Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню бакалавра

студента *Ахмєдова Ахмеда Анара огли*

академічної групи *125-16-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Розробка міжмережевого захисту в системі захисту інформації ТОВ «Інтер-Транзит»*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	д.т.н., проф. Корнієнко В.І.			
розділів:				
спеціальний	к.т.н., доц. Флоров С.В.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Лізунова Т.Л.			

Дніпро

2020

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту *Ахмєдову Ахмеду Анару огли* **академічної групи** *125-16-1*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Розробка міжмережевого захисту в системі захисту інформації ТОВ «Інтер-Транзит»***

затверджену наказом ректора НТУ «Дніпровська політехніка» від _____ № ____

Розділ	Зміст	Термін виконання
Розділ 1	Аналіз заходів захисту від НСД інформаційно-телекомунікаційної системи ТОВ «Інтер-Транзит»	29.03.2020
Розділ 2	Розробка системи захисту інформації ТОВ «Інтер-Транзит» з детальною розробкою міжмережевого захисту	24.05.2020
Розділ 3	Визначення капітальних витрат на впровадження СЗІ, трудомісткості розробки і реалізації СЗІ. Аналіз економічної ефективності впровадження СЗІ	14.06.2020

Завдання видано _____ _____
(підпис керівника) (прізвище, ініціали)

Дата видачі: 08.01.2020р.

Дата подання до екзаменаційної комісії: 15.06.2020р.

Прийнято до виконання _____ _____
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка:___ с., ___ рис., ___ табл., ___ додатки, ___ джерел.

Об'єкт розробки: система захисту конфіденційної інформації товариства з обмеженою відповідальністю «Інтер-Транзит».

Мета роботи: на підставі чинних законодавчих і нормативних документів України розробити систему захисту інформації на товаристві з обмеженою відповідальністю «Інтер-Транзит» з детальною розробкою міжмережевого захисту.

У спеціальній частині дана характеристика об’єкту захисту, розроблена політика безпеки, модель загроз, розроблене технічне завдання на створення системи захисту конфіденційної інформації

В економічному розділі визначені капітальні витрати на впровадження СЗІ, трудомісткість розробки і реалізації СЗІ. Аналіз економічної ефективності впровадження СЗІ

Практичне значення роботи полягає в підвищенні рівня захищеності конфіденційної інформації, що циркулює в інформаційній мережі товариства з обмеженою відповідальністю «Інтер-Транзит».

СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, ПОЛІТИКА БЕЗПЕКИ, МОДЕЛЬ ЗАГРОЗ, МОДЕЛЬ ПОРУШНИКА, НЕСАНКЦІОНОВАНИЙ ДОСТУП, ПОЛІТИКА ДОСТУПУ

РЕФЕРАТ

Объяснительная записка:___ с., ___ рис. ___ табл., ___ дополнения ___ источников.

Объект разработки: система защиты конфиденциальной информации общества с ограниченной ответственностью «Интер-Транзит».

Цель работы: на основании действующих законодательных и нормативных документов Украины разработать систему защиты информации на обществе с ограниченной ответственностью «Интер-Транзит» с детальной разработкой межсетевой защиты.

В специальной части дана характеристика объекта защиты, разработанная политика безопасности, модель угроз, разработанное техническое задание на создание системы защиты конфиденциальной информации

В экономическом разделе определены капитальные затраты на внедрение СЗИ, трудоемкость разработки и реализации СЗИ. Анализ экономической эффективности внедрения СЗИ

Практическое значение работы состоит в повышении уровня защищенности конфиденциальной информации, циркулирующей в информационной сети общества с ограниченной ответственностью «Интер-Транзит».

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ, ПОЛИТИКА БЕЗОПАСНОСТИ, МОДЕЛИ УГРОЗ, МОДЕЛЬ НАРУШИТЕЛЯ, НЕСАНКЦИОНИРОВАННОГО ДОСТУПА, ПОЛИТИКА ДОСТУПА

ABSTRACT

Explanatory message:___ s., ___ fig. ___ tablas., ___ additions ___ sources.

Object of development: system of protection of confidential information of the limited liability company Inter-Transit.

Purpose of work: on the basis of the current legislative and regulatory documents of Ukraine to develop a system of protection of information at the limited liability company "Inter-Transit" with a detailed development of firewall protection.

The special part describes the characteristics of the security object, developed a security policy, a model of threats, developed a technical task for creating a system of protection of confidential information

The economic section identifies capital costs for the implementation of the GIS, the complexity of the development and implementation of GIS. Cost-effectiveness analysis of GIS implementation

The practical importance of the work is to increase the level of protection of confidential information circulating in the information network of the limited liability company "Inter-Transit".

INFORMATION PROTECTION SYSTEM, SECURITY POLICY, THRESHOLD MODEL, VIOLENCE MODEL, UNAUTHORIZED ACCESS, ACCESS POLICY

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС	—	автоматизована система;
ЕОМ	—	електронно-обчислювальна машина;
КЗЗ	—	комплекс засобів захисту
КС	—	комп'ютерна система;
КСЗІ	—	комплексна система захисту інформації;
НД	—	нормативний документ;
НД ТЗІ	—	нормативний документ системи технічного захисту інформації;
НСД	—	несанкціонований доступ;
ОС	—	обчислювальна система;
ПЗ	—	програмне забезпечення;
СЗІ	—	служба захисту інформації;
ТЗІ	—	технічний захист інформації.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС	—	автоматизована система;
ЕОМ	—	електронно-обчислювальна машина;
КЗЗ	—	комплекс засобів захисту
КС	—	комп'ютерна система;
КСЗІ	—	комплексна система захисту інформації;
НД	—	нормативний документ;
НД ТЗІ	—	нормативний документ системи технічного захисту інформації;
НСД	—	несанкціонований доступ;
ОС	—	обчислювальна система;
ПЗ	—	програмне забезпечення;
СЗІ	—	служба захисту інформації;
ТЗІ	—	технічний захист інформації.

ЗМІСТ

с.

ВСТУП

Сьогодні значна частина будь-якого бізнесу так чи інакше зводиться до роботи з інформацією, її аналізом, подальшим бізнесом-плануванням і т.д. У результаті інформація, що накопичується усередині компанії, стає дуже цінною. Наявність засобів інформаційної безпеки для запобігання витоку корпоративних даних вже є для компанії важливим активом і конкурентною перевагою.

При зміні способу зберігання інформації з паперового виду на цифровий, з'явилося головне питання – як цю інформацію захистити, адже дуже велика кількість факторів впливає на збереження конфіденційних даних. Для того щоб організувати безпечне зберігання даних, спочатку потрібно описати перелік загроз інформаційної безпеки.

Сьогодні система безпеки інформації це не просто комплекс засобів, а комплекс засобів, направлених на запобігання втраті інформації. Компанії більше не хочуть викидати гроші на вітер, вони хочуть купувати тільки те, що їм дійсно необхідно для побудови надійної системи захисту інформації і при цьому з мінімальними витратами.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Загальні відомості про Товариство з обмеженою відповідальністю «Інтер-Транзит»

В якості об’єкту інформаційної діяльності в роботі розглядається товариство з обмеженою відповідальністю «Інтер-Транзит» (далі ТОВ «Інтер-Транзит).

Підприємство займається документальним супроводженням та експедицією товарів та цінних вантажів.

Юридична адреса: індекс 49027, м. Дніпро, провулок Урицького, будинок 13, 1-й поверх.

Організаційна структура компанії приведена на рисунку 1.1.

Загальна чисельність співробітників підприємства 13 чоловік.

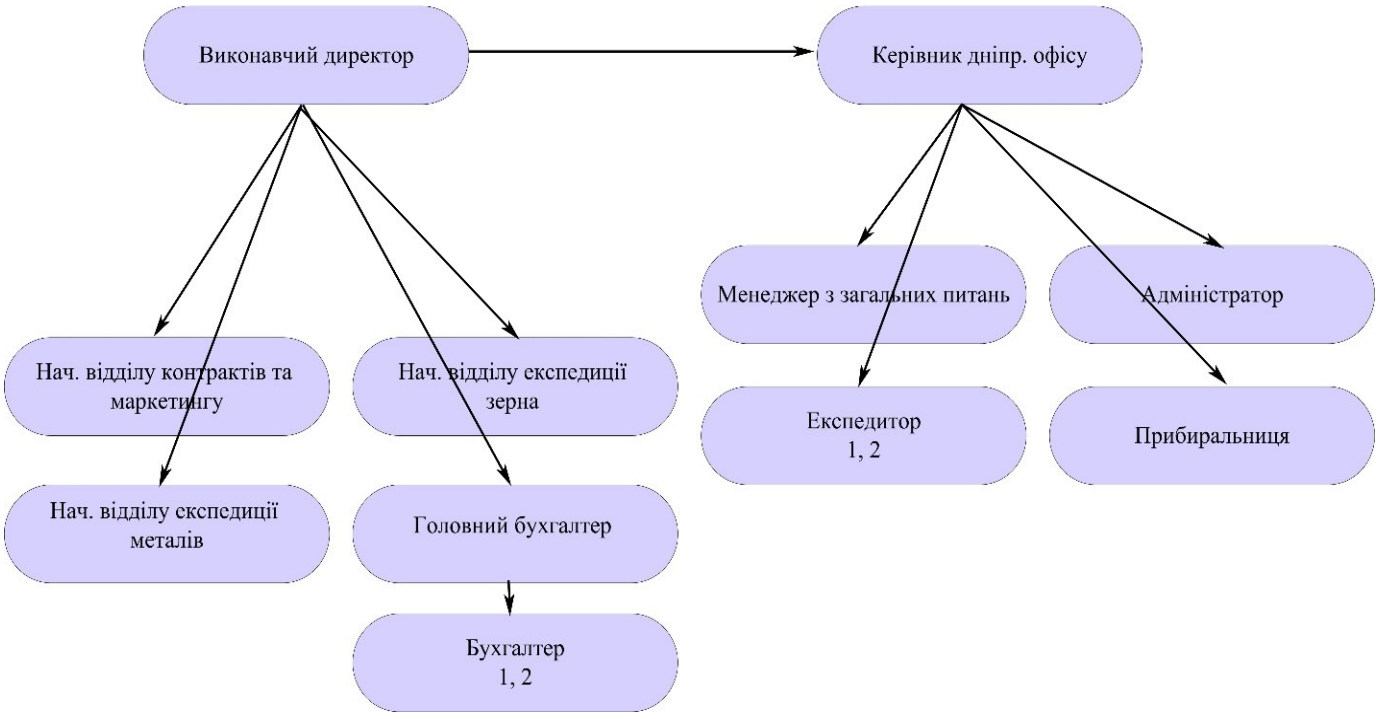


Рисунок 1.1 – Організаційна структура компанії

Для аналізу об'єкту ТОВ «Інтер-Транзит» необхідно слідувати складеному алгоритму:

I. Вивчення об’єкту:

– інформаційне середовище;
– фізичне середовище;
– обчислювальне середовище;
– середа користувачів.

II. Аналіз існуючої системи захисту інформаційних ресурсів.

III. Виявлення потенціальних каналів витоку інформації:

– розробка моделі порушника;
– розробка моделі загроз.

1.2 Характеристика інформації, що циркулює в інформаційно-комунікаційній системі підприємства

В якості інформаційно-комунікаційної системи (ІКС) підприємства виступає організаційно-технічна система, яка реалізує технологію обробки інформації за допомогою засобів обчислювальної техніки і програмного забезпечення, а також інформаційний обмін за допомогою технічних і програмних засобів передачі і прийому інформації у вигляді сигналів, знаків, звуків, зображень або іншим способом.

Інформація на підприємстві представлена в електронному вигляді і на паперових носіях. Інформація, представлена в електронному вигляді зберігається на сервері комп'ютерної мережі підприємства і знімних носіях (диски, дискети). Доступ до інформації визначається правами доступу кожного користувача.

1.2.1 Класифікація інформації, яка обробляється в інформаційно-комунікаційній системі підприємства

Всю інформацію на підприємстві можна класифікувати наступним чином:

За режимом доступу:

– відкрита;
– з обмеженим доступом (за правовим режимом).

Відкрита інформація ділиться на:

– відкриту, таку, що не потребує захисту (відомості про сплату податків і обов'язкових платежів, відомості про ліквідність підприємства, відомості про чисельність та склад працівників, фонд заробітної плати, умови праці і наявність вільних робочих місць);

– відкриту, таку, що потребує захисту (правила і інструкції роботи в ІКС, відомості із засновницьких документів статуту, відомості з документів, що дають право на підприємницьку діяльність, відомості по статутних формах звітності про фінансово-господарську діяльність);

До інформації з обмеженим доступом на підприємстві відноситься конфіденційна інформація (має велику цінність для підприємства, втрата або передача її іншим особам може нанести організації значних збитків).

До конфіденційної інформації відносяться відомості:

У сфері управління:

– про перспективні методи управління виробництвом;

Планові відомості:

– розвиток підприємства;

– про плани підприємства по розширенню виробництва;

– інвестиції підприємства;

– про проекти річних і перспективних експортно-імпортних планах по зовнішньоекономічних організаціях;

У сфері фінансів:

– планові і фактичні показники фінансового плану;

– дані про баланси підприємства;

– майнове положення;

– бюджет, обороти, дані про обороти грошових потоків підприємства;

– банківські операції, дані про фінансові операції;

– банківські зв'язки;

– специфіка міжнародних розрахунків з інофірмами;

– планові і звітні дані по валютних операціях;

– рівень доходів;

– боргові зобов'язання;

– стан кредиту;

– розміри і умови банківських кредитів;

– джерела кредитів;

– генеральна лінія і тактика у валютних і кредитних питаннях;

Про партнерів:

– круг клієнтів;

– комерційні зв'язки;

– дані про клієнтів;

– про фінансовий стан, репутації і інші дані, що характеризують ступінь надійності інофірми або представників як торгового партнера;

У сфері переговорів:

– про отримувані і опрацьовувані замовлення і пропозиції;

– про факти підготовки і ведення переговорів;

– терміни, виділені для опрацьовування і ведення операції;

– директиви по проведенню переговорів, включаючи тактику, межі повноважень посадових осіб по цінах;

– про заходи, що проводяться перед переговорами;

– про хід і результати комерційних переговорів і результати зовнішньоекономічних операцій;

– про ділові прийоми;

Про контракти:

– умови контрактів, що включають особливі умови контракту (знижки, приплати, розстрочки платежів);

– умови платежу по контрактах;

Про ціни:

– розрахунок цін;

– структура ціни і калькуляції;

– дані для калькуляції цін;

– внутрішні прейскуранти і тарифи;

– про собівартість і контрактні ціни товарів і послуг;

Про співробітників:

– домашні адреси, телефони, паспортні дані, ідентифікаційний код і інші особисті дані;

– стан здоров'я.

1.3 Аналіз фізичного середовища інформаційно-комунікаційної системи підприємства

1.3.1 Ситуаційна обстановка

Ситуаційний план приведений в Додатку Б.

Контрольована зона (КЗ) обмежена приміщенням офісу (Додаток Б). Офіс знаходиться на 1-му поверсі жилого дев’ятиповерхового будинку, за адресою: 49027, м. Дніпро, провулок Урицького, 13.

Розташування підприємства на місцевості:

Сусідами є:

– Із заходу - проїзна частина на відстані 10м, за нею знаходиться житловий 3 поверховий будинок на відстані 40м;

– Зі сходу - гаражний кооператив на відстані 40м;

– З півдня - проїзна частина на відстані 10м за нею знаходиться сквер;

– З півночі - ресторан «Святий Яков» на відстані10м.

Представництв іноземних держав поблизу даного підприємства немає.

1.3.2 Фізичне середовище інформаційно-комунікаційної системи підприємства

Елементи конструкції приміщення:

Стіни:

– зовнішні: цеглина, товщина 0.6м.

– внутрішні: залізобетон, товщина 0,3м.

З внутрішньої сторони стіни приміщення обшиті гіпсокартоном.

Підлога покрита лінолеумом: 0,3м - товщина плити, 0,05м - товщина стягування, 0,01м - товщина звукоізоляційного матеріалу, 0,008м - товщина лінолеума.

Стеля підвісна: 0,25м - простір між плитою і підвісною стелею, 0,012м – гіпсокартон.

Вікна: 1,4х1,9м, а в бухгалтерії – 1,4х2,1 металопластикові однокамерні склопакети, товщина скла 6 мм. Вікна виходять в двір будівлі, а також на проїзну частину (Додаток Д), закриті вертикальними шторами жалюзями зсередини та ролетами з вулиці.

Двері міжкімнатні: 2,04х0,8м.

Вхідні двері: 1,14х2,24, броньовані, електромагнітний замок (12/24 В, 300 кг, сірий). Двері в кабінети директора і бухгалтерію обладнані механічними замками. Всі міжкімнатні двері виконані з твердих порід дерева.

Система освітлення виконана з використанням світлодіодні лампи, які використовуються в темний період доби.

У приміщенні відсутні незадіяні кабелі.

У приміщенні відсутні засоби і системи, застосування яких не обґрунтовано службовою і виробничою необхідністю.

Кабель телефонної мережі сполучений з АТС підприємства, яка знаходиться в тамбурі (Додаток Б).

Електроживлення здійснюється від трансформаторної підстанції (№256130), яка знаходиться у дворі будинку, за межами КЗ і має сторонніх споживачів: інші квартири, розташовані в будинку. Безпосередньо електроживлення здійснюється від щита освітлення Що-№420 6 кабелем, який проходить в межах КЗ.

Система опалювання, комунікації системи опалювання мають вихід за межі КЗ.

Система вентиляції в приміщенні підприємства забезпечується за допомогою систем кондиціонування і вентиляційних шахт.

Пожежна і охоронна сигналізації запрограмовані від централі РС 585. Радіостанції у виділеному приміщенні відсутні.

Сейф знаходиться в кабінеті директора і призначений для зберігання готівки.

1.4 Характеристика персоналу інформаційно-комунікаційної системи підприємства

Весь персонал підприємства складається з 13 чоловік: виконавчий директор, керівник дніпровського офісу, начальник відділу контрактів та маркетингу, начальник відділу експедиції металів, начальник відділу експедиції зерна,менеджер з загальних питань, адміністратор(внештатний), екпедитор1 і експедитор2, головний бухгалтер, бухгалтер1 і бухгалтер2, прибиральниця.

У ІКС підприємства можна виділити 3 основні категорії користувачів і обслуговуючого персоналу, які мають відповідні повноваження по доступу до інформаційних, програмних і інших ресурсів ІКС підприємства:

- персонал, що управляє;
- системний адміністратор;
- бухгалтерія.

Системний адміністратор - користувач, що володіє правом управління безпекою інформації і настройками мережі.

Персонал, що управляє, - група користувачів, що має повноваження проглядати всі інформаційні ресурси.

Бухгалтерія - група простих користувачів, що мають повноваження роботи з інформаційними ресурсами у сфері бухгалтерії.

1.5 Аналіз існуючої системи захисту інформаційних ресурсів на підприємстві

Для організації системи захисту інформаційних ресурсів на підприємстві реалізовані наступні заходи:

- система контролю доступу на територію підприємства;
- система пожежної сигналізації;

– система охоронної сигналізації;

– система розмежування прав і доступу до інформаційних ресурсів ІКС підприємства;

– система захисту ІКС підприємства при роботі з Internet;

– система зберігання архівних даних.

Система контролю доступу на територію підприємства виконана за допомогою установки на вхідних дверях централі контролю доступу(РС 585). Кожен співробітник підприємства, якому наданий доступ на територію офісу, має ключі до електро-замку. При вході співробітник відкриває двері ключем спрацьовує сигналізація, при успішному наборі паролю звукова сигналізація вимикається.

При вході до кабінету менеджерів (Додаток Б) на стіні біля дверей, а також у тамбурі біля вхідних дверей розташована тривожна кнопка. При виникненні пожежі персонал негайно викликає службу пожежної охорони..

Програмування централі проводять фахівці компанії інформаційної безпеки (ПП «Алмаз»).

Пожежна і охоронна сигналізації запрограмовані від централі РС 585.

Установка охоронної сигналізації в черговий режим проводиться співробітником підприємства, який останній уходить з території офісу.

Зняття з охорони проводиться співробітником підприємства який перший приходить до офісу.

Підприємство не має своєї особистої охорони, тому в неробочий час приміщення офісу здається під охорону охоронному агентству «Левіт».

Система охоронної сигналізації знаходиться в черговому режимі тільки в неробочий час доби і у вихідні дні.

Система охоронної сигналізації складається з ІЧ-датчиків руху (Додаток Б).

Система пожежної сигналізації складається з димових датчиків (Додаток Б).

Підприємство в своєму складі містить 13 співробітників, кожен з яких має своє робоче місце, оснащене ПК. Всі комп'ютери складають ІКС підприємства. Вся інформація, необхідна для виробничого процесу зберігається на сервері баз

даних підприємства. При роботі користувача з даними, відбувається копіювання цих даних на робочу станцію користувача, їх обробка, і, при завершенні роботи користувача, переміщення і збереження цих даних знову на сервері.

Кожна робоча станція має вихід в Internet. Для забезпечення безпечної роботи в Internet ІКС підприємства містить Internet сервер, в якому встановлений програмний брандмауер Windows. На кожній робочій станції і серверах встановлений антивірус ESET NOD32. Кожен користувач ІКС ознайомлений під розписку з правилами роботи з ресурсами Internet мережі і з антивірусною програмою. Оновлення антивірусної програми відбувається у міру оновлення антивірусної бази.

Настройки операційної системи включають ідентифікацію користувача при вході в систему. Тобто користувач при вході в систему натискає комбінацію клавіш Ctrl-alt-del і в діалоговому вікні вводить своє ім'я і пароль. Кожен користувач ІКС підприємства під розписку ознайомлений з правилами складання, використання і зберігання паролів.

Обслуговування ІКС, внесення яких-небудь змін, забезпечення безпеки інформаційних ресурсів є відповідальністю адміністратора. Адміністратор створює і видаляє облікові записи користувачів ІКС, надає права доступу користувачів до ресурсів, необхідних їм для нормальної роботи і забороняє доступ до ресурсів, потребу користувача в яких не обґрунтовано виробничим процесом. До деяких програм, таким як 1с бухгалтерія, всім користувачам, окрім бухгалтерії, надані права тільки на читання.

Користувачам заборонено встановлювати і записувати на робочу станцію програми будь-якого характеру, використання яких не обґрунтовано виробничим процесом.

Наради, в ході яких циркулює конфіденційна інформація підприємства, проходять в конференцзалі (Додаток Б). Кабінет спеціально обладнаний для забезпечення захисту акустичної інформації. Під час нарад віконні отвори кабінету захищені шторами жалюзі з метою запобігання просочуванню

конфіденційної інформації оптико електронним каналом, відключена телефонна станція (запобігання електроакустичному каналу просочування інформації.)

Всі металоконструкції ІКС підприємства заземлені за допомогою занулення до трансформаторної будки.

У кабінеті директора знаходиться сейф для зберігання готівки фірми.

1.6 Аналіз обчислювального середовища інформаційно-комунікаційної системи підприємства

ІКС підприємства – локальна мережа, розташована на території КЗ підприємства. Кожна робоча станція має вихід в Internet. Для забезпечення безпечної роботи в Internet ІКС підприємства містить Internet сервер, в якому встановлений програмний брандмауер Windows. На кожній робочій станції і серверах встановлений антивірус ESET NOD32.

Основні завдання мережі:

- ведення безперервного виробничого процесу;
- обробка і зберігання даних різного характеру;
- організація робочого простору співробітникам;
- перегляд існуючих ресурсів, необхідних для роботи, і можливість створення нових.

Комплекс технічних засобів ІКС підприємства включає засоби обробки даних (10 ПК, сервер баз даних, сервер Internet), засоби обміну даними з можливістю виходу в глобальні мережі (кабельна система, комутатори, модем), а також засоби зберігання (в т.ч. архівації) даних.

Сервер Internet здійснює доступ до зовнішньої мережі Internet.

Сервер баз даних забезпечує зберігання і обробку всієї інформації, циркулюючої на підприємстві. На всіх робочих станціях ІКС встановлена операційна система Windows 10. На серверах ІКС встановлена операційна система Windows 2012 Server.

Об'єкти інформатизації ІКС ТОВ «Інтер-Транзит» включають:

– технологічне устаткування (засоби обчислювальної техніки, мережеве і кабельне устаткування);

– інформаційні ресурси, що містять відомості обмеженого доступу і представлені у вигляді документів або записів на носіях на магнітній, оптичній і іншій основі, інформаційних фізичних полях, і базах даних;

– програмні засоби (операційна система, система управління базами даних, інше загальносистемне і прикладне програмне забезпечення);

– канали зв'язку, по яких передається інформація;

1.7 Розробка моделі порушника

Порушник – це особа, яка виконала спробу виконання заборонених операцій (дій) помилково, незнанню або усвідомлено із злим наміром (з корисливих інтересів) або без такого (ради гри або задоволення, з метою самоствердження і т. п.) і що використовує для цього різні можливості, методи і засоби.

Система захисту ІКС ТОВ «Інтер-Транзит» повинна будуватися виходячи з пропозицій про наступні можливі типи порушників в системі (з урахуванням категорії осіб, мотивації, кваліфікації, наявності спеціальних засобів і ін.):

1. «Недосвідчений (неуважний) користувач» – співробітник підприємства, який може робити спроби виконання заборонених операцій, доступу до захищених ресурсів ІКС з перевищенням своїх повноважень, введення некоректних даних і тому подібні дії помилково, некомпетентності або халатності без злого наміру і що використовує при цьому тільки штатні (доступні йому) апаратні і програмні засоби.

2. «Любитель» – користувач, що намагається подолати систему захисту без корисливих цілей і злого наміру, для самоствердження і інтересу. Для подолання системи захисту і здійснення заборонених дій він може використовувати різні методи отримання додаткових повноважень доступу до ресурсів (імен, паролів інших користувачів), недоліки в побудові системи захисту і доступні йому штатні (встановлені на робочій станції) програми (несанкціоновані дії за допомогою перевищення своїх повноважень на використання дозволених засобів). Крім цього він може намагатися використовувати додатково нештатні інструментальні і

технологічні програмні засоби (відладчики, службові утиліти), самостійно розроблені програми або стандартні додаткові технічні засоби.

3. «Шахрай» – користувач, який може робити спроби виконання незаконних технологічних операцій, введення спотворених даних і тому подібні дії в корисливих цілях, з примусу або із злого наміру, але що використовують при цьому тільки штатні (встановлені на робочій станції і доступні йому) апаратні і програмні засоби від свого імені або від імені іншого співробітника (знаючи його ім'я і пароль, використовуючи його відсутність).

4. «Зовнішній порушник (зловмисник)» – стороння особа, яка може робити спроби незаконного знімання інформації через технічні канали просочування інформації.

5. «Внутрішній порушник (зловмисник)» – співробітник підприємства, що діє цілеспрямовано з корисливих інтересів або мести за нанесену образу. Він може використовувати весь набір методів і засобів злому системи захисту.

Користувачі і обслуговуючий персонал з числа співробітників мають найбільш широкі можливості по здійсненню несанкціонованих дій, унаслідок наявності у них певних повноважень по доступу до ресурсів і хорошого знання технології обробки інформації і захисних мерів. Дії цієї групи осіб безпосередньо пов'язаних з порушенням правил, що діють, і інструкцій.

Звільнені співробітники можуть використовувати для досягнення своїх цілей свої знання про технологію роботи, захисні заходи і права доступу.

Отримані знання і досвід виділяють їх серед інших джерел зовнішніх загроз.

Приймаються наступні обмеження і пропозиції про характер дій можливих порушників:

– робота по підбору кадрів і спеціальні заходи виключають можливість створення коаліцій порушників, тобто об'єднання (змови) і цілеспрямованих дій два і більш за порушників по подоланню системи захисту;

– несанкціоновані дії можуть бути наслідком помилок експлуатуючого і обслуговуючого персоналу, адміністратора безпеки, а також недоліків прийнятої технології обробки і зберігання інформації.

– у своїй протиправній діяльності вірогідний порушник може використовувати будь-який наявний засіб перехоплення інформації, дії на інформацію, адекватні фінансові кошти для підкупу персоналу, шантаж і інші засоби і методи для досягнення цілей, що стоять перед ним.

1.8 Можливі загрози безпеці інформації

Найбільш значущими загрозами безпеці інформації ІКС підприємства є:

– порушення конфіденційності (розголошування, витік) відомостей, що містять конфіденційну інформацію;

– порушення цілісності (спотворення, підміна, знищення інформаційних, програмних і інших ресурсів ІКС, а також фальсифікація документів) конфіденційної інформації;

– порушення доступності (блокування інформації, зрив своєчасного вирішення завдань) конфіденційної інформації.

У таблиці 1.1 приведені основні загрози інформації в ІКС підприємства і основні властивості інформації, які при цьому втрачаються.

У дипломному проекті не розглядаються загрози, викликані технічними каналами просочування інформації. Відповідно до постанови КМУ №373 «Правила забезпечення захисту інформації в інформаційних, телекомунікаційних і інформаційно-телекомунікаційних системах», в системах, де обробляється конфіденційна інформація комерційного характеру, необхідність в захисті інформації від витоку технічними каналами визначається керівником підприємства. Керівником підприємства технічні канали витоку інформації визначені як неістотні загрози конфіденційній інформації підприємства і ухвалено рішення не розглядати їх при побудові системи захисту інформації.

Таблиця 1.1 – Загрози інформації в ІКС підприємства

Можливі загрози інформації	Властивості інформації, які втрачаються		
	Конфіденційність	Цілісність	Доступність
Загрози, обумовлені стихійними джерелами			
Пожежа, землетрус, ураган, потоп, різні непередбачені явища і обставини		+	+

Продовження таблиці 1.1

Можливі загрози інформації	Властивості інформації, які втрачаються		
	Конфіденційність	Цілісність	Доступність
Загрози, обумовлені технічними засобами			
Відмова технічних засобів обробки інформації: – відмова компонентів комп'ютера; – відмова принтера, ксерокса; – відмова серверів ІКС (вихід з ладу жорсткого диска); – відмова компонентів мережі підприємства (комутатор, патч-панель);		+	+
Відмова інженерно-технічних засобів захисту інформації	+		
Відмова в системі енергозабезпечення		+	+
Загрози, обумовлені діями суб'єктів			
Загрози, обумовлені діями суб'єктів, носіїв інформації, даних (читання і несанкціоноване копіювання), даних системи захисту. Незаконне отримання паролів і інших реквізитів розмежування доступу (агентурним шляхом, використовуючи халатність користувачів, шляхом підбору, шляхом імітації інтерфейсу системи програмними закладками) з подальшим маскуванням під зареєстрованого користувача.	+	+	+
Несанкціонована модифікація: ПЗ, даних, даних системи захисту - впровадження програмних «закладок» і «вірусів» («троянських коней» і «жучків»), тобто таких ділянок програм, які не потрібні для здійснення функцій, але дозволяють долати систему захисту, скрито і незаконно здійснювати доступ до ресурсів з метою реєстрації і передачі критичної інформації або дезорганізації функціонування системи.	+	+	+
Знищення: технічних засобів, носіїв інформації, програмного забезпечення, даних, даних системи захисту.		+	+

Продовження таблиці 1.1

Можливі загрози інформації	Властивості інформації, які втрачаються		
	Конфіденційність	Цілісність	Доступність
Порушення нормальної роботи за рахунок вичерпання: – ресурсів процесора; – об'єму вільної оперативної пам'яті; – об'єму вільного дискового простору. Шляхом впровадження і використання неврахованих програм (ігрових, повчальних, технологічних і інших, таких, що немає необхідними для виробничого процесу) з подальшим необґрунтованим витрачанням ресурсів.		+	+
Помилки: при інсталяції програмного забезпечення, при експлуатації програмного забезпечення, при експлуатації технічних засобів. Введення помилкових даних	+	+	+
Загрози, обумовлені роботою користувачів з мережею Internet			
Перехоплення даних при передачі/отриманні	+		+
Модифікація даних при передачі/отриманні	+	+	
Зараження вірусами, «Троєю» через електронну пошту, при перегляді Web- сторінок, при копіюванні файлів		+	+
Переповнювання вільної пам'яті за рахунок спаму.			+

1.9 Висновки. Постановка задачі

На підставі отриманих даних про об'єкт, ІКС підприємства, ступені важливості інформації, що обробляється в інтрамережі підприємства, організації захисту конфіденційної і критичної інформації, можна зробити висновки:

1) ІКС підприємства містить інформаційні ресурси, зміна, крадіжка, розголошування або видалення яких може привести до морального збитку, матеріальних втрат і порушення виробничого процесу.

2) Існуючі методи і засоби захисту інформації, в основному, направлені на запобігання загрозам, які можуть виникнути від зовнішнього порушника. Тому слід розробити систему захисту інформації, яка враховуватиме можливі загрози як від зовнішніх так і від внутрішніх порушників.

Постановка задачі

Для забезпечення безпеки конфіденційної інформації в ІКС ТОВ «Інтер-Транзит» необхідно:

1) створити службу інформаційної безпеки підприємства;

2) розробити захист від НСД в процес функціонування ІКС підприємства сторонніх осіб;

3) розробити права і привілеї кожного зареєстрованого користувача мережі; організувати розмежування доступу зареєстрованих користувачів до апаратних, програмних і інформаційних ресурсів ІКС, тобто захист від несанкціонованого доступу:

– до інформації, циркулюючої в ІКС підприємства;

– до засобів обчислювальної техніки ІКС підприємства;

– до апаратних і програмних засобів захисту, використовуваних в ІКС підприємства;

4) розробити реєстрацію дій користувачів при використанні критичних ресурсів в системних журналах і періодичний контроль коректності дій користувачів системи шляхом аналізу вмісту цих журналів фахівцями підрозділів безпеки;

5) розробити захист від несанкціонованої модифікації і контроль цілісності програмних засобів, а також захист системи від впровадження несанкціонованих програм, включаючи комп'ютерні віруси;

6) розробити механізм оперативного реагування на загрози безпеки інформації;

7) розробити міжмережевий захист, для безпечного користування інтернет ресурсами.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Технічне завдання

2.1.1 Найменування і область застосування

Областю застосування є інформаційно-телекомунікаційна система ТОВ «Інтер-Транзит»

2.1.2 Призначення розробки

Метою роботи є створення системи захисту інформації з детальною розробкою міжмережевого захисту.

2.1.3 Етапи виконання робіт

Етап 1

Обґрунтування актуальності вибраної теми.

Аналіз інформаційно-телекомунікаційної системи ТОВ «Інтер-Транзит».

Виявлення можливих загроз безпеці конфіденційної інформації.

Етап 2

Розробка політики безпеки і технічного завдання на створення системи захисту конфіденційної інформації.

Розробка проектних рішень, що підтримують систему захисту інформації від НСД.

Етап 3

Детальна розробка міжмережевого захисту.

Встановлення та налаштування Comodo Firewall.

2.1.4 Економічний розділ

В даній частині роботи потрібно визначити капітальні витрати на впровадження СЗІ, трудомісткість розробки і реалізації СЗІ. Аналіз економічної ефективності впровадження СЗІ.

2.2 Розробка політики безпеки автоматизованої системи обробки конфіденційної інформації

Для створення системи захисту на підприємстві необхідно розробити політику безпеки.

Письмовий документ про політику безпеки повинен бути доступний всім співробітникам, що відповідають за забезпечення режиму інформаційної безпеки.

Вище керівництво повинне надати задокументовану політику інформаційної безпеки всім підрозділам організації. Цей документ повинен містити наступне:

– визначення інформаційної безпеки, її основні цілі і область її застосування, а також її значення як механізму, що дозволяє колективно використовувати інформацію;

– виклад позиції керівництва по питаннях реалізації цілей і принципів інформаційної безпеки;

– роз'яснення конкретних варіантів політики безпеки, принципів, стандартів і вимог до її дотримання, включаючи:

– виконання правових і договірних вимог;

– вимоги до навчання персоналу правилам безпеки;

– політика попередження і виявлення вірусів;

– політика забезпечення безперебійної роботи організації.

– визначення загальних і конкретних обов'язків по забезпеченню режиму інформаційної безпеки;

– роз'яснення процесу повідомлення про події, що таять загрозу безпеці.

Необхідно розробити процес перевірки, визначити обов'язки і задати дати перевірок для дотримання вимог документа про політику безпеки.

Політика безпеки, що розробляється, застосовна до автоматизованої системи (АС) для обробки конфіденційної інформації, якій необхідний особливий захист (надалі АС, призначена для обробки конфіденційної

інформації, яка потребує особливого захисту, позначатиметься як АС.3).

Відповідальність за забезпечення захисту конфіденційної інформації, яка потребує особливого захисту, покладається на керівника (заступника керівника) підприємства.

Організація і проведення робіт по захисту конфіденційної інформації, яка потребує особливого захисту, повинна проводитися службою інформаційної безпеки, яка визначає вимоги до модернізації системи захисту інформації, виконання робіт по експлуатації і контроль за станом захищеності інформації. Служба інформаційної безпеки повинна створюватися наказом керівника підприємства. Враховуючи штаб співробітників служба інформаційної безпеки повинна складатися з адміністратора інформаційної безпеки, обов'язки якого повинен виконувати адміністратор ІКС підприємства.

Для забезпечення безпечного створення, обробки і зберігання конфіденційної інформації, яка потребує особливого захисту, на підприємстві необхідно виконати локалізацію такої інформації.

Під час обробки конфіденційної інформації в АС повинен забезпечуватися її захист від несанкціонованого і неконтрольованого ознайомлення, модифікації, знищення, копіювання і розповсюдження.

Об'єкти доступу

Текстові документи, представлені в електронному вигляді і на паперових носіях, які містять конфіденційну інформацію критичного характеру.

Технічні засоби (персональний комп'ютер, принтер, ксерокс, знімний жорсткий диск, дисковод для знімних дисків), зокрема засоби захисту;

Програмне забезпечення ПК

Резервні копії конфіденційної інформації;

Атрибути доступу

Об'єктів доступу:

Атрибутом доступу текстового документа є його рівень доступу, який відповідає характеру конфіденційної інформації, що зберігається в документі: бухгалтерська інформація і інформація виробничого характеру.

Користувачів:

Атрибутом доступу користувача є його роль (звичайний користувач, адміністратор інформаційної безпеки або системний адміністратор) і група, до якої відноситься користувач.

Види доступу

КЗЗ повинен підтримувати такі види доступу до текстових документів: читання, запис, видалення, друк, експорт, імпорт.

Для даних захисту необхідно передбачити такі види доступу: читання і запис.

Правила розмежування доступу

Правила розмежування доступу до текстових документів

Необхідно забезпечити виконання наступних умов:

– Користувач отримує доступ до текстового документа, якщо він виконує роль звичайного користувача і його рівень допуску співпадає з рівнем допуску текстового документа.

– Система повинна забезпечити доступ користувачів тільки до тих даних, які необхідні їм за родом діяльності.

– Користувачі АС повинні мати відповідним чином оформлені допуски до відомостей, що містять конфіденційну інформацію. Допуск до АС повинен оформлятися наказом керівника підприємства з відома служби інформаційної безпеки підприємства

– Доступ до конфіденційної інформації повинен надаватися тільки ідентифікованим і аутентифікованим користувачам. Спроби доступу до такої інформації неідентифікованих персон або користувачів з непідтвердженою під час автентифікації відповідності пред'явленого ідентифікатора повинні блокуватися.

– У випадку, якщо користувачеві за родом діяльності необхідний доступ до заборонених йому ресурсів, він може оформити тимчасовий доступ наказом керівника підприємства після згоди адміністратора інформаційної безпеки.

– Адміністратор інформаційної безпеки повинен регулярно проводити перевірку прав користувачів.

– Реалізація функції копіювання конфіденційної інформації в електронному вигляді на знімні носії інформації повинна проводитися тільки адміністратором інформаційної безпеки підприємства. Цей процес повинен контролюватися шляхом реєстрації в системному журналі імені користувача, об'єкту копіювання, часу копіювання.

– Копіювання конфіденційної інформації, представленої в текстовому вигляді повинно проводитися тільки на копіювальному апараті АС. Цей процес повинен виконуватися адміністратором інформаційної безпеки. Адміністратор інформаційної безпеки повинен зареєструвати процес копіювання в журнал подій: ім'я користувача, об'єкт копіювання, час копіювання.

– Видалення конфіденційної інформації, представленої в електронному і паперовому вигляді, може виконувати тільки адміністратор інформаційної безпеки після дозволу директора підприємства.

Правила розмежування доступу до даних захисту

– Права на читання і запис даних і право на проглядання системного журналу безпеки повинен мати тільки користувач з роллю адміністратора безпеки.

– Право на читання і зміни значень параметрів конфігурації КЗЗ, а також права на читання і зміни значень інших параметрів конфігурації КЗЗ, права на читання даних про поточну поведінку КЗЗ і право на оперативне керівництво КЗЗ повинен мати тільки користувач з роллю адміністратора безпеки.

Правила розмежування доступу до резервних копій конфіденційної інформації:

– Право на створення резервних копій, видалення і використання повинен мати тільки адміністратор інформаційної безпеки.

Правила адміністрування системи захисту інформації

– Ведення переліку користувачів і їх атрибути доступу виконує адміністратор інформаційної безпеки.

– Адміністратор інформаційної безпеки повинен створити для кожного користувача АС обліковий запис з наданням ним відповідних прав і дозволів відповідно до групи і ролі користувача.

– Внесення змін до атрибутів доступу до об'єктів доступу виконує адміністратор інформаційної безпеки.

– Установку і оновлення всіх програмних засобів виконує системний адміністратор.

– Для надійності збереження конфіденційної інформації адміністратор інформаційної безпеки повинен щодня в кінці робочого дня виконувати резервне копіювання інформації. Резервні диски повинні зберігатися в сейфі служби інформаційної безпеки підприємства.

– Цілісність і достовірність архівної інформації перевіряється адміністратором інформаційної безпеки.

– Всі користувачі АС повинні бути навчені правилам роботи в АС.

Реєстрація дій користувача:

– КЗЗ повинен вести системний журнал захисту.

– Облік подій повинен проводитися автоматично, а зареєстровані дані повинні бути захищені від модифікації і знищення користувачами, які не мають повноважень адміністратора інформаційної безпеки.

– Засоби реєстрації повинні забезпечувати запис в системний журнал безпеки таких подій: результи ідентифікації і автентифікації користувачів, результати виконання користувачами операцій по обробці даних (резервному копіюванні, друку, зміні інформації, спробах видалення інформації).

– Необхідно регулярно проводити перевірку вмісту системного журналу безпеки.

– Адміністратор інформаційної безпеки повинен реєструвати інформацію про сеанс роботи користувача в АС з конфіденційною

інформацією, представленою на паперовому носієві (ім'я користувача, час тривалості роботи, об'єкт обробки) в журналі подій.

– Інформація про друк і копіювання даних, створення резервних копій, видаленні резервної інформації із знімних носіїв по закінченню терміну зберігання, зберіганні конфіденційної інформації, повинна фіксуватися в журналі подій.

– Записи в журнал подій повинен проводити тільки адміністратор інформаційної безпеки. Журнал подій повинен зберігатися в сейфі служби інформаційної безпеки підприємства.

Правила захисту фізичного середовища АС від несанкціонованого доступу до об'єктів доступу:

– Система захисту фізичного середовища АС повинна складатися з:

  – системи пожежної сигналізації;

  – системи охоронної сигналізації;

  – системи контролю доступу.

– На підприємстві повинна бути організована охорона всього фізичного середовища підприємства і фізичного середовища АС зокрема в неробочий час доби і у вихідні дні.

– Установку і програмування систем пожежної і охоронної сигналізацій повинна проводити фірма, яка має ліцензію або дозвіл на право проведення такого виду робіт.

– Система охоронної сигналізації повинна забезпечувати захист фізичного простору АС від можливого несанкціонованого проникнення зловмисника.

– Система пожежної сигналізації повинна забезпечити захист фізичного простору від можливого виникнення пожежі шляхом сповіщення про спалах.

– Система контролю доступу повинна забезпечувати неможливість несанкціонованого проникнення осіб на територію АС в робочий і неробочий час.

2.3 Розробка технічного завдання на створення системи захисту конфіденційної інформації

Загальні відомості

Розробка системи захисту конфіденційної інформації виконується для автоматизованої системи (АС.3), призначеної для обробки конфіденційної інформації, яка потребує особливого захисту, для «ТОВ «Інтер-Транзит»».

Результатом роботи повинна бути система захисту інформації, яка забезпечить можливість створення, обробки і зберігання конфіденційної інформації, представленої в електронному вигляді і текстових документів.

Призначення і мета створення системи захисту інформації

АС призначена для обробки конфіденційної інформації, представленої в електронному вигляді і на паперових носіях. Метою створення СЗІ є забезпечення захисту цієї інформації.

У АС надаються особливі вимоги до конфіденційності, цілісності і доступності інформації. Відповідно із специфікаціями, приведеними в документі НД ТЗІ 2.5-004-99 «Критеріїв оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу», комплекс засобів захисту (КЗЗ) повинен надавати такі послуги безпеки:

- базова довірча конфіденційність – КД-2;
- повторне використання об'єктів – КО-1;
- мінімальна конфіденційність при обміні – КВ-2;
- мінімальна довірча цілісність – ЦД-1;
- обмежений відкат – ЦО-1;
- мінімальна цілісність при обміні – ЦВ-2;
- квоти – ДР-1;
- модернізація – ДЗ-1;
- ручне відновлення – ДВ-1;

- захищений журнал – НР-2;
- одиночна ідентифікація і автентифікація – НИ-2 ;
- однонаправлений достовірний канал – НК-1;
- виділення адміністратора – НО-2;
- СЗІ з контролем цілісності – НЦ-1;
- автентифікація вузла – НВ-1;
- базова автентифікація відправника – НА-1;
- самотестування при старті – НП-1.

Процес розробки КЗЗ повинен відповідати рівню гарантій Г-2 (відповідні вимоги приведені в документі НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу»).

СЗІ розробляється відповідно до вимог, які визначені в таких законодавчих і нормативних документах: НД ТЗІ 1.4-001-00 «Типове положення про службу захисту інформації в автоматизованій системі»

Характеристика автоматизованої системи і умов її функціонування

Характеристика фізичного середовища

Технічні засоби АС розміщені в межах контрольованої зони. Приміщення облаштоване електромеханічним замком, системами пожежної і охоронної сигналізацій. Система пожежної сигналізації виконана з димових датчиків. Система охоронної сигналізації виконана з ІЧ-датчиків руху, магнітоконтактного датчика відкриття дверей.

Характеристика обчислювальної системи:

– АС складається з 10 робочих станцій, 2 принтерів, 1 ксерокса та 1 сканера.

Відповідно до документа НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» АС відноситься до АС класу 3.

– На всіх робочих станціях необхідно встановити операційну систему Microsoft Windows 10 і таке програмне забезпечення: антивірус ESET NOD32, Microsoft Office 2016, брандмауер Comodo Firewall, а додатково на робочій станції в бухгалтерії встановити 1С Бухгалтерію.

Характеристика користувачів

В процесі функціонування АС, користувачі, які мають доступ до АС, діляться на наступні категорії:

– звичайні користувачі – користувачі, які мають деякі повноваження доступу до конфіденційної інформації критичного характеру;

– користувачі, які забезпечують функціонування АС, адміністрування операційної системи;

– працівники служби інформаційної безпеки, які забезпечують функціонування СЗІ;

– технічний персонал.

Характеристика інформації

У АС обробляється конфіденційна інформація, представлена в електронному вигляді і на паперових носіях. Інформація, представлена в електронному вигляді зберігається на сервері компанії, а конфіденційна інформація представлена в паперовому вигляді знаходиться в сейфі директора, окрім бухгалтерської. Інформація бухгалтерського характеру зберігається в сейфі бухгалтерії.

Характеристика технології обробки інформації

– Конфіденційна інформація, представлена в електронному вигляді зберігається на сервері компанії. Кожен користувач має доступу до інформації, відповідної його правам і повноваженням.

– Конфіденційна інформація, представлена на паперових носіях зберігається в сейфі директора підприємства. Користувачі мають доступ до тих паперових документів, на які у них оформлені права і повноваження.

– Створення документа проводиться шляхом створення нового документа або імпорту того, що існує. Імпорт документа може проводитися з носіїв інформації адміністратором інформаційної безпеки.

– Документ може бути експортований на дискету або інший носій, надрукований або скопійований. Друк, копіювання і експорт інформації проводиться тільки адміністратором інформаційної безпеки.

– Видалення інформації проводиться тільки адміністратором інформаційної безпеки.

Можливі загрози інформації

– Умови функціонування АС, які впливають на безпеку інформації, визначають можливі загрози інформації. Вони розрізняються по дії на захищеність інформації, тобто на її конфіденційність, цілісність і доступність. У таблиці 2.1 приведені основні загрози інформації в АС і основні властивості інформації, які при цьому втрачаються.

Таблиця 2.2 – Загрози інформації в АС

Можливі загрози інформації	Властивості інформації, які втрачаються		
	Конфіденційність	Цілісність	Доступність
Загрози, обумовлені стихійними джерелами			
Пожежа, землетрус, ураган, потоп, різні непередбачені явища і обставини		+	+
Загрози, обумовлені технічними засобами			
Відмова технічних засобів обробки інформації: – відмова компонентів комп'ютера; – відмова принтера, ксерокса;		+	+
Відмова інженерно-технічних засобів захисту інформації	+		
Відмова в системі енергозабезпечення		+	+
Загрози, обумовлені діями суб'єктів			
Крадіжка: технічних засобів, носіїв інформації, даних (читання і несанкціоноване копіювання), даних системи захисту.	+	+	+
Підміна (модифікація): програмних засобів, даних, даних системи захисту.	+	+	+
Знищення: технічних засобів, носіїв інформації, програмного забезпечення, даних, даних системи захисту.		+	+
Помилки: при інсталяції програмного	+	+	+

забезпечення, при експлуатації програмного забезпечення, при експлуатації технічних засобів			

Вимоги до системи захисту конфіденційної інформації

Організаційне забезпечення захисту

– З метою забезпечення безпечної обробки конфіденційної інформації в АС указом керівника створюється служба інформаційної безпеки в АС, якою надаються повноваження організації і впровадження СЗІ, контроль за станом захищеності інформації. Служба інформаційної безпеки повинна складатися з адміністратора інформаційної безпеки, обов'язки якого повинен виконувати системний адміністратор.

– Відповідно до рівня повноважень доступу до конфіденційної інформації, характеру робіт, які виконуються в процесі функціонування АС для користувачів АС визначаються такі ролі:

Звичайний користувач – користувач, який працює з текстовими документами

Адміністратор безпеки – користувач, який забезпечує безпеку конфіденційної інформації, що обробляється в АС.

Системний адміністратор – користувач, який забезпечує функціонування АС.

Кожну роль може виконувати один або декілька користувачів.

Окрім цього, роботу АС забезпечує технічний персонал.

Групи користувачів:

Системний адміністратор – користувач, який виконує роль системного адміністратора;

Адміністратор безпеки – користувач, який виконує роль адміністратора безпеки;

Управляючий персонал – користувачі, які виконують роль звичайного користувача і мають доступ до всієї інформації;

Бухгалтерія – користувачі, які виконують роль звичайного користувача і мають доступ до бухгалтерської інформації.

Співробітники підприємства – користувачі, які виконують роль звичайного користувача і мають доступ до інформації, необхідної їм по руду діяльності.

Технічний персонал, обслуговуючий приміщення, в якому знаходяться технічні засоби АС, не мають права доступу до інформації.

– Користувачі АС повинні мати відповідним чином оформлені допуски до відомостей, що містять конфіденційну інформацію.

Вимоги до системи захисту інформації в комп'ютерній системі АС.3 від несанкціонованого доступу

Вимоги до послуг безпеки

– Довірча конфіденційність

КЗЗ повинен реалізовувати рівень КД-2 – Базова довірча конфіденційність.

Послуга застосовується до таких об'єктів доступу: текстові документи, дані захисту, програмні засоби КЗЗ.

Доступ до текстових документів:

– КЗЗ повинен надавати звичайним користувачам можливість працювати з документами тільки за допомогою призначеного для цього процесу.

– КЗЗ повинен надавати доступ до документів на підставі атрибутів доступу користувача і документа.

– КЗЗ повинен надавати можливість зміни прав доступу користувачів до об'єкту тільки адміністраторові інформаційної безпеки.

– Атрибути доступу документа повинні встановлюватися у момент створення документа.

– При виконанні друку або експорту текстових документів адміністратор інформаційної безпеки контролює відповідність атрибутів доступу документа і носія.

Доступ до програмних засобів СЗІ:

– КЗЗ повинен надавати доступ до процесів, за допомогою яких обробляється конфіденційна інформація, тільки користувачам АС.

– КЗЗ повинен надавати доступ до процесів, за допомогою яких виконується ведення бази даних захисту і проглядання системного журналу безпеки, тільки адміністраторові інформаційної безпеки.

– КЗЗ повинен надавати можливість змінювати атрибути доступу файлів тільки адміністраторові інформаційної безпеки.

Доступ до даних захисту:

– КЗЗ повинен надавати можливість роботи даними захисту тільки за допомогою призначеного для цього процесу;

– КЗЗ повинен реалізовувати правила розмежування доступу даним захисту.

Повторне використання об'єктів

КЗЗ повинен реалізувати рівень КО-1 – повторне використання об'єктів.

– Політика повторного використання об'єкту, яка реалізується КЗЗ, відноситься до всіх об'єктів КС.

– Перш ніж користувач або процес може отримати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, встановлені для попереднього користувача або процесу має рацію до даного об'єкту повинні бути відмінені.

– Перш ніж користувач або процес може отримати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, вся інформація, яка містилася в даному об'єкті, повинна стати недосяжною.

– Конфіденційність при обміні

КЗЗ повинен реалізувати рівень КВ-2 – базова конфіденційність при обміні.

КЗЗ повинен забезпечувати захист від безпосереднього ознайомлення з інформацією, що міститься в об'єкті, який передається.

Послуга конфіденційність при обміні дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що в них міститься, під час їх експорту/імпорту через незахищене середовище. Найчастіше дана послуга реалізується з використанням криптографічних перетворень. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування. Під повнотою захисту в даному випадку розуміють множину типів загроз, від яких забезпечується захист. Під ступенем захищеності об'єктів, що експортуються, як правило, розуміють криптостійкість використовуваних алгоритмів шифрування.

Так, реалізація даної послуги на рівні КВ-2 забезпечує захист від несанкціонованого ознайомлення за рахунок пасивного спостереження за лініями зв'язку або розкрадання носіїв інформації. Прикладом реалізації може служити програмне шифрування файлів перед їх передачею каналами зв'язку або прозоре шифрування файлів перед їх записуванням на диск. Запити на призначення або зміну рівня захищеності повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження.

– Довірча цілісність

КСЗ повинен реалізовувати рівень ЦД-1 – мінімальна довірча цілісність.

Послуга застосовується до таких об'єктів доступу: текстові документи, дані захисту, програмні засоби КЗЗ.

Доступ до текстових документів:

– КЗЗ повинен надавати доступ до документів на підставі атрибутів доступу користувача і документа відповідно до правил розмежування доступу.

– КЗЗ повинен надавати можливість зміни прав доступу користувачів до об'єкту тільки адміністраторові інформаційної безпеки.

Доступ до програмних засобів СЗІ

– КЗЗ повинен надавати доступ до процесів, за допомогою яких обробляється конфіденційна інформація, тільки користувачам АС.

– КЗЗ повинен надавати доступ до процесів, за допомогою яких виконується ведення бази даних захисту і проглядання системного журналу безпеки, тільки адміністраторові інформаційної безпеки і системному адміністраторові.

– КЗЗ повинен надавати можливість змінювати атрибути доступу файлів тільки адміністраторові інформаційної безпеки.

Доступ до даних захисту:

– КЗЗ повинен реалізовувати правила розмежування доступу даним захисту;

– Відкат

КЗЗ повинен реалізовувати рівень ЦО-1 – обмежений відкат.

Відкат повинен виконуватися для таких об'єктів доступу: текстові документи, дані захисту, програмні засоби КЗЗ.

– Відкат може проводитися у випадку видалення або модифікації об'єкту доступу.

– КЗЗ повинен забезпечувати можливість адміністраторові інформаційної безпеки відкоту дій за допомогою автоматизованих засобів.

– КЗЗ повинен забезпечити фіксацію відкоту в системному журналі безпеки.

– Цілісність при обміні

КЗЗ повинен реалізовувати рівень ЦВ-2 – базова цілісність при обміні.

КЗЗ повинен забезпечувати можливість виявлення порушення цілісності інформації, що міститься в об'єкті, який передається, а також фактів його видалення або дублювання.

Дана послуга дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Найчастіше ця послуга реалізується з використанням таких механізмів криптографічного захисту, як цифровий підпис і коди автентифікації повідомлень. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування. Під повнотою захисту, як і для

послуги конфіденційність при обміні, треба розуміти множину типів загроз, від яких забезпечується захист. Під ступенем захищеності об'єктів, що експортуються, як правило, слід розуміти криптостійкість використовуваних алгоритмів шифрування.

Рівень ЦВ-2 даної послуги забезпечує базовий захист. Запити на присвоєння або зміну рівня захищеності повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження.

– Використання ресурсів

КЗЗ повинен реалізовувати рівень ДР-1 – квоти.

– Всі об'єкти, що захищаються, повинні ідентифікуватися і контролюватися диспетчером доступу шляхом накладення обмежень на максимальний об'єм даного ресурсу, який може бути виділений користувачеві.

– Гаряча заміна

КЗЗ повинен реалізовувати рівень ДЗ-1 – модернізація.

– Модернізацію або заміну окремих компонентів комп'ютерної системи може виконувати тільки системний адміністратор.

– Модернізація комп'ютерної системи повинна виконуватися у разі

порушення умов функціонування системи в цілому або окремих її компонентів.

– Відновлення після збоїв

КЗЗ повинен реалізовувати рівень ДВ-1 – ручне відновлення.

– У системі необхідно передбачити певний порядок обробки помилок (збійних ситуацій), які з'являються під час роботи системи. Програмні засоби повинні надати адміністраторові можливість вказати системі, яким чином вона повинна реагувати на помилку.

– Повинні бути присутніми ручні процедури, за допомогою яких системний адміністратор зможе безпечним чином повернути КС до нормального функціонування.

– Реєстрація (аудит)

КЗЗ повинен реалізовувати рівень НР-2 – захищений журнал.

– Для реєстрації подій в СЗІ слід передбачити журнал безпеки, який повинен бути захищений від несанкціонованого ознайомлення, модифікації і знищення.

– Всі записи про події повинні містити інформацію про дату, час і тип події, а для подій аудиту – також про користувача, процес і об'єкт, пов'язані з подією.

– Ідентифікація і автентифікація

КЗЗ повинен не реалізовувати рівень НИ-2 – одиночна ідентифікація і автентифікація.

– Кожен користувач повинен однозначно ідентифікуватися КСЗ на підставі свого імені.

– Перш ніж дозволити якому-небудь користувачеві виконувати які-небудь контрольовані КЗЗ дії, КЗЗ винен автентифіціювати цього користувача на підставі введеного ним пароля.

– Введення імені і пароля повинне проводитися з клавіатури. КСЗ повинен забезпечити захист даних автентифікації від несанкціонованого ознайомлення, модифікації і руйнування.

– Достовірний канал

КЗЗ повинен реалізовувати рівень НК-1 (однонаправлений достовірний канал).

– КЗЗ гарантує, що користувач взаємодіє безпосередньо з КЗЗ і ніякою інший користувач або процес не може втрутитися у взаємодію

– Достовірний канал використовується для початкової ідентифікації і аутентифікації користувача (для введення імені і пароля). Достовірний канал встановлюється з ініціативи користувача. Для зв'язку між користувачем і КЗЗ використовується клавіатура.

– Розподіл обов'язків

КСЗ повинен реалізовувати рівень НО-2 – виділення адміністратора.

– У АС слід визначити 3 ролі користувачів:

Звичайний користувач;

Адміністратор інформаційної безпеки;

Системний адміністратор.

– Політика розподілу обов'язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та іншого адміністратора. Функції, притаманні кожній із ролей, повинні бути мінімізовані так, щоб включати тільки ті функції, які необхідні для виконання даної ролі.

– Користувач повинен мати можливість виступати в певній ролі тільки після того, як він виконає певні дії, що підтверджують прийняття їм цієї ролі

– Цілісність комплексу засобів захисту

КЗЗ повинен реалізовувати рівень НЦ-1 – КЗЗ з контролем цілісності.

– КЗЗ повинен перевіряти цілісність таких об'єктів: програмні компоненти КЗЗ, параметри і розділи системного реєстру, в яких зберігаються важливі для захисту дані, завантажувальні сектори жорстких дисків.

– У разі виявлення порушень КЗЗ повинен зареєструвати в журналі відповідну подію.

– Можливість повернути КЗЗ в робочий стан повинні мати тільки адміністратори.

– Всі помилки, які виникають під час перевірки цілісності, необхідно вважати порушенням цілісності.

– Відновлення програмних засобів КЗЗ повинне проводитися системним адміністратором.

– Самотестування

КЗЗ повинен реалізовувати рівень НТ-2 – самотестування при старті.

– КЗЗ виконує перевірку і на підставі цього гарантує правильність функціонування і цілісність деякого набору функцій КС.

– Ідентифікація і автентифікація при обміні

КЗЗ повинен реалізовувати рівень НВ-1 – автентифікація вузла.

КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, повинен ідентифікувати і автентифікувати цей КЗЗ с використанням захищеного механізму.

Ця послуга дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію. Рівні даної послуги ранжируються на підставі повноти реалізації.

Реалізація рівня НВ-1 даної послуги дозволяє виключити можливість несанкціонованого зовнішнього підключення і є необхідною умовою для реалізації високих рівнів послуг конфіденційності і цілісності при обміні.

– Автентифікація відправника

КЗЗ повинен реалізовувати рівень НА-1 – базова автентифікація відправника.

Політика автентифікації відправника, що реалізується КЗЗ, повинна визначати множину властивостей і атрибутів об'єкта, що передається, користувача-відправника і інтерфейсного процесу, а також процедури, які дозволяли б однозначно встановити, що даний об'єкт був відправлений (створений) певним користувачем.

Встановлення належності має виконуватися на підставі затвердженого протоколу автентифікації.

– Автентифікація отримувача

КЗЗ повинен реалізовувати рівень НП-1 – базова автентифікація отримувача.

Ця послуга дає можливість забезпечити захист від відмови одержання і дозволяє однозначно встановити факт одержання певного об'єкта певним користувачем. Рівні даної послуги ранжируються на підставі можливості підтвердження результатів перевірки незалежною третьою стороною.

Політика автентифікації одержувача, що реалізується КЗЗ, повинна визначати множину властивостей і атрибутів об'єкта, що передається, користувача-одержувача і інтерфейсного процесу, а також процедури, які

дозволяли б однозначно встановити, що даний об'єкт був одержаний певним користувачем.

Встановлення одержувача має виконуватися на підставі затвердженого протоколу автентифікації

Відповідно до НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» вимоги до функціонального складу КЗЗ 3.КЦД.І={КД-2, КО-1, КВ-2, ЦД-1, ЦО-1, ЦВ-2, ДР-1, ДЗ-1, ДВ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-1, НТ-2, НВ-1, НА-1, НП-1}

– Керованість КЗЗ

– Для проведення різних видів робіт необхідно передбачати декілька станів КЗЗ: робочий стан для нормальної роботи і деякі службові стани. Правом переведення КЗЗ з одного полягання в іншій повинні володіти тільки адміністратор інформаційної безпеки або системний адміністратор.

– КЗЗ повинен надавати звичайним користувачам можливість роботи АС тільки під час перебування КЗЗ в робочому стані.

– Засоби адміністрування КЗЗ повинні забезпечувати: ведення переліку користувачів АС, тобто введення, видалення користувачів і встановлення їх атрибутів доступу; настройка параметрів роботи КЗЗ; оперативне управління КЗЗ.

Вимоги до гарантій реалізації

Процес реалізації повинен відповідати рівню гарантій Г-2 відповідно до НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу»

Приведені послуги безпеки реалізуються за допомогою програмного забезпечення. Програмне забезпечення КЗЗ складається з таких частин:

– засоби захисту операційної системи;

– функціональне ПЗ (антивірусні програми);

– спеціальне ПЗ (програмні засоби, призначені для вирішення спеціальних завдань захисту в АС).

Операційна система і програмне забезпечення повинні бути ліцензійними. В якості спеціального ПЗ повинні використовуватися програмні засоби з гарантією реалізації на рівні Г-2 (відповідні вимоги приведені в документі НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу»).

Архітектура

Спеціальне ПЗ повинно містити в своєму складі наступні компоненти:

– сервер безпеки, який виконує функції ядра КЗЗ, запускається автоматично під час завантаження ОС і працює у власному домені;

– адміністративні утиліти – програмні засоби, призначені для адміністрування КЗЗ, роботи з журналом безпеки і оперативного управління КЗЗ;

– засоби захисту документів.

Середовище функціонування

– Необхідно надати засоби інсталяції, генерації і запуску КС, які гарантують, що експлуатація КС починається з безпечного стану; перелік всіх можливих параметрів конфігурації, які можуть використовуватися в процесі інсталяції, генерації і запуску.

– Повинна існувати система технічних, організаційних і фізичних засобів безпеки, яка гарантує, що програмне і програмно-апаратне забезпечення КЗЗ, яке надається, точно відповідає еталонній копії.

Випробування КЗЗ

– Необхідно скласти програму і методику випробувань, процедури випробувань всіх механізмів, які реалізують послуги безпеки;

– Необхідно надати докази тестування у вигляді детального переліку результатів тестів і відповідно процедур тестування, з тим, щоб отримані результати могли бути перевірені шляхом повторного тестування;

– Необхідно усунути або нейтралізувати всі знайдені «слабкі місця» і провести повторне тестування КЗЗ для підтвердження того, що виявлені недоліки були усунені і не з'являться нові «слабкі місця».

2.4 Проектні рішення

2.4.1 Організація обробки і зберігання конфіденційної інформації в автоматизованій системі

Для створення служби безпеки підприємства наказом директора прийнято рішення взяти штатного системного адміністратора, який буде об’єднувати дві ролі: роль адміністратора інформаційної безпеки та роль системного адміністратора. А з часом, при розширені штабу підприємства рекомендовано створити окрему посаду адміністратора безпеки.

В якості програмного забезпечення використовується тільке ліцензійне програмне забезпечення. Дані наведені у таблиці 2.4.1.

Таблиця 2.3 – Програмне забезпечення

Операційна система на робочих станціях	Microsoft Windows 10
Операційна система на сервері	Windows Server 2012
Антивірусна програма для робочих станцій	ESET NOD32
Антивірусна програма для сервера	ESET NOD32 Smart Security Business Edition
Офісні програми	Microsoft Office 2016 WinRAR 1С Бухгалтерія
Брандмауер	Comodo Firewall

2.4.2 Організація процесу роботи з конфіденційною інформацією

Настройки операційної системи включають ідентифікацію користувача при вході в систему. Тобто користувач при вході в систему натискає комбінацію клавіш Ctrl-alt-del і в діалоговому вікні вводить своє ім'я і пароль. Кожен користувач ІКС підприємства під розписку ознайомлений з правилами складання, використання і зберігання паролів.

Обслуговування ІКС, внесення яких-небудь змін, забезпечення безпеки інформаційних ресурсів є відповідальністю адміністратора. Адміністратор створює і видаляє облікові записи користувачів ІКС, надає права доступу користувачів до ресурсів, необхідних їм для нормальної роботи і забороняє доступ до ресурсів, потребу користувача в яких не обґрунтовано виробничим

процесом. До деяких програм, таких як 1с бухгалтерія, всім користувачам, окрім бухгалтерії, надані права тільки на читання.

Користувачам заборонено встановлювати і записувати на робочу станцію програми будь-якого характеру, використання яких не обґрунтовано виробничим процесом.

Створено два журнали: журнал подій та журнал обліку носіїв конфіденційної інформації.

АС.3 фіксує в журналі подій копіювання, зміну, збереження та видалення даних. Копіювання, видалення та будь-яка зміна конфіденційної інформації проводиться тільки з відома або в присутності адміністратора.

Вся конфіденційна інформація представлена в електронному вигляді зберігається на сервері підприємства.

Адміністратор зобов’язаний регулярно перевіряти журнал подій. В кінці кожного тижня адміністратор проводить резервне копіювання даних.

Всі носії конфіденційної інформації повинні бути промаркеровані та зберігатися у сейфі (їх облік ведеться в журналі обліку носіїв конфіденційної інформації.).

Для організації антивірусного захисту використовується антивірус ESET NOD32 на робочих станціях та ESET NOD32 Smart Security Business Edition на сервері.

2.4.3 Організація доступу персоналу до конфіденційної інформації

У ІКС підприємства можна виділити 3 основні категорії користувачів і обслуговуючого персоналу, які мають відповідні повноваження по доступу до інформаційних, програмних і інших ресурсів ІКС підприємства:

- управляючий персонал;
- системний адміністратор;
- бухгалтерія.

Кожній категорії користувача відведені окремі права доступу.

Управляючий персонал, - група користувачів, що має право на перегляд всіх інформаційних ресурсів.

Системний адміністратор - користувач, що виконує обов’язки по управлінню безпекою інформації і настройками мережі.

Бухгалтерія - група простих користувачів, що мають право роботи з інформаційними ресурсами у сфері бухгалтерії.

Системний адміністратор має право доступу до інформації, яка зберігається на сервері.

Управляючий персонал має право на запис, видалення, зміну, копіювання всієї інформації окрім бухгалтерської.

Бухгалтерія має право на запис, видалення, зміну, копіювання інформації бухгалтерського характеру.

За кожним користувачем закріплена робоча станція. Інформація конфіденційного характеру не зберігається на робочих станціях. На робочих станціях може зберігатися відкрита інформація та інформація особистого характеру.

Всі робочі станції мають вихід в глобальну мережу Інтернет. Налаштування брандмауера забезпечують блокування доступу до сайтів, що містять ігрові та розважальні ресурси.

Інтернет використовується для забезпечення виробничого процесу.

Режим роботи:

- Організована 5-ти денний робочий тиждень
- Робочий день з 9.00 до 18.00
- Перерва з 12.30 до 13.00
- Вихідні дні: суббота та неділя
- Прибирання проводиться 2 рази на тиждень з 17.00 до 18.00

2.4.4 Сейфи

На підприємстві використовується два сейфи. Сейф №1 знаходиться в кабінеті директора і має дві секції. До сейфу мають доступ: директор та адміністратор безпеки. Директор має право доступу до обох секцій сейфу, а адміністратор тільки до секції, де зберігаються носії конфіденційної інформації

та журнал обліку носіїв конфіденційної інформації. Сейф №2 знаходиться в кабінеті бухгалтерії, до нього має право доступу лише головний бухгалтер.

Сейфи зачиняються на ключ та опечатуються особистою печаткою користувачів, які мають право доступу до сейфів.

2.4.5 Установка та налаштування міжмережевого екрану

Брандмауер – програма, що виконує функції захисного екрану між ПК і мережею Інтернет. Блокує шкідливі підключення ззовні до персонального комп'ютера, перешкоджаючи таким чином, просочуванню конфіденційної інформації. Брандмауер надає повний контроль над всією мережевою активністю і автоматично запобігає відомим типам атак.

Міжмережеві екрани (firewall, брандмауер) роблять можливою фільтрацію вхідного і вихідного трафіку, що йде через систему. Міжмережевий екран використовує одне або більше «правило» для перевірки мережевих пакетів при їх вході або виході через мережеве з'єднання, він або дозволяє проходження трафіку або блокує його. Правила міжмережевого екрану можуть перевіряти одну або декілька характеристик пакетів, включаючи але не обмежуючись типом протоколу, адресою хоста джерела або призначення і портом джерела або призначення.

Міжмережеві екрани можуть серйозно підвищити рівень безпеки хоста або мережі. Вони можуть бути використані для виконання одного або декількох завдань:

– для захисту і ізоляції додатків, сервісів і машин у внутрішній мережі від небажаного трафіку, що приходить із зовнішньої мережі інтернет;

– для обмеження або заборони доступу хостов внутрішньої мережі до сервісів зовнішньої мережі Інтернет;

– для підтримки перетворення мережевих адрес.

Для заданих умов функціонування КСЗІ були розроблені параметри, приведені в таблиці 2.4

Таблиця 2.4 – Параметри для АС класу 3

№ п/п	Назва параметру	АС класу 3
1	Захистити всі мережеві підключення	Включено
2	Не дозволяти виключення	Не рекомендується
3	Задати виключення для програм	Рекомендується
4	Дозволяти локальні виключення для программ	Включено

Продовження таблиці 2.4

№ п/п	Назва параметру	АС класу 3
5	Відстежувати DLL- впровадження	Включено
6	Відстежувати повідомлення Windows	Рекомендується
7	Відстежувати COM/OLE автоматизацію	Рекомендується
8	Відстежувати DNS-запити	Включено
9	Відстежувати витік батьківських додатків	Включено
10	Відстежувати зміни пам’яті іншими процесами	Включено
11	Дозволяти виключення для віддаленого управління	Відключено
12	Дозволяти виключення для загального доступу до файлів та принтерів	Відключено
13	Дозволяти виключення ICMP	Не рекомендується
14	Дозволяти виключення для віддаленого робочого столу	Рекомендується
15	Дозволяти виключення для UPnP – інфраструктури	Не рекомендується
16	Заборонити повідомлення	Не рекомендується
17	Заборонити одноадресові відповіді на багатоадресові або широкомовні запити	Включено
18	Задати виключення для портів	Не рекомендується
19	Дозволяти локальні виключення для портів	Відключено
20	Забороняти будь-які зєднання при завантаженні	Не рекомендується
21	Блокувати фрагментовані IP	Включено
22	Аналізувати протокол	Включено
23	Перевіряти контрольну суму пакету	Не рекомендується
24	Відстежувати інші NDIS протоколи, окрім TCP/IP	Не рекомендується

2.5 Висновок

В розділі наведено обґрунтування актуальності вибраної теми, проведений аналіз інформаційно-телекомунікаційної системи ТОВ «Інтер-Транзит», виявленні можливі загрози безпеці конфіденційної інформації. Виконана розробка політики безпеки і технічного завдання на створення системи захисту конфіденційної інформації. Виконана розробка проектних рішень, що підтримують систему захисту інформації від НСД.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

Метою економічного розділу є обґрунтування економічної доцільності розробки системи захисту інформації ТОВ «Інтер-Транзит» з детальною розробкою міжмережевого захисту. Відповідно до цього необхідно виконати наступні розрахунки:

– капітальні витрат на придбання і налагодження складових системи інформаційної безпеки або витрат, що пов’язані з виготовленням апаратури, приладів, програмного забезпечення;

– річні експлуатаційні витрати на утримання і обслуговування об'єкта проектування;

– річний економічний ефект від впровадження запропонованих заходів;

– показники економічної ефективності впровадження системи захисту на підприємстві.

3.1 Розрахунок (фіксованих) капітальних витрат

Капітальні інвестиції – це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

Витрати на впровадження системи захисту інформації на підприємстві визначаються, виходячи з трудомісткості кожної операції, та належать до капітальних витрат.

Визначення трудомісткості розробки системи захисту інформації на підприємстві

Трудомісткість розробки системи захисту інформації на підприємстві визначається тривалістю кожної робочої операції, до яких належать наступні:

До капітальних витрат належать витрати на розробку політики безпеки інформації, які визначаються виходячи з трудомісткості розробки політики безпеки інформації.

Визначення трудомісткості розробки політики безпеки інформації

Трудомісткість розробки політики безпеки інформації визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації (за умови роботи одного спеціаліста з інформаційної безпеки):

$$t = t_{\text{тз}} + t_{в} + t_{а} + t_{\text{вз}} + t_{\text{озб}} + t_{\text{овр}} + t_{д}, \text{ годин,}$$

де $t_{\text{тз}}$ – тривалість складання технічного завдання на розробку політики безпеки інформації, $t_{тз}$=12 годин;

$t_{в}$ – тривалість розробки концепції безпеки інформації у організації, $t_{в}$=30 годин;

$t_{а}$ – тривалість процесу аналізу ризиків, $t_{тз}$=20 годин;

$t_{\text{вз}}$ – тривалість визначення вимог до заходів, методів та засобів захисту, $t_{вз}$=16 годин;

$t_{\text{озб}}$ – тривалість вибору основних рішень з забезпечення безпеки інформації, $t_{озб}$=12 годин;

$t_{\text{овр}}$ – тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організації, $t_{овр}$=10 годин;

$t_{д}$ – тривалість документального оформлення політики безпеки, $t_{д}$=5 годин.

Отже, t=12+30+20+16+12+10+5= 105 годин,

Розрахунок витрат на розробку системи захисту інформації на підприємстві

Витрати на розробку системи захисту інформації на підприємстві Крп складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки

Ззп і вартості витрат машинного часу, що необхідний для розробки політики безпеки інформації Змч.

$$К_{рп} = З_{зп} + З_{мч} .$$

$$К_{рп} = З_{зп} + З_{мч} = 26250+345,53 = 25415,53 \text{ грн.}$$

$$З_{зп} = t\ З_{пр} = 105*250 = 26250 \text{ грн.}$$

де t – загальна тривалість розробки політики безпеки, годин;

Зіб – средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину.

Вартість машинного часу для розробки політики безпеки інформації на ПК визначається за формулою:

$$З_{мч}= t*С_{мч}=105*3,17=345,53 \text{ грн.}$$

де $t_д$ – трудомісткість підготовки документації на ПК, годин;

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$C_{\textbf{мч}} = 0,8 \cdot 1 \cdot 1,64 + \frac{3600 \cdot 0,4}{1920} + \frac{5300 \cdot 0,1}{1920} = 3,17 \text{ грн.}$$

На всіх комп’ютерах (13 робочих станцій) підприємства ТОВ «Інтер-Транзит» вже встановлене необхідне для реалізації запропонованих заходів програмне забезпечення, а саме: операційна система Microsoft Windows 10, антивірус ESET NOD32, Microsoft Office 2016 та брандмауер Comodo Firewall. На серверах ІКС встановлена операційна система Windows 2012 Server. Тому додаткові витрати на придбання апаратного чи програмного забезпечення не потрібні.

Таким чином, капітальні (фіксовані) витрати на створення політики безпеки інформації:

$$К = К_{рп} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н} = 25415{,}53 \text{ грн.}$$

де $К_{рп}$ – вартість розробки політики інформаційної безпеки та залучення для цього зовнішніх консультантів, тис. грн;

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), тис. грн;

$К_{пз}$ – вартість створення основного й додаткового програмного забезпечення, тис. грн;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу,

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки.

3.1.1 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_{в} + С_{к} + С_{ак}, \quad \text{грн.}$$

де $С_{в}$ - вартість відновлення й модернізації системи ($С_{в} = 0$);

$С_{к}$ - витрати на керування системою в цілому;

$С_{ак}$ - витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак} = 0$ грн.).

Витрати на керування системою інформаційної безпеки ($С_{к}$) складають:

$$С_{к} = С_{н} + С_{а} + С_{з} + С_{ел} + С_{о} + С_{тос}, \text{ грн.}$$

Витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються ($С_н$ = 14000 грн.).

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_з$), складає:

$$С_з = З_{осн} + З_{дод}, \text{ грн.}$$

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата – в розмірі 8-10% від основної заробітної плати.

Основна заробітна плата одного спеціаліста з інформаційної безпеки на місяць складає 12000 грн. Додаткова заробітна плата – 10% від основної заробітної плати. Виконання роботи щодо впровадження системи захисту інформації на підприємстві потребує залучення спеціаліста інформаційної безпеки на 0,25 ставки. Отже,

$$С_з = (12000*12 + 12000*12*0,1)*0,25= 39600 \text{ грн.}$$

З 01.01.2019 р. Ставка ЄСВ для всіх категорій платників складає 22%.

$$С_{єв} = 39600*0,22 = 8712 \text{ грн.}$$

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_{ел}$), визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е, \text{ грн.,}$$

де Р – встановлена потужність апаратури інформаційної безпеки, (Р=1,1 кВт);

$F_р$ – річний фонд робочого часу системи інформаційної безпеки ($F_р$ = 1920 год.);

$Ц_е$ – тариф на електроенергію, ($Ц_е$ = 1,64 грн./кВт за годину).

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року:

$$С_{ел} = 1,1*1920*1,64 = 3463,68 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат - 1% (Стос =25415,53*0,01=254,16 грн).

Витрати на керування системою інформаційної безпеки ($С_к$) визначаються:

$$С_к = 14000+39600+8712+3463,68 +254,16= 66029,84 \text{ грн.}$$

Таким чином, річні поточні витрати на функціонування системи інформаційної безпеки складають 66029,84 грн.

3.2 Оцінка можливого збитку від атаки на вузол або сегмент мережі

3.2.1 Оцінка величини збитку

Для розрахунку вартості такого збитку можна застосувати наступну спрощену модель оцінки для умовного підприємства.

Необхідні вихідні дані для розрахунку:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, 5 години;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 2 години;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, 2 години;

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), 16000 грн./міс.;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 12000 грн./міс.;

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.), 1 особи;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 12 осіб.;

О – обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 550 тис. грн. у рік;

$П_{зч}$ – вартість заміни встаткування або запасних частин, грн;

I – число атакованих сегментів корпоративної мережі, 1;

N – середнє число атак на рік, 32.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить:

$$U = П_п + П_в + V,$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

$П_в$ – вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки:

$$П_п = \frac{\sum Зс}{F} \cdot t_п = \frac{12000 \cdot 12}{176} \cdot 5 = 4090,91 \text{ грн},$$

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить 176 ч).

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_в = П_{ви} + П_{пв} + П_{зч},$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн.;

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{ви} = \frac{\sum Зс}{F} \cdot t_{ви} = \frac{12000 \cdot 12}{176} \cdot 2 = 1636,36 \text{ грн.}$$

Витрати на відновлення сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{пв} = \frac{\sum Зо}{F} \cdot t_в = \frac{16000 \cdot 1}{176} \cdot 2 = 181,82 \text{ грн.}$$

Витрати на заміни встаткування або запасних частин можуть скласти 1000 грн.

Тоді витрати на відновлення працездатності вузла або сегмента корпоративної мережі складуть:

$$П_в = 1636,36 + 181,82+1000 = 2818,18 \text{ грн.}$$

Втрати від зниження очікуваного обсягу прибутків за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи із средньогодинного обсягу прибутку і сумарного часу простою сегмента корпоративної мережі:

$$V = \frac{O}{Fг} \cdot (t_п + t_в + t_{ви})$$

$$V = \frac{550000}{2080} \cdot (5+2+2) = 2379,81 \text{ грн.}$$

де $F_г$ – річний фонд часу роботи філії (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько 2080 год.

$$U = 4090,91+ 2818,18 +2379,81 = 9288,9 \text{ грн.}$$

Таким чином, загальний збиток від атаки на сегмент корпоративної мережі організації складе:

$$B = \sum_i \sum_n U = \sum_1 \sum_{32} 9288,9 = 297244,8 \text{ грн.}$$

3.2.2 Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної:

$$E = B \cdot R - C \text{ грн.,}$$

де B – загальний збиток від атаки у разі перехоплення інформації, тис. грн.;

R – вірогідність успішної реалізації атаки на сегмент мережі, частки одиниці (50%);

С – щорічні витрати на експлуатацію системи інформаційної безпеки.

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки:

$$E = 297244,8*0,5 – 66029,84 = 82592,56 \text{ грн.}$$

3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки:

$$ROSI = \frac{E}{K}, \quad \text{частки одиниці,}$$

де E – загальний ефект від впровадження системи інформаційної безпеки грн.;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Коефіцієнт повернення інвестицій ROSI:

$$ROSI = \frac{82592,56}{25415,53} = 3,25, \quad \text{частки одиниці,}$$

Проект визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції:

$$ROSI > (N_{деп} – N_{інф})/100),$$

де $N_{деп}$ – річна депозитна ставка, (19%);

$N_{інф}$ – річний рівень інфляції, (14%).

Розрахункове значення коефіцієнта повернення інвестицій:

$$3,25 > (19 – 14)/100 = 3,25 > 0,05.$$

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$T_o = \frac{K}{E} = \frac{1}{ROSI} = \frac{1}{3,25} = 0,31 \text{ , років.}$$

3.4 Висновок

Розробка системи захисту інформації ТОВ «Інтер-Транзит» з детальною розробкою міжмережевого захисту є економічно доцільною, виходячи з показників економічної ефективності, а саме: коефіцієнт повернення інвестицій ROSI складає 3,02 грн/грн., термін окупності при цьому складатиме 0,31 років. Щорічні витрати на експлуатацію системи захисту інформації для ТОВ «Інтер-Транзит» складатимуть 66029,84 грн. при наявності економічного ефекту у 82592,56 грн.

ВИСНОВКИ

У роботі розроблена система захисту конфіденційної інформації підприємства ТОВ «Інтер-Транзит» та розроблені:

– організаційно-технічні заходи щодо захисту інформації;

– групи і ролі користувачів, відповідно до поставлених ним завдань і прав доступу;

– програмні заходи щодо захисту інформації;

– комплект документів, що регламентують організаційні аспекти захисту.

У економічному розділі визначено, що об'єм втрат підприємства в рік у разі дії погроз на конфіденційну інформацію підприємства значно перевищують об'єм витрат на реалізацію розробленої системи захисту інформації.

При порівняно високому рівні інвестиційного капіталу розробка дає великий економічний ефект. Це видно при розрахунку показника оцінки ефективності інвестицій проекту ЧПВ. Оскільки показник значно більше 0 необхідно зробити висновок, що з економічної точки зору розробка є ефективною і конкурентоздатною.

ПЕРЕЛІК ПОСИЛАНЬ

1 НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі. Затверджено наказом Департаменту спеціальних телекомунікаційних систем і захисту інформації Служби безпеки України від 04 грудня 2000 р. № 53. // Офіційний сайт Службы безпеки України. Спосіб доступу: URL: http: // www.dstszi.gov.ua/. – Загол. з экрану.

2 Соколов А.В., Шаньгин В.Ф. Захист інформації в розподілених корпоративних мережах і системах. – М.: ДМК Пресс, 2002. – 656 с., ил.

3 Домарев В. В. Безпека інформаційних технологій. Системний підхід. Київ. 2004.

4 НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу від 28 квітня 1999 р. №22.

5 НД ТЗІ 3.7-001-99 Методичні вказівки для розробки технічного завдання на створення комплексною систем захисту інформації в автоматизованій системі. Затверджено наказом Департаменту спеціальних телекомунікаційних систем і захисту інформації Служби безпеки України від 28 квітня 1999 р. би 22. // Офіційний сайт Служби безпеці України. Спосіб доступу: URL: http: // www.dstszi.gov.ua/. – Загол. с экрана.

6 НД ТЗІ 2.5-006-99 и НД ТЗИ 2.7-002-99 Методичні вказвки з використання засобів копіювально-розмножувальної техніки.

7 Журнал «Бизнес и безопасность» № 1/2019, Захист інформації. Аналіз об'єкту. Ст. 41 – 42.

8 Методичні вказівки по складанню економічної частини дипломного проекту для студентів спеціальностей 7.091402 “Комп'ютеризовані системи керування та автоматики” і 7.092208 “Електропривод та автоматизація промислового обладнання і технологічних комплексів” / Упорядн.: І.В. Шереметьєва, О.Г. Немцов. – Дніпропетровськ, НГА України, 1997. – 52с.

9 Прайс-лист (ОПТА-БЕЗПЕКА), mailto: info@opta.com.ua; http://www.opta.com.ua

10 Закон України № 2658-XII від 02.10.92 ”Про інформацію”. // Безопасность информации. – 1995. – № 2.

11 НД ТЗІ 1.1-003-99. Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом Департаменту спеціальних телекомунікаційних систем і захисту інформації Служби безпеці України від 28 квітня 1999 р. би 22. // Офіційний сайт Служби безпеці України. Спосіб доступу: URL: http: // www.dstszi.gov.ua/. – Загол. с экрана.

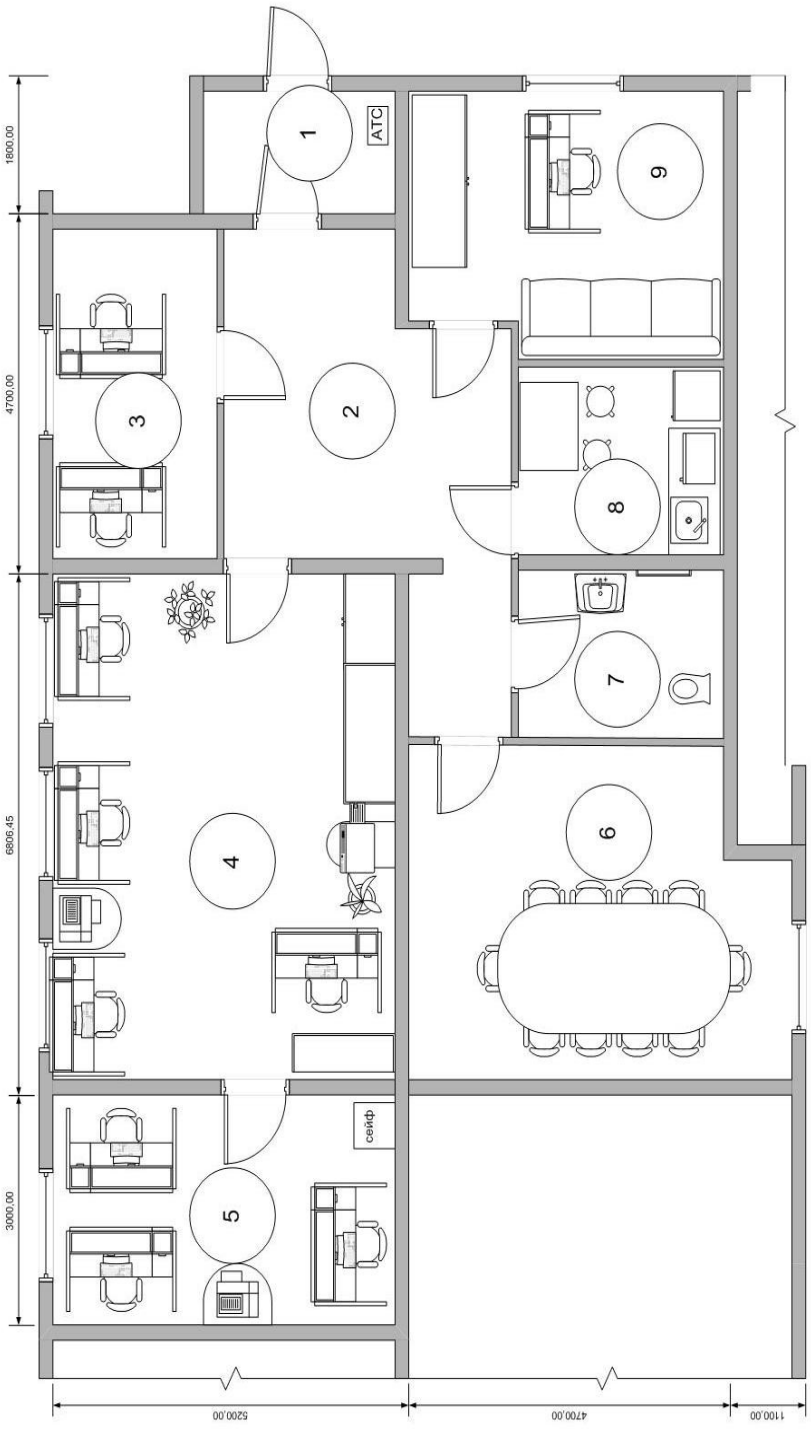
12 НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом Департаменту спеціальних телекомунікаційних систем і захисту інформації Служби безпеці України від 28 квітня 1999 р. би 22. // Офіційний сайт Служби безпеці України. Спосіб доступу: URL: http: // www.dstszi.gov.ua/. – Загол. с экрана.

13 Буров Є. Комп'ютерні мережі. 2-ге оновлене і доповнене видання. Львів: БаК, 2003. – 584 с., іл.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	1	
5	А4	1 Розділ	16	
6	А4	2 Розділ	27	
7	А4	3 Розділ	11	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	4	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	
14	А4	Додаток Д	1	

ДОДАТОК Б. Схема приміщення ТОВ «Інтер-Транзит»



№ п/п	Найменування приміщень
1	Тамбур
2	Коридор
3	Бухгалтерія
4	Експедиційний відділ
5	Кабінет директора
6	Конференц зал
7	Санвузол
8	Кухня
9	Кімната відпочинку

Рисунок 1 – Схема приміщення ТОВ «Інтер-Транзит»

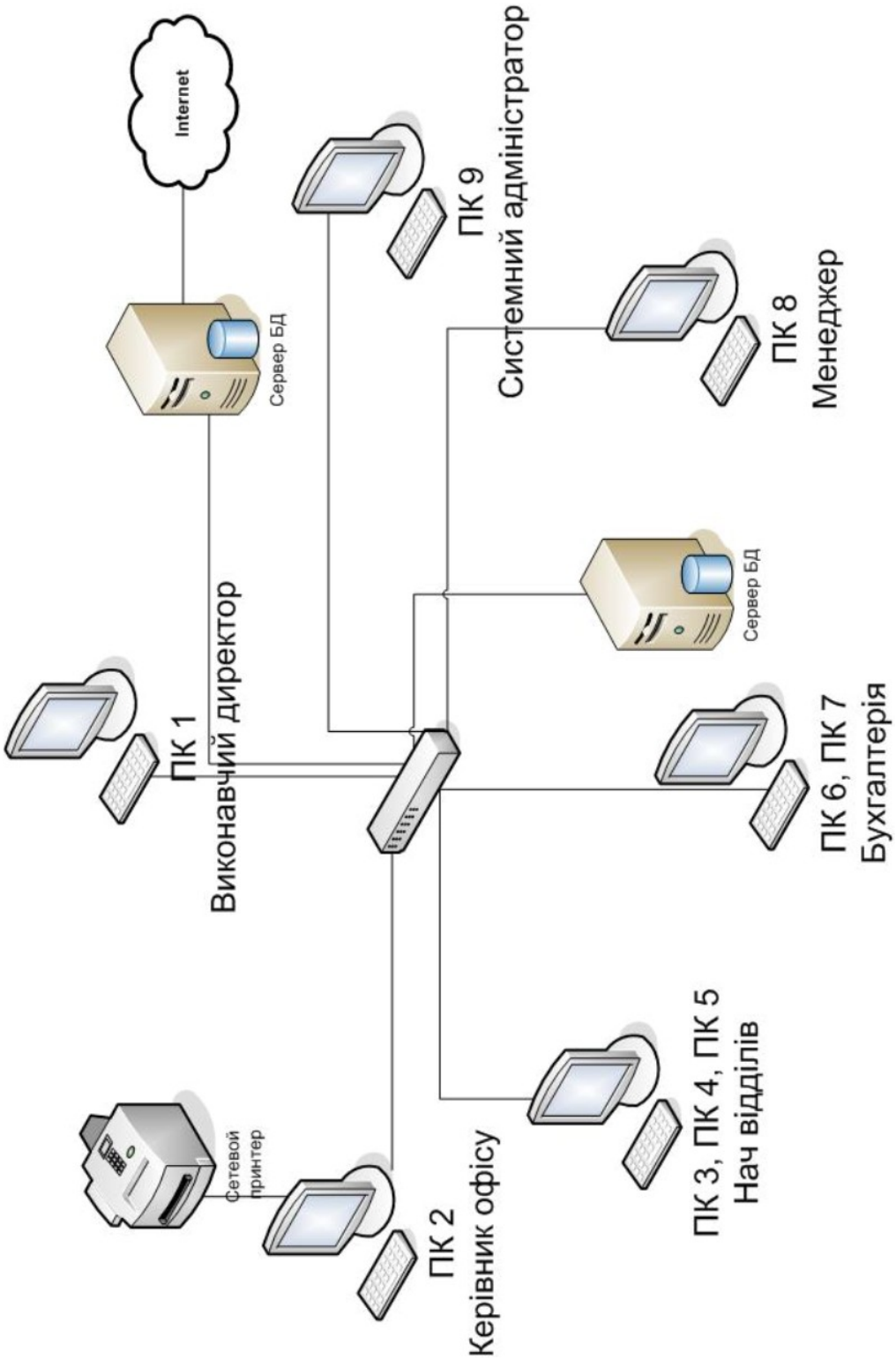


Рисунок 2 – Схема локальної комп’ютерної мережі ТОВ «Інтер-Транзит»

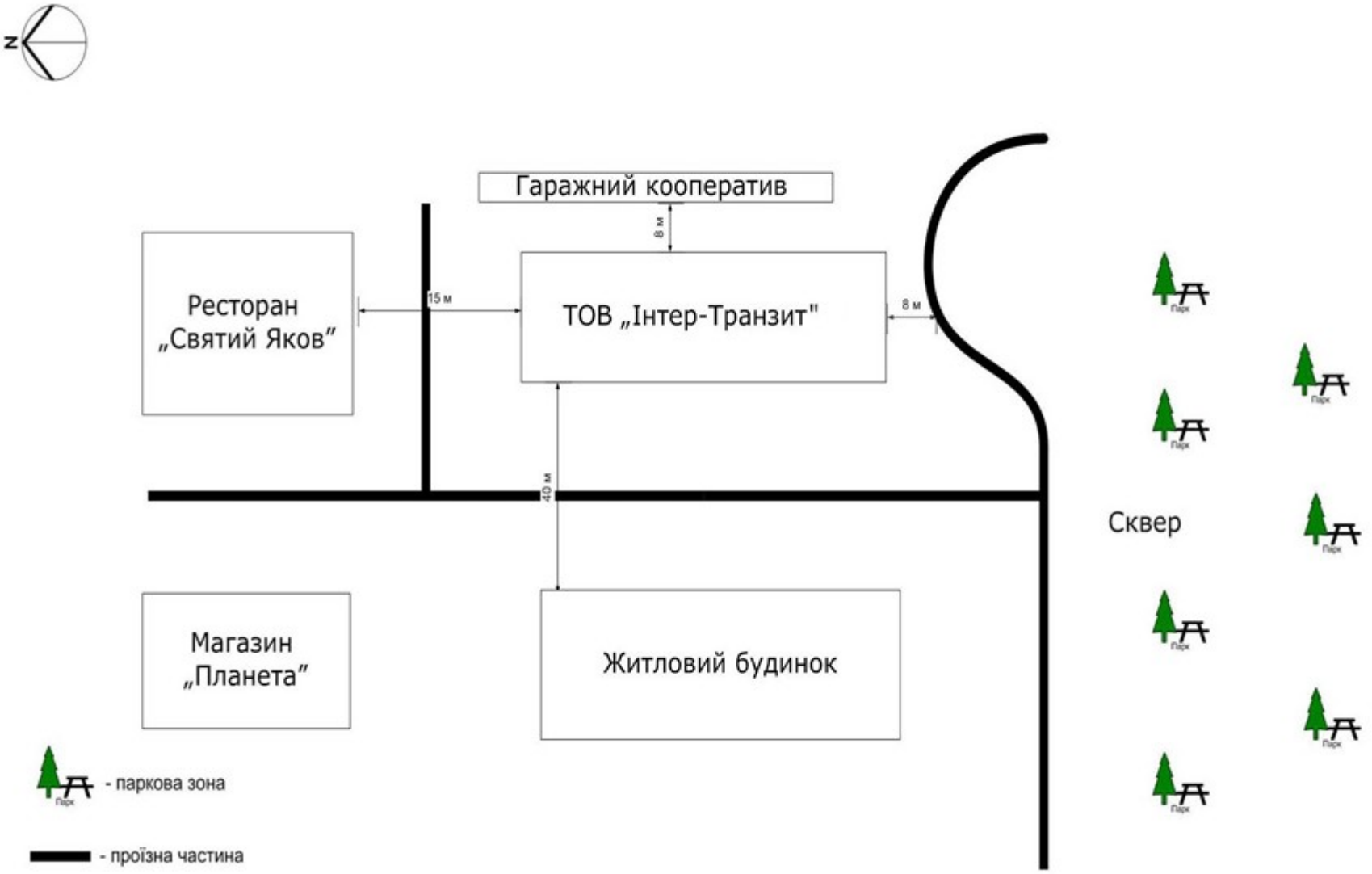

N
Гаражний кооператив
8 м
Ресторан
„Святий Яков”
15 м
ТОВ „Інтер-Транзит"
8 м
40 м
Сквер
Магазин
„Планета”
Житловий будинок
- паркова зона
- проїзна частина

Рисунок 3 – Ситуаційний план

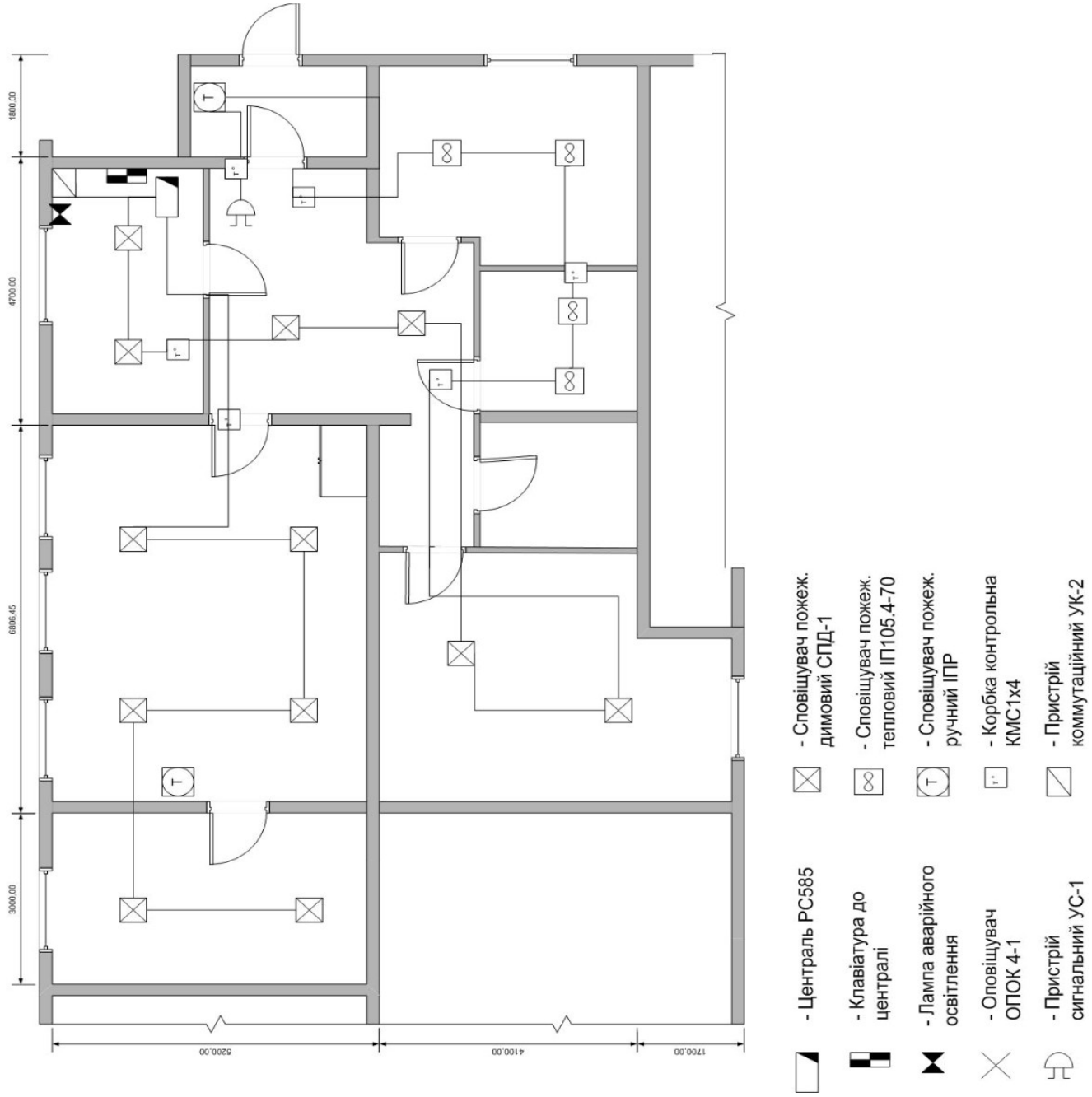


Рисунок 4 – Схема пожежної та охоронної сигналізації ТОВ «Інтер-Транзит»

ДОДАТОК В. Перелік документів на оптичному носії

1 Титульна сторінка.doc

2 Завдання.doc

3 Реферат.doc

4 Список умовних скорочень.doc

5 Зміст.doc

6 Вступ.doc

7 Розділ 1.doc

8 Розділ 2.doc

9 Розділ 3.doc

10 Висновки.doc

11 Перелік посилань.doc

12 Додаток А.doc

13 Додаток Б.doc

14 Додаток В.doc

15 Додаток Г.doc

16 Додаток Д.doc

Презентація.pptx

ДОДАТОК Г. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Д. ВІДГУК

на кваліфікаційну роботу бакалавра на тему:
Розробка міжмережевого захисту в системі захисту інформації ТОВ «Інтер-Транзит»
Ахмєдова Ахмеда Анара огли

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на __ сторінках та містить __ рисунків, __ таблиць, __ джерел та __ додатка.

Мета роботи: на підставі чинних законодавчих і нормативних документів України розробити систему захисту інформації на товаристві з обмеженою відповідальністю «Інтер-Транзит» з детальною розробкою міжмережевого захисту.

У спеціальній частині дана характеристика об’єкту захисту, розроблена політика безпеки, модель загроз, розроблене технічне завдання на створення системи захисту конфіденційної інформації

Практичне значення роботи полягає в підвищенні рівня захищеності конфіденційної інформації, що циркулює в інформаційній мережі товариства з обмеженою відповідальністю «Інтер-Транзит».

Студент показав достатній рівень володіння теоретичними положеннями з обраної теми, показав здатність формувати власну точку зору (теоретичну позицію).

Робота оформлена та написана грамотною мовою. Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

В цілому робота задовольняє усім вимогам і може бути допущена до захисту, а його автор заслуговує на оцінку «_____».

Керівник