тривоги. Іноді причиною послужать мережева помилка, неправильно конфігурований сервер або робочі місця.

Щоб уникнути помилкового сигналу тривоги застосовують різні підходи. Перш за все, використовують комплексний шаблон: ймовірності того, що вони з'являються в звичайному трафіку, невелика. Однак комплексний шаблон погіршує продуктивність сенсорів, і цей шлях не є перспективним

- адже виробник постійно намагається перевершити і так досить велику максимальну пропускну здатність сенсора.

Важливою ознакою якісних систем виявлення атаки є не тільки і не стільки те, яка кількість трафіку вони здатні проконтролювати і проаналізувати, а, перш за все, точність виявлення і наявний інструментарій у адміністраторів для додаткових стеження і аналізування вручну. У цьому випадку просто і швидко отримати інформації про іншу протоколюються діяльності по тому ж самому початковому або кінцевому адресою - це тільки самий початок роботи.

Криптографія.

Криптографія використовується для вирішення трьох основних завдань:

- забезпечення конфіденційності даних;
- контроль цілісності даних;

- забезпечення достовірності авторства даних.

Перше завдання вирішується за допомогою симетричних алгоритмів шифрування. Для вирішення другої і третьої задач потрібне використання асиметричних алгоритмів та електронного цифрового підпису (ЕЦП).

У симетричних алгоритмах для шифрування і розшифрування застосовується один і той же криптографічний ключ. Для того щоб і відправник, і одержувач могли прочитати вихідний текст (або інші дані, не обов'язково текстові), обидві сторони повинні знати ключ алгоритму.

Асиметричні алгоритми шифрування використовують два математично пов'язаних ключа: відкритий ключ і закритий ключ. Для шифрування застосовується відкритий ключ, для розшифрування - закритий ключ. Відкритий ключ поширюється вільно. Закритим ключем володіє тільки користувач, який створює пару асиметричних ключів. Закритий ключ слід зберігати в секреті, щоб виключити можливість його перехоплення.

Цифровий підпис захищає дані в такий спосіб:

- для підписання даних використовується хеш-функція, за допомогою якої визначається хеш-сума вихідних даних. За хеш-суми можна визначити, чи мають місце будь-які зміни в цих даних.
- отримана хеш-сума підписується цифровим підписом, дозволяючи підтвердити особистість підписала. Крім того, цифровий підпис не дозволяє підписала особі відмовитися від авторства, так як тільки воно володіє закритим ключем, використаним для підписання. Неможливість відмовитися від авторства називається невідокремленістю.

В організаційні заходи щодо захисту інформації включена політика безпеки. Від її ефективності залежать в значній мірі заходи з метою забезпечення інформаційної безпеки.

Політика інформаційної безпеки являє собою сукупність документованих управлінських рішень, призначених для захисту інформаційних ресурсів організації, що забезпечує ефективне управління і з боку керівництва організації надається підтримка політики в сфері інформаційної безпеки.

Політику безпеки будують на основі аналізу ризиків. З урахуванням ризику, виявленого в організаціях, в політику інформаційної безпеки для організації можуть бути включені наступні розділи:

1. Введення. Необхідність створення політики безпеки внаслідок того, що виявлені недоліки в інформаційній безпеці ТОВ ТОРГОВИЙ ДІМ “Гранд-трейд”;

2. Мета політики. Розробка СІБ необхідна з метою комплексного вирішення завдання забезпечення інформаційної безпеки в підрозділі на основі нової технології і обладнання, які відповідають сучасним вимогам, а також з чинними нормативними документами, техвимоги і умов органів держнагляду.

Основна функція систем інформаційної безпеки - це забезпечити адекватний захист, цілісність і конфіденційність інформаційного ресурсу компанії.

Головна мета систем забезпечення інформаційної безпеки - це забезпечити стійке функціонування підприємств, запобігти загрозам їх безпеки, захистити законні інтереси підприємств від протиправного посягання, не допустити втрату фінансових коштів, розголошення, втрату, витік, спотворення і знищення службової інформації, забезпечити нормальну діяльність усіх співробітників підприємства. Ще одна мета системи інформаційної безпеки - це підвищити якість наданої послуги і гарантій безпеки інтересів клієнта.

3. Область застосування.

ТОВ ТОРГОВИЙ ДІМ “Гранд-трейд” є підприємством з розподілом по корпоративній мережі комерційних інформаційних ресурсів, що підлягають захисту. Дану політику застосовують до всіх співробітників, які мають доступ до будь-якого інформаційного ресурсу компанії;

4. Політика.

4.1. Вимога до Системи в цілому:

Вимоги до структури і функцій системи. ІБ повинна мати:

- CRM систему, розгорнуту на підприємстві;
- організаційне забезпечення;
- нормативно-правове забезпечення;
- прикладне програмне забезпечення;
- комплекс технічних засобів;
- інформаційне забезпечення.

Вимога до способу і засобу захисту зв'язку з метою інформаційних обмінів:

- транспортний і мережевий рівень взаємодії повинен використовувати стандартизований стек протоколів Тср/IP.

- на канальному і фізичному рівні взаємодії необхідно реалізовувати засоби локальних мереж користувачів та Інтернет.

Необхідно забезпечення функціонування системи інформаційної безпеки в одному з наступних режимів:

- в штатному режимі (в режимі роботи, що забезпечує виконання користувачем своєї функціональної обов'язки);
- в сервісному режимі (при проведенні обслуговування, реконфігурації та поповненні новим компонентом);
- в аварійному режимі.

1. Вимога до персоналу системи (чисельність і кваліфікація) і режиму його роботи:

Персонал ІБ повинен включати:

- користувачів ІБ;
- адміністратора ІБ.

2. Вимога до надійності:

3. Вимога безпеки.

4. Вимоги, пов'язані з експлуатацією, технічному обслуговуванням, ремонтом і зберіганням комплектів системи: експлуатацію ІБ необхідно проводити відповідно до експлуатаційних документів і Регламентом

технічного обслуговування та обслуговування ІБ повинен виробляти адміністратор інформаційної безпеки.

Допускається використовувати спеціалізовані служби або підрозділу на об'єкті впровадження при обслуговуванні та ремонті устаткування.

5. Вимоги до патентної чистоти.

6. Вимоги до стандартизації та уніфікації.

2) Вимоги до функцій.

2.1. Підсистема, що управляє доступом:

- Необхідно ідентифікувати термінали, ЕОМ, вузли мережі ЕОМ, канали зв'язку, зовнішні пристрої ЕОМ по їх логічним адресами (номерах);
- Необхідно здійснювати реєстрацію входу (виходу) суб'єкта доступу в систему (з системи);
- Необхідно управляти потоком інформації за допомогою мітки конфіденційності;
- Необхідно реєструвати запуск (завершення) програми і процесу (завдання, задачі), призначеної для обробки захищається файлу;
- Необхідно реєструвати спроби доступу програмних засобів до будь-якого з об'єктів, що захищаються доступу: ПК, вузли мережі, лінії (канали) зв'язку, зовнішні пристрої, програми, каталоги, файли, записи, поля записів.

2.2. Криптографічна підсистема. Необхідно шифрувати всю інформацію, яка записується на носії даних, що використовуються спільно різними суб'єктами доступу, в канали зв'язку, а також на знімний носій даних довготривалої зовнішньої пам'яті, щоб зберігати поза межами сеансу роботи санкціонованого суб'єкта доступу. При цьому повинна автоматично звільнятися і очищатися область зовнішньої пам'яті, що містила раніше незашифровану інформацію;

- доступ суб'єкта до операції шифрування і криптографічного ключа необхідно контролювати за допомогою підсистеми управління доступом.

### 2.3. Забезпечення цілісності:

- необхідно забезпечити цілісність програмного засобу СЗІ, оброблюваної інформації, а також сталість програмної середовища.

При цьому:

- перевіряти цілісність СЗІ при завантаженні систем за наявності ідентифікаторів (імен) компонент СЗІ;

- необхідно здійснювати фізичну охорону СВТ (пристрої та носія інформації), передбачено постійна наявність охорони на території будівлі, де розміщено АС (відеоспостереження, суворий пропускний режим, спеціальне обладнання приміщення АС);

- необхідна наявність адміністратора (служби) захисту інформації, відповідального за ведення, нормальну діяльність і контроль роботи СЗІ;

- необхідно періодично тестувати функції СЗІ при змінах програмного середовища і персоналу АС за допомогою тест - програми, що імітує спробу несанкціонованого доступу;

- необхідно використовувати сертифіковані засоби захисту.

### 3. Вимоги до забезпечення.

#### 3.1. Вимоги до програмного уязі забезпечення:

- При побудові СІБ необхідно користуватися сучасними програмними рішеннями від провідних виробників в області інформаційної безпеки.

#### 3.2. Вимоги до технічного виду забезпечення:

- СІБ повинна бути забезпечена комплексний захист додатків і кожного об'єкта ІТ-інфраструктури, заснована на передових технологіях безпеки, можливість працювати з будь-якими апаратними платформами (Windows, aUnix / Linux), можливість масштабувати і мати гнучку конфігурацію використовуваного апаратно-програмного продукту безпеки.

#### 3.3. Вимоги до організаційного виду забезпечення:

- Необхідна наявність відповідальності за порушення режимів безпеки інформації (вимоги до метрологічного, математичного та лінгвістичного забезпечення).

#### 4. Порядок контролю системи:

##### 4.1. Контроль за функціонуванням СБ повинен бути забезпечений з допомогою:

- сил власних підрозділів по захисту інформації (адміністратор безпеки);

#### 5. Вимоги до документування:

В проектну документацію на системи захисту інформації повинна бути включена така документація з інформаційної безпеки:

- посадові інструкції користувачів;
- посадові інструкції адміністраторів по ІБ (Додаток);
- тестові та інструктивно-методичні документи;
- конструкторські (проектні) документи.

#### 6. Джерела розробки:

##### 1. Технічні завдання на створення автоматизованих систем.

2. Види, комплектність і позначення документації при створенні автоматизованої системи.

##### 3. Вимоги до змісту документтації.

Відстежує всі внесені в документи зміни (дату, автора, коротку суть змін).

За допомогою такої структури можливо короткий опис всіх основних моментів, пов'язаних з політикою безпеки організації, «не прив'язуючись» до конкретного технічного рішення, продукту і виробнику. Інакше при зміні політичної ситуації на підприємстві тощо. Може виникнути необхідність в зміні концепції ІБ, а цього відбуватися не повинно.

Також в політиці безпеки організації повинно бути визначення обов'язків посадової особи для вироблення програм безпеки та проведення їх в життя. Таким чином, політика безпеки - це основа підзвітності персоналу.

На адміністративний рівень інформаційної безпеки відносять дії загального характеру, які робляться керівництвом підприємства.

Головний сенс заходів на адміністративному рівні - формування програми робіт в областях інформаційної безпеки і забезпечення її виконання, виділення необхідних ресурсів і контроль стану справ.

Основою програм є політики безпеки, що відображають підходи організації до захисту інформаційного активу. Керівництво компанії має усвідомлювати необхідність підтримки режимів безпеки і виділення на ці цілі значного ресурсу, а також призначення відповідального за розробку, впровадження та супровід систем безпеки.

Для ТОВ ТОРГОВИЙ ДІМ "Гранд-трейд" актуальним є створення політик інформаційної безпеки разом генеральним директором і адміністраторами з інформаційної безпеки, які будуть нести відповідальність за розробку, впровадження та вдосконалення системи безпеки.

З практичної точки зору політика безпеки доцільно розглядається на трьох рівнях деталізації. До верхнього рівня відносять рішення, що зачіпає підприємство в цілому. Воно носить досить загальний характер і виходить від керівництва організації. Повідомлення про ухвалені рішення цього рівня включають в себе наступне:

- рішення формувати або переглядати комплексні програми забезпечення інформаційної безпеки, призначення відповідальних за просування програм;
- формулювання мети, яку переслідує організація в області інформаційної безпеки, визначення загального напрямку досягнення цієї мети;
- забезпечити базу для дотримання законів і правил;
- сформулювати адміністративні рішення по тому питанню реалізації програми безпеки, яке повинні розглядати на рівні підприємства в цілому.

Для політик верхнього рівня мета організацій в області інформаційної безпеки формулюють в термінах цілісності, доступності та конфіденційності. Так як в організації відбувається безперервний потік даних у всіх структурних підрозділах, то на першому плані знаходяться завдання зменшення числа втрат, розкрадань або спотворення даних.

На верхньому рівні знаходяться управління захисним ресурсом і координація використання цього ресурсу, виділення спеціальних персоналів для захисту критично важливої системи і взаємодія з іншими підприємствами, які забезпечують або контролюють режими безпеки.

Політику верхнього рівня застосовують в трьох аспектах: законослухняності і виконавської дисципліни.

По-перше, організації повинні дотримуватися існуючих законів.

По-друге, необхідний контроль дій осіб, які відповідають за роботу над програмою безпеки. Нарешті, слід забезпечувати певні ступеня старанності персоналу, а для цього слід виробляти системи заохочень і покарань.

### **3.3. Обґрунтування економічної доцільності запропонованого проєкту**

Відправною точкою при економічній ефективності є майже очевидне припущення: з одного боку, при порушенні захищеності інформації наноситься деякий збиток, з іншого - забезпечення захисту інформації пов'язане з витрачанням коштів. Повна очікувана вартість захисту може бути виражена сумою витрат на захист і втрат від її порушення.

Оптимальним рішенням було б виділення на захист інформації засобів, які мінімізують загальну вартість робіт із захисту інформації.

Економічна ефективність заходів щодо захисту інформації може бути визначена, через обсяг запобігання шкоди або величину зниження ризику для інформаційних активів організації.

Для того щоб скористатися даною підходом до вирішення проблеми, необхідно знати:

- по-перше, очікувані втрати при порушенні захищеності інформації;
- по-друге, залежність між рівнем захищеності і засобами, затраченими на захист інформації.

Для визначення рівня витрат  $R_i$ , що забезпечують необхідний рівень захищеності інформації, необхідно, принаймні знати:

- по-перше, повний перелік загроз інформації;
- по-друге, потенційну небезпеку для інформації для кожної із загроз;
- по-третє, розміри витрат, необхідних для нейтралізації кожної із загроз.

Оскільки оптимальне вирішення питання про доцільний рівні витрат на захист полягає в тому, що цей рівень повинен бути дорівнює рівню очікуваних втрат при порушенні захищеності, досить визначити тільки рівень втрат. В якості однієї з методик визначення рівня витрат можливо використання наступної емпіричної залежності очікуваних втрат (ризиків) від  $i$ -й загрози інформації.

Для розрахунку будуть взяті 4 найцінніших активу організації ТОВ ТОРГОВИЙ ДІМ “Гранд-трейд”, визначених у попередньому розділі і відповідні їм загрози з оцінкою «висока».

Наведемо приклад розрахунку величини втрати для інформаційного активу про послуги, що надаються і загрози для нього - перехоплення інформації:

1) по шкалі очікуваної частоти появи загрози, виберемо передбачуване значення  $S_i = 5$  (1 раз на місяць, приблизно 10 раз в рік);

2) за шкалою очікуваного значення можливого збитку при появі загрози, виберемо передбачуване значення  $V_i = 4$  (300 тис. грн.).

3) підставимо значення в формулу:

$$R_i = 10 (S_i + V_i - 4), \quad \text{де:}$$

$S_i$  - коефіцієнт, що характеризує можливу частоту виникнення відповідної загрози;

$V_i$  - коефіцієнт, що характеризує значення можливого збитку при її виникненні

$$R_i = 10 (5 + 4 - 4)$$

$$R_i = 100\,000 \text{ грн}$$

В результаті розрахунку визначаємо сумарну вартість втрат: сумарна вартість втрат визначається формулою

$$R = \sum_{i=1} R_i$$

де  $N$  - кількість загроз інформаційних активів, визначених, в п.1.2.3; варто відзначити, що сумарна вартість втрат розраховується окремо для кожного активу.

Наведемо приклад розрахунку сумарної величини втрати для інформаційного активу про послуги, що надаються :

1)  $N = 3$ ; тому саме 3 загрози для даного активу мають значення оцінки «Висока»;

$$2) R_i = 210\,000 (100\,000 + 100\,000 + 10\,000);$$

3) підставимо значення в формулу:

$$R = \sum_{i=1} 210\,000$$

$$R = 630\,000 \text{ грн}$$

Розрахунок для всіх найцінніших активів і актуальних для них загроз представлений в табл. 3.1.

Таблиця 3.1

**Величини втрат для критичних інформаційних ресурсів  
до модернізації системи захисту інформації**

| Актив                         | Загроза                                                                      | Величина втрат |
|-------------------------------|------------------------------------------------------------------------------|----------------|
| Послуги, що надаються         | нелегальне проникнення зловмисників під виглядом санкціонованих користувачів | 100000         |
|                               | перехоплення інформації                                                      | 100000         |
|                               | зміна сенсу переданої інформації                                             | 10000          |
| 3 питань забезпечення безпеки | нелегальне проникнення зловмисників під виглядом санкціонованих користувачів | 100000         |
|                               | перехоплення інформації                                                      | 100000         |

Продовж. табл. 3.1

|                               |                                                                             |                |
|-------------------------------|-----------------------------------------------------------------------------|----------------|
| Відомості ділового характеру  | нелегальне проникнення зломисників під виглядом санкціонованих користувачів | 10000          |
|                               | зміна сенсу переданої інформації                                            | 10000          |
| Торгово-економічні питання    | нелегальне проникнення зломисників під виглядом санкціонованих користувачів | 10000          |
| <b>Сумарна величина втрат</b> |                                                                             | <b>1080000</b> |

Джерело: розраховано автором

Найбільш загальною формою подання ресурсу є грошова міра.

Ресурс, що виділяється на захист інформації, може мати разовий і постійний характер. Зміст і обсяг разового ресурсу, що виділяється на захист інформації в ТОВ ТОРГОВИЙ ДІМ “Гранд-трейд” представлено в табл. 3.2

Таблиця 3.2

**Зміст і обсяг разового ресурсу, що виділяється  
на захист**

| <b>Організаційні заходи</b>                                        |                                            |                                   |                        |
|--------------------------------------------------------------------|--------------------------------------------|-----------------------------------|------------------------|
| Дії                                                                | Середньогодинна зарплата спеціаліста (грн) | Трудомісткість операції (люд/год) | Вартість, всього (грн) |
| Встановлення та налаштування ViPNet Office 2.2                     | 250                                        | 1/18                              | 4500                   |
| Вартість проведення організаційних заходів, всього                 |                                            |                                   | 4500                   |
| <b>Заходи інженерно-технічного захисту</b>                         |                                            |                                   |                        |
| Номенклатура витратних матеріалів                                  | вартість, одиниці (грн)                    | Кількість (од)                    | Вартість, всього (грн) |
| ViPNet Office 2.2                                                  | 135,000                                    | 1 шт.                             | 135000                 |
| IBM PC 2480 GS                                                     | 11,230                                     | 1 шт.                             | 11200                  |
| IBM PC 5700 L                                                      | 22,150                                     | 1 шт.                             | 22,100                 |
| Вартість проведення заходів інженерно-технічної захисту            |                                            |                                   | 168300                 |
| <b>Обсяг разового ресурсу, що виділяється на захист інформації</b> |                                            |                                   | <b>172800</b>          |

Джерело: розраховано автором

Зміст і обсяг постійного ресурсу, що виділяється на захист інформації в ТОВ ТОРГОВИЙ ДІМ “Гранд-трейд” представлено в таблиці 3.3.

Сумарне значення ресурсу виділяється на захист інформації на підприємстві ТОВ ТОРГОВИЙ ДІМ “Гранд-трейд” становить 682000 грн (172800 + 509200).

Таблиця 3.3

**Зміст і обсяг постійного ресурсу, що виділяється на захист**

| <b>Організаційні заходи</b>                                                   |                                        |                                   |                              |
|-------------------------------------------------------------------------------|----------------------------------------|-----------------------------------|------------------------------|
| Дії                                                                           | Середньогодинна зарплата фахівця (грн) | Трудовісткість операції (люд/год) | Вартість, всього (тис. грн.) |
| Заробітна плата адміністратора ІБ                                             | 220                                    | 1/2160                            | 475200                       |
| Навчання і підвищення професійних навичок                                     | 40                                     | 6/100                             | 24000                        |
| <b>Вартість проведення організаційних заходів, всього</b>                     |                                        |                                   | 499200                       |
| <b>Заходи інженерно-технічного захисту</b>                                    |                                        |                                   |                              |
| Номенклатура витратних матеріалів                                             | Вартість, одиниці (тис. грн)           | Кількість (од.виміру)             | Вартість, всього (тис. грн.) |
| Ліцензія на рік Kaspersky Internet Security (10 роб. станцій + 1 файл сервер) | 10000                                  | 1 шт.                             | 10000                        |
| <b>Вартість проведення заходів інженерно-технічної захисту</b>                |                                        |                                   | 10000                        |
| <b>Обсяг постійного ресурсу, що виділяється на захист інформації</b>          |                                        |                                   | 509200                       |

Джерело: розраховано автором

Проведемо розрахунок часу окупності модернізованої системи захисту інформації, виконаний аналітичним і графічним способом. Для цього необхідно отримати прогнозовані дані про величину втрат для критичних інформаційних ресурсів після модернізації системи захисту інформації, табл. 3.4

Таблиця 3.4

**Величини втрат для критичних інформаційних ресурсів після модернізації системи захисту інформації**

| Актив                         | Загроза                                                                      | Величина втрат (грн) |
|-------------------------------|------------------------------------------------------------------------------|----------------------|
| Послуги, що надаються         | нелегальне проникнення зловмисників під виглядом санкціонованих користувачів | 10000                |
|                               | перехоплення інформації                                                      | 1 000                |
|                               | зміна сенсу переданої інформації                                             | 1 000                |
| З питань забезпечення безпеки | нелегальне проникнення зловмисників під виглядом санкціонованих користувачів | 1 000                |
|                               | перехоплення інформації                                                      | 1 000                |
| Відомості ділового характеру  | нелегальне проникнення зловмисників під виглядом санкціонованих користувачів | 100                  |
|                               | зміна сенсу переданої інформації                                             | 100                  |
| Торгово-економічні питання    | нелегальне проникнення зловмисників під виглядом санкціонованих користувачів | 100                  |
| <b>Сумарна величина втрат</b> |                                                                              | 40500                |

Джерело: розраховано автором

Проведемо оцінку динаміки величин втрат за період не менше 1 року, табл. 3.5.

Таблиця 3.5

**Оцінка динаміки величин втрат, грн**

|                        | 1 кв. | 2 кв. | 3 кв. | 1 рік | 1 кв. | 2 кв. | 3 кв. | 2 рік |
|------------------------|-------|-------|-------|-------|-------|-------|-------|-------|
| До впровадження СЗІ    | 270   | 540   | 810   | 1080  | 1350  | 1620  | 1890  | 2160  |
| Після впровадження СЗІ | 10    | 20    | 30    | 40    | 50    | 60    | 70    | 80    |
| Зниження втрат         | 260   | 530   | 790   | 1040  | 1300  | 1560  | 1820  | 2080  |

Джерело: розраховано автором

Розрахуємо термін окупності системи ( $T_{ок}$ ) за допомогою формули:

$$T_{ок} = R\Sigma / (R_{ср} - R_{прогн})$$

$$T_{ок} = 682000 / (1080000 - 40500)$$

$$T_{ок} = 0,66$$

З проведених розрахунків стає зрозуміло, що впроваджується нами засіб захисту інформації починає себе окупати практично відразу, і окупить себе повністю приблизно по закінченні семи місяців, тим самим значно знижуючи грошові втрати підприємства ТОВ ТОРГОВИЙ ДІМ “Гранд-трейд” при виникненні загроз інформаційної безпеки.

## ВИСНОВКИ

На основі проведеного дослідження можна зробити наступні висновки та пропозиції:

На даний момент інформаційні ресурси стають одними з найбільш потужних інструментів економічного розвитку.

Володіння інформацією необхідних видів і якостей в потрібний момент часу і в потрібних місцях стає запорукою успіху в різних видах господарсько-економічної діяльності.

Монопольне володіння певними типами інформації виявляється часто одним з вирішальних переваг в конкурентній боротьбі та може зумовити, таким чином, високу цінність інформаційних факторів.

Широке впровадження персонального комп'ютера виводить рівень інформатизації господарського життя на якісно нові щаблі.

У наш час досить важко виявити організації або підприємства (навіть найменші), які не мали б сучасних засобів оброблення і передачі даних.

На різних носіях даних фізичні та юридичні особи накопичують величезні обсяги інформації, яка становить велику цінність для їх власників.

Процес створення індустрії обробки і зберігання інформації, хоча і створюючи об'єктивні чинники для значного збільшення ефективності процесів діяльності людини, породив безліч складних і великомасштабних проблем.

Одна з таких проблем - це забезпечення надійного збереження та встановлення статусу застосування інформації, яка циркулює і обробляється в розподіленій інформаційній системі.

Дана випускна кваліфікаційна робота присвячена модернізації системи інформаційної безпеки для локальної обчислювальної мережі ТОВ ТОРГОВИЙ ДІМ "Гранд-трейд".

Знаходження рішення даної проблеми було здійснено на базі програмного комплексу інструментів захисту інформації, яке дає можливість

побудувати надійний і високозахищений канал передачі персональних даних в рамках локальної мережі та мережі Internet (VPN), а також вирішити широкий спектр завдань захисту інформації.

Запропоновано вирішення наступних задач:

1. Проведено дослідження інфраструктури ТОВ ТОРГОВИЙ ДІМ “Гранд-трейд” і встановлені вихідні дані, які, в першу чергу, будуть використані при розробці системи захисту інформації;
2. Визначено оцінки ризиків за допомогою виявлених загроз і вразливостей в аналізованій інформаційній структурі організації;
3. Для найбільш цінного активу, схильного до високих ризиків, обрані організаційні та інженерно-технічні заходи, які покликані зменшити появу загрози інформаційної безпеки до мінімуму;
4. Вироблено опис переваг, принципів робіт, інсталяції та налаштувань обраних засобів захисту інформації;
5. Здійснено розрахунки економічної ефективності впровадження даного засобу захисту інформації.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Александров В.А. Вступление в ВТО: экономическая безопасность отечественных предприятий // Микроэкономика. - 2012. - N 6.
2. Белов Е.Б. Основы информационной безопасности. Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. -М.: Горячая линия - Телеком, 2015. – 544 с.
3. Близнюк І.М. Інформаційна безпека України та заходи її забезпечення / І.М. Близнюк //Науковий вісник Національної академії внутрішніх справ України. – 2008. – № 5. – С. 206-214.
4. Бурцев В.В. Проблемы государственной экономической безопасности // Финансы. - 2013. - N 8.
5. Галатенко В.А. Стандарты информационной безопасности: курс лекций. Учебное пособие. - 2-ое издание. М.: ИНТУИТ.РУ «Интернет-университет Информационных Технологий», 2012. - 264 с.
6. Горбатюк О.М. Сучасний стан та проблеми інформаційної безпеки України на рубежі століть /О.М. Горбатюк // Вісник Київського університету імені Т.Шевченка. – 2009. – Вип. 14: Міжнародні відносини. – С. 46-48.
7. Гуцалюк М.О. Інформаційна безпека України: нові загрози / М.О. Гуцалюк // Бизнес и безопасность. – 2007. – № 5. – С. 2–3.
8. Доповідь про інформаційну економіку: огляд проблематики розвитку // Конференція Організації Об'єднаних Націй з торгівлі та розвитку. – 2008. – С.8–10.
9. Дронов Р. Подходы к обеспечению экономической безопасности // Экономист. - 2012. - N 2.
10. Ильяшенко С.Н. Составляющие экономической безопасности кооператива и подходы к их оценке // Актуальные проблемы экономики. – 2013. - № 3.

11. Калашников А. Формирование корпоративной политики внутренней информационной безопасности. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации/ М.2014 280с.

12. Комплексні рішення по забезпеченню інформаційної безпеки  
 Подробнее: <https://goobkas.com/ua/g80296837-kompleksni-rishennya-zabezpechennyu>. (2020, 12 14). Retrieved from Goobkas: <https://goobkas.com/ua/g80296837-kompleksni-rishennya-zabezpechennyu>.

13. Коноплева И.А. Управление безопасностью и безопасностью бизнеса: учеб. пособие для вузов / И.А. Коноплева, И.А. Богданов; под ред. И.А. Коноплевой. - М.: ИНФРА-М, 2013.

14. Крошилин, С.В. Возможные угрозы безопасности экономических информационных систем и методы их устранения / С.В. Крошилин // Проблемы и методы управления экономической безопасностью регионов: Материалы межвузовской научной конференции профессорско-преподавательского состава, Коломна: КГПИ. – 2014.

15. Микадзе, С. Ю. Приоритеты экономической безопасности Российской Федерации / С. Ю. Микадзе. СПб. : Изд-во С.-Петерб. гос. ун-та экономики и финансов, 2013. - 280 с.

16. Остроухов В.В. До проблеми забезпечення інформаційної безпеки України / В.В. Остроухов //Політичний менеджмент. – 2008. – № 4. – С. 135–141.

17. Про інформацію: закон України [прийнято ВР 02.10.1992 р.] // Закони України. -К., 1996. – Т.4.

18. Родичев Ю. Информационная безопасность: Нормативно-правовые аспекты. СПб.: Питер, 2012. — 264 с. — ISBN 978-5-388-00069-9.

19. Фокина Н.П.. Экономика предпринимательства – важнейшая составляющая финансовой устойчивости // Актуальные проблемы экономики. – 2013. - № 8.

20. Цимбалюк В.С. Інформаційна безпека підприємницької діяльності: визначення сутності та змісту поняття за умов входження України до інформаційного суспільства (глобальні кіберцивілізації) / В.С.Цимбалюк // Підприємництво, господарство і право. – 2007. – № 3. – С. 88–91.
21. Чубарук Т.І. Проблеми законодавчого забезпечення інформаційної безпеки в Україні / Т.І.Чубарук // Право України. – 2007 . – № 9. – С. 67–69.
22. Шлыков В.В. Комплексное обеспечение экономической безопасности предприятия / В.В. Шлыков. - СПб.: Алетейя, 2009.
23. Шубина Т.В. Финансовые аспекты экономической безопасности компании // Микроэкономика. - 2015. - N 4.
24. Ярочкин В.И., Информационная безопасность: учебник для студентов вузов// - М.: Академический проект; Гаудеамус, 2-е изд., 2013 г., 544 с
25. Яскевич, В.И. Секьюрити. Организационные основы безопасности фирмы: учеб. пособие / В.И. Яскевич. М.: Ось-89, 2012. - 230 с.
26. Dallas Lock. Руководство по эксплуатации СЗИ НСД Dallas Lock 8.0. URL: [www.dallaslock.ru](http://www.dallaslock.ru).
27. Deming W. Edward. Out of the Crisis: Quality, Productivity, and Competitive Position. –Cambridge (Mass.) Mass. Inst. of Technology, Center for Advanced Engineering Study:Cambridge University Press, 1982.
28. Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28-STD, 1985 [Electronic resource]. – Access mode : <http://csrc.nist.gov/publications/history/dod85.pdf>.
29. Dynamic категории Threat Protection/ Руководство (дата обращения: 10.12.20).
30. Information Tecnhology Security Evaluation Criteria, v. 1.2. – Office for Officialublications of the European Communities, Printed and published by the Department of Trade andIndustry, London, 1991. – 164 p.

31. ISO/TC 176/SC 2/N 544R2, ISO 9000 Introduction and Support Package: Guidance on the Concept and Use of the Process Approach for management systems, 13 May 2004.
32. ISO/IEC 27001:2005, Information technology – Security techniques – Information security management systems – Requirements.
33. ISO/IEC 38500:2008, Corporate governance of information technology.
34. ISO GUIDE 72:2001, Guidelines for the justification and development of management system standards.
35. ISO/IEC 27003, Information technology – Security techniques – Information security management system implementation guidance.
36. NIST Special Publication 800-61, Computer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Technology, January 2004.
37. Securelist. [Electronic resource]. – Access mode : <https://statistics.securelist.com/>.
38. Secret Net 7. Руководство администратора. Настройка механизмов защиты // Компания "Код Безопасности". URL: [www.securitycode.ru](http://www.securitycode.ru).
39. Technical Report ISO/IEC TR 18044, Information technology – Security techniques – Information security incident management.