**ЗМІСТ**

[ВСТУП 6](#_Toc355391683)

[1 АНАЛІЗ СТРУКТУРИ ПІДПРИЄМСТВА ТА ЇЇ ІНФОРМАЦІЙНИХ ПОТОКІВ 7](#_Toc355391684)

[1.1 Структура підприємства 7](#_Toc355391685)

[1.2 Види інформації на підприємстві 9](#_Toc355391686)

[1.3 Аналіз ресурсів підприємства 9](#_Toc355391687)

[1.4 Аналіз інформаційних потоків підприємства 13](#_Toc355391688)

[2 АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ ЗАХИСТУ КОМП’ЮТЕРНИХ МЕРЕЖ 15](#_Toc355391689)

2.1 Аналіз типів атак та методів захисту……………………….…………………15

2.2 Методи захисту від атак………………………………………………………..16

[3 РОЗРОБКА ТОПОЛОГІЇ МЕРЕЖІ 15](#_Toc355391690)

[3.1 Аналіз структури мережі підприємства. 19](#_Toc355391691)

[3.2 Розподіл адресного простору 19](#_Toc355391692)

[3.3 Налаштування мережі 22](#_Toc355391693)

[4 ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОМП’ЮТЕРНОЇ МЕРЕЖІ 24](#_Toc355391694)

[4.1 Аналіз застосовуваних методів 24](#_Toc355391695)

[4.2 Технічний захист інформації 25](#_Toc355391696)

[5 РЕАЛІЗАЦІЯ ЗАХИСТУ 28](#_Toc355391697)

[5.1 Вибір міжмережевого екрана 28](#_Toc355391698)

[5.2 Аналіз систем виявлення вторгнень 29](#_Toc355391699)

[5.3 Аналіз антивірусних програм 30](#_Toc355391700)

[ВИСНОВКИ 32](#_Toc355391701)

[ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ 33](#_Toc355391702)

[Додаток А. Технічне завдання](#_Toc355391703) 33

# ВСТУП

Проблема забезпечення внутрішньої інформаційної безпеки стає усе більш актуальною для автомобільних підприемств. Це пов'язано із загостренням конкурентної боротьби на внутрішніх ринках, і з виходом компаній на міжнародний рівень. З точки зору інформаційної безпеки багато компаній сьогодні нагадують фортеці, оточені декількома периметрами потужних стін. Проте практика показує, що інформація все одно витікає, а це завдає нечуваних збитків. Доцільно розглядати побудову захисту як комплексну систему заходів, оскільки непередбачені або навмисні антропогенні загрози можуть виникати в різні моменти життєвого циклу і за різних обставин функціонування апаратури, програмного забезпечення, кваліфікації персоналу.

Надзвичайно актуальною на сьогоднішній день є проблема захисту комп'ютерних мереж та даних, що циркулюють в них, оскільки перевагою мережі є доступ до спільних даних та пристроїв, що зумовлює можливість несанкціонованого доступу до даних. Тому захист інформаційного середовища стає таким же важливим, як і захист технічного обладнання, із якого побудована мережа, як захист навколишнього середовища, підприємства, власного майна.

КСЗІ призначена для забезпечення безпеки критичної інформації та інформаційних ресурсів у процесі функціонування АС.

Мета функціонування КСЗІ полягає в підтримці необхідного рівня інформаційної безпеки АС відповідно політиці безпеки, яка визначається її власником.

Для інформації, що є власністю держави, вимоги щодо її захисту встановлені на законодавчому рівні.

# АНАЛІЗ СТРУКТУРИ ПІДПРИЄМСТВА ТА ЇЇ ІНФОРМАЦІЙНИХ ПОТОКІВ

## Структура підприємства

Рис1.1- Структура підприємства ТОВ «Укроптторг».

1) Адміністративний відділ. Відповідає за організацію управління всіма службами підприємства, вирішує фінансові питання, питання кадрового забезпечення, займається створенням і підтримкою необхідних умов праці для персоналу, контролює дотриманням встановлених норм і правил по охороні праці, техніці безпеки, протипожежній і екологічній безпеці.  
Склад відділу: секретаріат, кадрова служба, директор.

2) Фінансовий відділ. Займається питаннями оперативного і стратегічного планування. Аналізує результати господарської і фінансової діяльності.

Склад відділу: комерційний директор, служба маркетингу, бухгалтерія.

3) Інженерний (технічний)відділ. Створюють умови для функціонування систем кондиціонування, теплопостачання, санітарно-технічного устаткування, електротехнічних пристроїв, служб ремонту і будівництва, систем зв'язку.

Склад відділу: головний інженер; дизайнерська лабораторія ; конструкторський відділ,відділ випробувань, виробничий відділ.

4)Відділ обслуговування клієнтів - займається вирішенням наступних питань: прийняття замовлень на купівлю товару, повідомлення клієнтів про вихід нового товару, послуги або акції; надає необхідну інформацію і консультацію.

Відділ обслуговування включає наступні підрозділи:

* Менеджер.
* Служба отримання замовлень по місту. Це служба, з якою більше всього контактує клієнт і куди він найчастіше звертається за інформацією і послугами. Перше сприятливе враження означає дуже багато для загальної оцінки роботи підприємства. Негативне враження може призвести до антиреклами (чорного піару). До найважливіших функцій служби отримання замовлень: власне отримання замовлень на товар, виписка рахунків і виробництво розрахунків з клієнтами (попередніх і остаточних); ведення журналу реєстрації, слідкування за доставкою товару до клієнта.

Служба отримання замовлень по області. Дана служба виконує ті ж самі дії, що і попередня, але тільки працює не у обласному центрі, а по всій області.

5) Служба безпеки***.*** Займається питаннями захисту в середині підприємства.

Головні вимоги до відділу:

* заходи повинні прийматися оперативно і ефективно з економічної точки зору.
* головна увага повинна приділятися так званим проблемам попереджувальної безпеки, а не розслідуванню вже здійснених злочинів і покаранню.

Заходи, здійснювані службою безпеки підприємства включають в себе:

* режимні заходи;
* фізичну охорону;
* технічні засоби захисту;
* попереджувально-профілактичну роботу.

## Види інформації на підприємстві

Усю інформацію з якою працює підприємство потрібно поділити на окремі групи, щоб чітко визначити який підрозділ до якої інформації має доступ.

На підприємстві можна виділити такі види інформації:

* фінансова;
* юридична;
* конфіденційна;
* робоча.

Звичайно на практиці можна використати значно детальніший поділ інформації на підвиди. При цьому збільшиться надійність системи захисту, але і значно збільшиться складність її реалізації, а отже більш складнішу систему недоцільно використовувати в рамках даної курсової роботи (табл. 1.1).

Таблиця 1.1 Розподіл доступу до інформації

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Відділ\Інформація | Фінансова | Юридична | Конфіденційна | Робоча |
| Фінансовий відділ | + | + | + | + |
| Адміністративний відділ | + | + | + | + |
| Відділ обслуговування | + | - | - | + |
| Технічний відділ | - | - | - | - |
| Служба безпеки | - | + | + | - |

## Аналіз ресурсів підприємства

На підприємстві постійно йде обмін інформацією. Вона може бути паперова, електронна, акустична. Паперова інформація – це інформація, яку передають на папері (напр. звіти, контракти, договори та ін.), електронна – інформація, яку отримують за допомогою переносних носіїв інформації, вона зберігається на комп’ютері і при потребі її можна подати у паперовому вигляді, акустична – інформація, яку ми отримуємо за допомогою телефону, відеоапаратури.

Інформаційний потенціал підприємства регулює виробничі процеси, сприяє підвищенню продуктивності живої праці ефективності використання предметів праці й енергетичних ресурсів, допомагає підняти рівень і ефективність технологій [2].

Часто інформацію класифікують за трьома ознаками: доступність, цілісність та конфіденційність. Саме ці ознаки визначають рівень доступу до інформації (табл. 1.2).

Таблиця 1.2 – Модель класифікації інформації

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Класифікація інформації | | | | | |
| Цілісність | | Доступність | | Конфіденційність | |
| Ц0 | Критична | Д0 | Критична | К0 | Критична |
| Ц1 | Дуже важлива | Д1 | Дуже важлива | К1 | Дуже важлива |
| Ц2 | Важлива | Д2 | Важлива | К2 | Важлива |
| Ц3 | Значима | Д3 | Корисна | К3 | Значима |
| Ц4 | Не значна | Д4 | Неістотна | К4 | Мало значима |
|  |  | Д5 | Шкідлива | К5 | Не значна |

Визначимо, які ознаки мають основні інформаційні ресурси підприємства (табл. 1.3).

Таблиця 1.3 – Інформаційні ресурси підприємства

|  |  |  |  |
| --- | --- | --- | --- |
| № | Вид | Ознаки КІ | Користувачі інформацією |
| 1. | Аналітичні звіти | Ц2, Д2, К1 | Директор, бухгалтерія |
| 2. | Фінансові звіти | Ц0, Д2, К0 | Директор, бухгалтерія |
| 3. | Службова інформація | Ц3, Д3, К4 | Всі працівники організації |
| 4. | Технічна інформація | Ц0, Д1, К2 | ІТ-відділ |
| 5. | Персональні дані працівників | Ц2, Д2, К2 | Директор, відділ кадрів, служба безпеки, бухгалтерія |
| 6. | Інформація про організацію безпеки | Ц3,Д1,К0 | Директор, служба безпеки |
| 7. | Кредитна політика | Ц0, Д1, К1 | Директор, бухгалтерія, |
| 8 | Інформація про поточний стан грошових ресурсів | Ц0,Д1,К0 | Директор, бухгалтерський відділ |
| 9. | Персональні дані клієнтів | Ц1,Д2,К1 | Директор, відділ роботи обслуговування клієнтів, служба безпеки |
| 10. | Бухгалтерські звіти | Ц0, Д1, К0 | Директор, бухгалтерія |
| 11. | Кредитна інформація клієнтів | Ц1, Д2, К1 | Директор, бухгалтерія |
| 12. | Депозитна інформація клієнтів | Ц1, Д2, К1 | Директор, бухгалтерія, |
| 13. | Інформація про партнерів | Ц1, Д1, К2 | Директор, комерційний директор |

Інформація може бути розподілена по пріоритетності, а, отже, застосовуються різні методи захисту інформації при передачі. Основні методи захисту інформації при її використанні у організації наведені в табл.1. 4.

Таблиця 1.4 - Методи захисту інформації на підприємстві.

|  |  |
| --- | --- |
| № | Метод захисту |
| 1 | Автентифікація |
| 2 | Авторизація |
| 3 | Кодування |
| 4 | Моніторинг |
| 5 | Виявлення вторгнень |
| 6 | Реєстрація та аудит |
| 7 | Перевірка цілісності |

Будь-яка організація має власне технічне забезпечення. В наш час кожен офіс потребує комп’терного обладнання. Наближено, необхідні апаратні засоби для банківського відділення на ведено в таблиці 1.5.

Таблиця 1.5 – Технічна складова організації

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| № | Технічний засіб | К-сть | Виробник | Рік випуску | Інф. рес. | Відділи | Методи захисту |
| 1 | Серверний ПК | 1 | ASUSTeK | 2010 | 1-13 | 9 | 1-7 |
| 2 | Серверний ПК | 1 | ASUSTeK | 2010 | - | 9 | 1, 2, 3, 4, 6 |
| 3 | Робоча станція(ПК) | 1 | ACER | 2010 | 10 | 4 | 1, 4, 5, 6, 7 |
| 4 | Робоча станція(ПК) | 1 | ACER | 2010 | 2 | 2 | 1, 4, 5, 6, 7 |
| 5 | Робоча станція(ПК) | 1 | ACER | 2010 | 1 | 5 | 1, 2, 6, 7 |
| 6 | Робоча станція(ПК) | 1 | ACER | 2010 | 11,12 | 6 | 1, 2, 5, 6, 7 |
| 7 | Робоча станція(ПК) | 1 | ACER | 2010 | 8 | 3 | 1, 2, 5, 6, 7 |
| 8 | Робоча станція(ПК) | 27 | ACER | 2010 | 3, 4, 7 | Усі відділи | 1, 4, 6 |
| 9 | Принтер | 6 | Canon | 2010 | - | 1, 4, 5, 6, 10 | 4 |
| 10 | Маршрутизатор | 1 | CISCO | 2010 | - | 9 | 4 |
| 11 | Комутатор | 5 | D-Link | 2009 | - | 1, 2, 4, 5, 7, 8, 9 | 4 |

Необхідне для роботи програмне забезпечення наведено в таблиці 1.6.

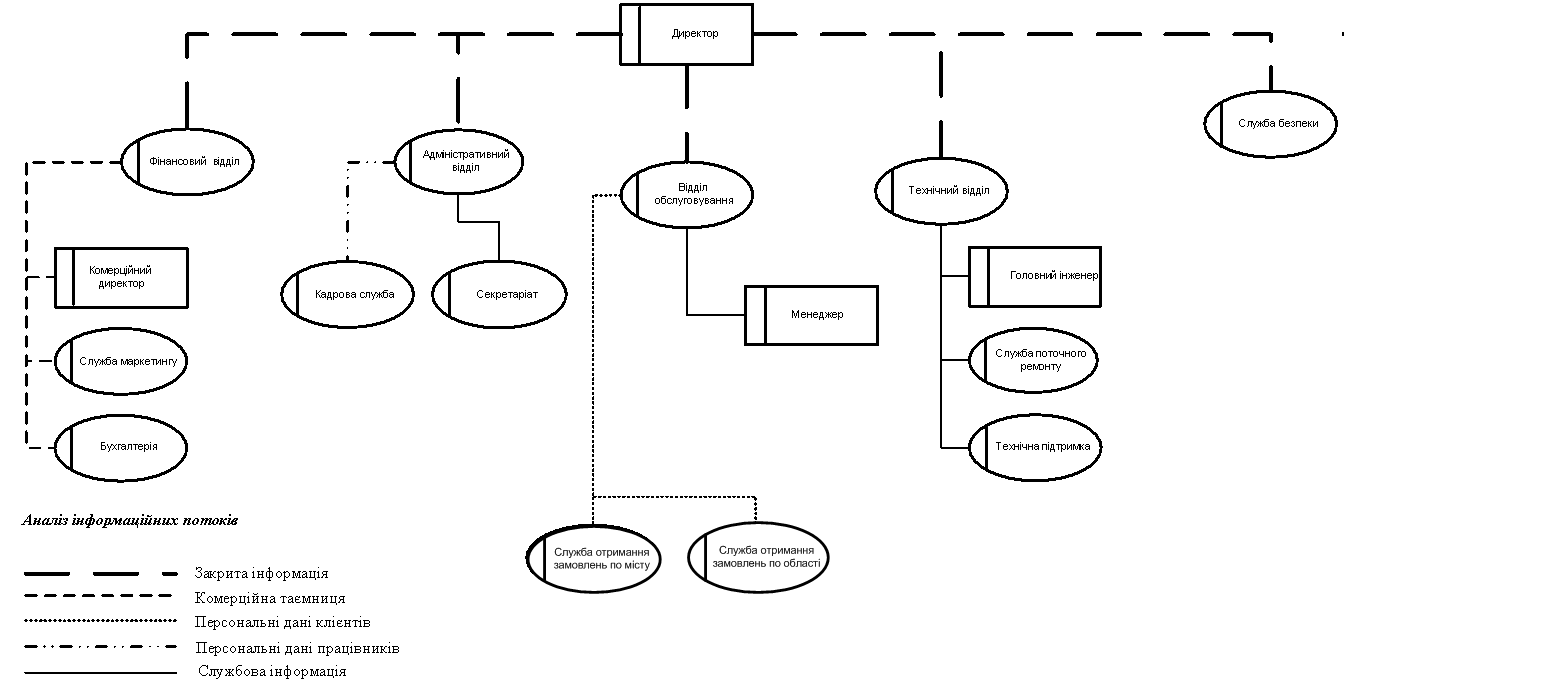
Таблиця 1.6 – Програмне забезпечення організації

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № | ПЗ | Назва | Ліцензія | Механізм захисту | Відділи | Встановна АЗ |
| 1 | OC | Windows Server 2008 | OEM | 1,2,3,4,5, 6,7 | 9 | 1,2 |
| 2 | OC | Windows 7 Professional | FPP | 9 | 3,4,5,6,7 |
| 3 | OC | Windows XP SP3 | OEM | Усі відд. | 8 |
|  | | | | | | |
| Продовження таблиці 1.6 | | | | | | |
|  | Сервер баз даних | Microsoft SQL Server 2008 | FPP | 1,4,5,6,7 | 9 | 1 |
| 4 | Офісне ПЗ | Microsoft Office 2010 | FPP | 4,7 | 1, 3, 5, 6, 7 ,8, 10 | 3,4,5,6,7,8 |
| 5 | Антивір. ПЗ | ESET NOD32 Antivirus 4 | Open License | 1,2,3,4,5, 6,7 | 1, 3, 5, 6, 7, 8, 10 | 3,4,5,6,7,8 |
| 7 | Спец. ПЗ | 1С | Open License | 1,2,3,4,5,6,7 | 2, 4 | 3,4,5,6,7,8 |
| 8 | PrintDrive | Canon Driver | FPP | 4 | 1, 4, 5, 10 | 9 |
| 9 | Мережа | IOS 345/3 | OEM | 2,3,5,7 | Усі відд. | 10,11 |

Також слід зазначити, що так як сервер є досить потужним комп’ютером, на нього буде покладено слідуючі функції:

* сервер Active Directory;
* внутрішній файловий сервер для зберігання інформації;
* мережевий екран (firewall).

## Аналіз інформаційних потоків підприємства

Рисунок 1.2 Інформаційні потоки на підприємстві

Інформаційні потоки — це фізичне переміщення інформації від одного співробітника підприємства до іншого або від одного підрозділу до іншого. Тому ми не розглядаємо перетворення інформації (наприклад, бухгалтерську проводку) як інформаційні потоки в системі контролінгу.

Система інформаційних потоків — сукупність фізичних переміщень інформації, яка дає можливість здійснити будь-який процес, реалізувати будь-яке рішення. Найзагальніша система інформаційних потоків — це сума потоків інформації, яка дозволяє підприємству вести фінансово-господарську діяльність.

Інформаційні потоки забезпечують нормальну роботу підприємства. Мета роботи з інформаційними потоками — оптимізація роботи підприємства. Існує безліч методів досягнення цієї мети.

Інформація, яка збирається в системі контролінгу для обробки і аналізу, повинна відповідати наступним вимогам:

* своєчасність, тобто інформація по витратах, виручці, прибутку повинна поступати тоді, коли ще має сенс їїаналізувати;
* достовірність (щоб не витрачати додаткові зусилля і час на перевірку інформації);
* релевантність (істотність), тобто інформація повинна допомагати ухвалювати рішення;
* корисність (ефект від використання інформації повинен перекривати витрати на її отримання);
* повнота, тобто не повинно бути упущень;
* зрозумілість, тобто інформація не повинна вимагати значних зусиль для "розшифровки";
* регулярність надходження.

Важливий аспект діагностики підприємств - аналіз інформаційних потоків, він допомагає контролеру зрозуміти механізм роботи підприємства. У процесі вивчення інформаційних зв'язків й інформаційних потоків служба контролінгу вивчає процеси виникнення, рухи й обробки інформації, а також спрямованість й інтенсивність документообігу на підприємстві.

Ціль аналізу інформаційних потоків на підприємстві - виявлення місць дублювання надлишку й недоліку інформації, причин її збоїв і затримок.  
 Найпоширеніший й, очевидно, самий практичний метод аналізу інформаційних потоків - складання графіків інформаційних потоків. Але для побудови графіків інформаційних потоків варто знати (або виробити самим) певні правила їхнього складання й умовні позначки окремих елементів.

# АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ ЗАХИСТУ КОМП’ЮТЕРНИХ МЕРЕЖ

2.1 Аналіз типів атак та методів захисту

З розвитком інформаційних технологій і проникненням їх в усі сфери сучасного життя росте число зловмисників, які активно ці технології використовують. Схематично зобразимо можливі типи атак на комп’ютерну мережу підприємства (рис. 2.1).

Рисунок 2.1 – Типи атак на мережу підприємства

Поштова атака або атака листами вважається найстарішим методом атак, хоча суть його проста й примітивна: велика кількість листів унеможливлюють роботу з поштовими скриньками, а іноді і з цілими поштовими серверами. Цю атаку складно запобігти, тому що провайдер може обмежити кількість листів від одного відправника, але адреса відправника і тема часто генеруються випадковим чином[3].

Віруси, троянські коні, черв’яки є більш витонченим методом отримання доступу до закритої інформації - це використання спеціальних програм для ведення роботи на комп'ютері жертви, а також подальшого розповсюдження (це віруси і черв'яки). Принципи дії цих програм дуже різноманітні і варіюються в залежності від потреби зловмисника.

Наступною атакою на комп’ютерну мережу є так звана мережева розвідка. У ході такої атаки хакер власне не робить ніяких деструктивних дій, але в результаті він може отримати закриту інформацію про побудову та принципи функціонування обчислювальної системи жертви. У ході такої розвідки зловмисник може проводити сканування портів, запити DNS, ехо-тестування відкритих портів, наявність і захищеність проксі-серверів[4].

Соціальна інженерія (від англ. Social Engineering) - використання некомпетентності, непрофесіоналізму або недбалості персоналу для отримання доступу до інформації. Як говорить стара приказка, «Найслабкіша ланка системи безпеки - людина».

Відмова в обслуговуванні або [DoS](http://wiki.tntu.edu.ua/%D0%9C%D0%B5%D1%82%D0%BE%D0%B4%D0%B8_%D0%B1%D0%BE%D1%80%D0%BE%D1%82%D1%8C%D0%B1%D0%B8_%D0%B7_Dos_%D0%B0%D0%B1%D0%BE_DDos_%D0%B0%D1%82%D0%B0%D0%BA%D0%B0%D0%BC%D0%B8)-атака (від англ. Denial of Service - відмова в обслуговуванні) - атака, яка має на меті змусити сервер не відповідати на запити реальних користувачів. Одним із найпоширеніших методів нападу є насичення атакованого комп'ютера або мережевого устаткування великою кількістю зовнішніх запитів (часто безглуздих або невірно сформульованих) таким чином атаковане устаткування не може відповісти користувачам, або відповідає настільки повільно, що стає фактично недоступним. Якщо атака відбувається одночасно з великої кількості [IP-адрес](https://uk.wikipedia.org/wiki/IP-%D0%B0%D0%B4%D1%80%D0%B5%D1%81%D0%B0), то її називають розподіленою (DDoS).

Також досить поширений вид атаки як сніффінг пакетів, заснований на роботі мережевої карти в режимі promiscuous mode, а також monitor mode для мереж Wi-Fi. У такому режимі всі пакети, отримані мережевою картою, пересилаються на обробку спеціальним додатком, який називається сніффер, для обробки. У результаті зловмисник може отримати велику кількість службової інформації: хто звідки куди передавав пакети, через які адреси ці пакети проходили.

2.2 Методи захисту від атак

Під захистом інформації розуміється сукупність заходів, методів і засобів, що забезпечують рішення наступних основних задач:

* перевірка цілісності інформації;
* виключення несанкціонованого доступу до ресурсів персонального комп’ютера (надалі ПК), а також до програм і даних, що зберігаються в ньому;
* виключення несанкціонованого використання програм, що зберігаються в  ПК.

Засоби захисту інформації можна розділяти на наступні категорії[5]:

* засоби власного захисту;
* засоби захисту як частина обчислювальної системи;
* засоби захисту із запитом інформації;
* засоби активного захисту;
* засоби пасивного захисту.

Найбільш надійними являються криптографічні методи захисту інформації, що відносяться до класу засобів захисту із запитом інформації.

Криптографічний захист – це захист даних за допомогою криптографічного перетворення: кодування та шифрування[6].

Для сучасних криптографічних систем захисту інформації сформульовані наступні загальноприйняті вимоги:

* зашифроване повідомлення повинно піддаватись читанню тільки при наявності ключа;
* число операцій, необхідних для визначення використаного ключа шифрування по фрагменту повідомлення і відповідного йому відкритого тексту, повинно бути не менше загального числа можливих ключів;
* число операцій, необхідних для розшифрування інформації шляхом перебору можливих ключів повинно мати строгу нижню оцінку і виходити за межі можливостей сучасних комп’ютерів ( із врахуванням можливості використання мережних обчислень)[7];
* знання алгоритму шифрування не повинно впливати на надійність захисту;
* незначна зміна ключа повинна приводити до значної зміни виду зашифрованого повідомлення навіть при використанні одного і того ж ключа;
* структурні елементи алгоритму шифрування повинні бути незмінними;
* алгоритм має допускати як програмну, так і апаратну реалізацію, при цьому зміна довжини ключа не повинна приводити до якісного погіршення алгоритму шифрування.

### Для забезпечення безпечного користування мережею з метою передачі повідомлень – використовується зашифрування вихідних повідомлень і розшифрування вхідних, щоб відкритий текст могли бачити лише кінцеві користувачі, використовуючи методи блокового шифрування.

На сьогодні склалася думка, що створити криптографічний алгоритм легко, і такі алгоритми реалізуються багатьма незалежними програмістами і фірмами. Проте реально оцінити стійкість цих алгоритмів не можливо, оскільки більшість їх творців не бажає їх розкривати, посилаючись на комерційну таємницю, а це не дає можливості провести криптоаналіз таких алгоритмів. Не варто розраховувати на те, що стійкість цих алгоритмів вища, ніж у тих, які були опубліковані.



Рисунок 2.2 – Методи захисту КМ

# РОЗРОБКА ТОПОЛОГІЇ МЕРЕЖІ

## Аналіз структури мережі підприємства.

Для побудови локальної мережі схематично використаємо структуру побудовану у вигляді зірки (топологія зірка ). У цьому випадку кожен комп'ютер підключається окремим кабелем до загального пристрою, називаному концентратором, що перебуває в центрі мережі. У функції концентратора входить напрямок переданої комп'ютером інформації одному або всім іншим комп'ютерам мережі. Головна перевага цієї топології перед загальною шиною - істотно більша надійність. Будь-які неприємності з кабелем стосуються лише того комп'ютера, до якого цей кабель приєднаний, і тільки несправність концентратора може вивести з ладу всю мережу. Крім того, концентратор може відігравати роль інтелектуального фільтра інформації, що надходить від вузлів у мережу, і при необхідності блокувати заборонені адміністратором передачі.

Для побудови даної мережі була вибрана топологія зірка, оскільки вона є базовою топологією комп’ютерних мереж. Вона є простою, достатньо надійною і досить дешевою при побудові. Топологія підмереж в кожному з відділів приблизно однакова. Вони відрізняються лише кількістю комп’ютерів в підмережах. Керівник підприємства матиме 1 комп’ютер, в якому зберігаються статистичні відомості, звіти всіх відділів про їх діяльність, тощо. Секретар керівника підприємства також матиме 1 комп’ютер.

Перелік комп’ютерів, що знаходяться в розпорядженні підприємства наведено в таблиці 5.

Таблиця 5 – Облік комп’ютерів у відділах підприємства

|  |  |  |  |
| --- | --- | --- | --- |
| Відділи | Кількість комп’ютерів | Доступ до LAN | Доступ до Internet |
| Директор | 1 | 1 | 1 |
| Адміністративний відділ | 5 | 5 | 5 |
| Фінансовий відділ | 5 | 5 | 5 |
| Технічний відділ | 6 | 6 | 6 |
| Відділ обслуговування | 5 | 5 | 5 |
| Служба безпеки | 9 | 9 | 6 |
| Сектерар | 1 | 1 | 1 |

Технічний відділ матиме в своєму розпорядженні 6 комп’ютерів для перегляду звітів підпорядкованих відділів, підготовки завдань та розпоряджень, аналізу діяльності відділів тощо.

Відділ обслуговування клієнтів для своєї звітності та виконання своїх службових обовязків матиме в своєму розпорядженні 5 комп’ютерів.

Служба безпеки має 10 комп’ютерів для аналізу загроз та попередження їх виникнення, перегляду записів відеокамер та інших функцій пов’язаних із безпекою інформаційних ресурсів підприємства.

Фінансовому та кадровому відділам для проведення аналізу діяльності підприємства необхідно по 5 комп’ютерів.

Комп’ютери кожного відділу з’єднані окремо до свого комутатора, а вже самі комутатори під’єднуються до маршрутизатора, що під’єднаний до сервера.

## Розподіл адресного простору

Мережа підприємства налічує 32 комп’ютери. Оскільки діяльність директора і його секретаря пов’язана та їх робоче місце розташоване близько один одного, то їх об’єднуємо в єдину підмережу. Всі інші відділи матимуть свої власні підмережі.

Комп’ютери підключені до загальної мережі організації, яка складається з наступного мережевого обладнання:

* 1 маршрутизатор;
* 6 комутаторів;
* 32 комп’ютерів, що підключені до локальної мережі;
* 1 сервер.

Локальна мережа поділена на підмережі по відділам. Кожна з підмереж буде під’єднана до комутаторів, а комутатори до маршрутизатора. Маршрутизатор напряму підключений до сервера організації, на якому зберігаються всі дані.

Оскільки мережа складається лише з 32 комп’ютерів, 1 сервера та одного маршрутизатора, то доцільно використати одну мережу, яку можна розбити на сегменти необхідної кількості. Для розподілення адресного простору потрібно визначити маски змінної довжини для кожного сегменту мережі.

Значення кількості комп’ютерів в підмережі обраховуємо за формулою:

2N – 2 > К,

де К – кількість комп’ютерів;

N – кількість біт, необхідних для опису К комп’ютерів.

Встановимо адресу мережі : 192.4.1.0. За допомогою масок змінної довжини визначимо діапазони адрес для відділів підприємства (табл. 6).

Таблиця 6 – Розподіл мережевих адрес відділам підприємства

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Сегменти | Відділи | Адреса мережі | К-сть вузл у сегм. | Діапазон доступн адрес | Широк.  адреса | Маска | Неви-користані адреси |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| №1 | Директор та секретар | 192.4.1.0 | 2 | 192.4.1.1  -  192.4.1.6 | 192.4.1.7 | 255.255.255.248 | 4 |
| №2 | Адміністративний відділ | 192.4.1.7 | 5 | 192.4.1.7  -192.4.1.21 | 192.4.1.22 | 255.255.255.240 | 9 |
| №3 | Служба безпеки | 192.4.1.23 | 10 | 192.4.1.24-192.4.1.40 | 192.4.1.41 | 255.255.255.240 | 6 |
| №4 | Фінансовий відділ | 192.4.1.42 | 5 | 192.4.1.43-192.4.1.53 | 192.4.1.54 | 255.255.255.248 | 5 |
| №5 | Технічний відділ | 192.4.1.55 | 6 | 192.4.1.56-192.4.1.66 | 192.4.1.67 | 255.255.255.248 | 4 |
| №6 | Відділ обслуговування | 192.4.1.68 | 4 | 192.4.1.69-192.4.1.79 | 192.4.1.80 | 255.255.255.248 | 6 |

За допомогою програми Cisco Packet Tracer змодельовано структуру мережі підприємства та призначено ІР для кожного комп’ютера мережі (див. рис. 3.1).

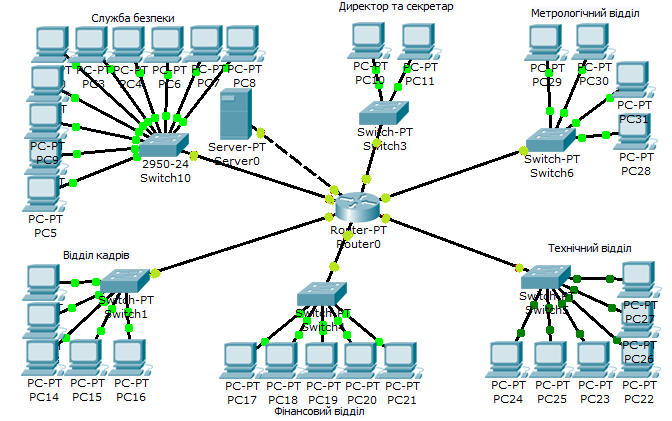


Рисунок 3.1 – Мережа підприємства «Укроптторг»

## Налаштування мережі

Для налаштування мережі необхідно налаштувати порти маршрутизатора та присвоїти комп’ютерам мережі ІР-адреси. Для цього потрібно задати порт, надати йому ІР-адресу та маску підмережі, яка під’єднується до загальної мережі через даний порт (рис. 3.2).

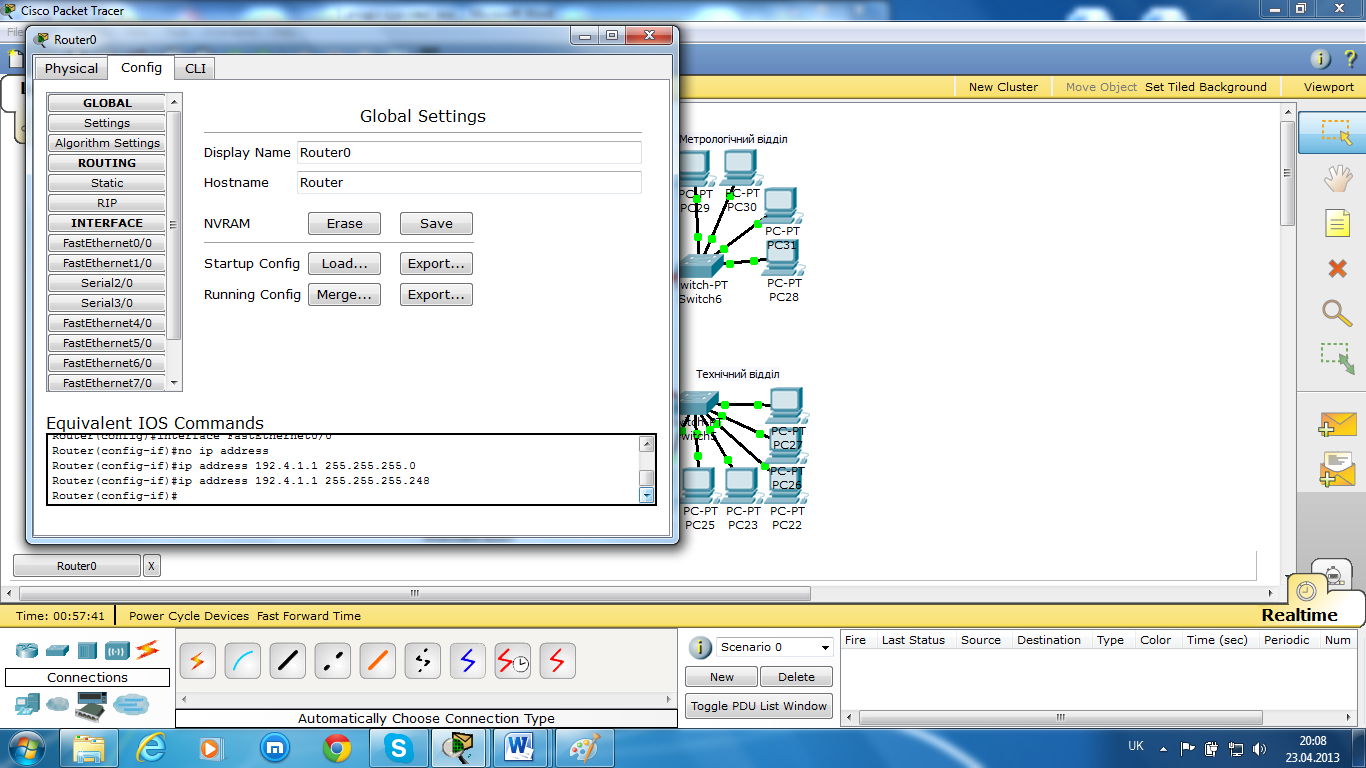


Рисунок 3.2 – Присвоєння порту маршрутизатора ІР та маски під мережі

Для подальшого налаштування мережі – необхідно кожному комп’ютеру надати ІР-адресу та вказати маску підмережі. У більшості випадків маска підмережі встановлюється автоматично після введення ІР-адреси комп’ютера, але в даному випадку її необхідно змінити, оскільки автоматично встановлюється маска постійної довжини для мережі обраного класу і вона не розрахована на розбиття мережі на підмережі із змінними масками (рис. 3.3).

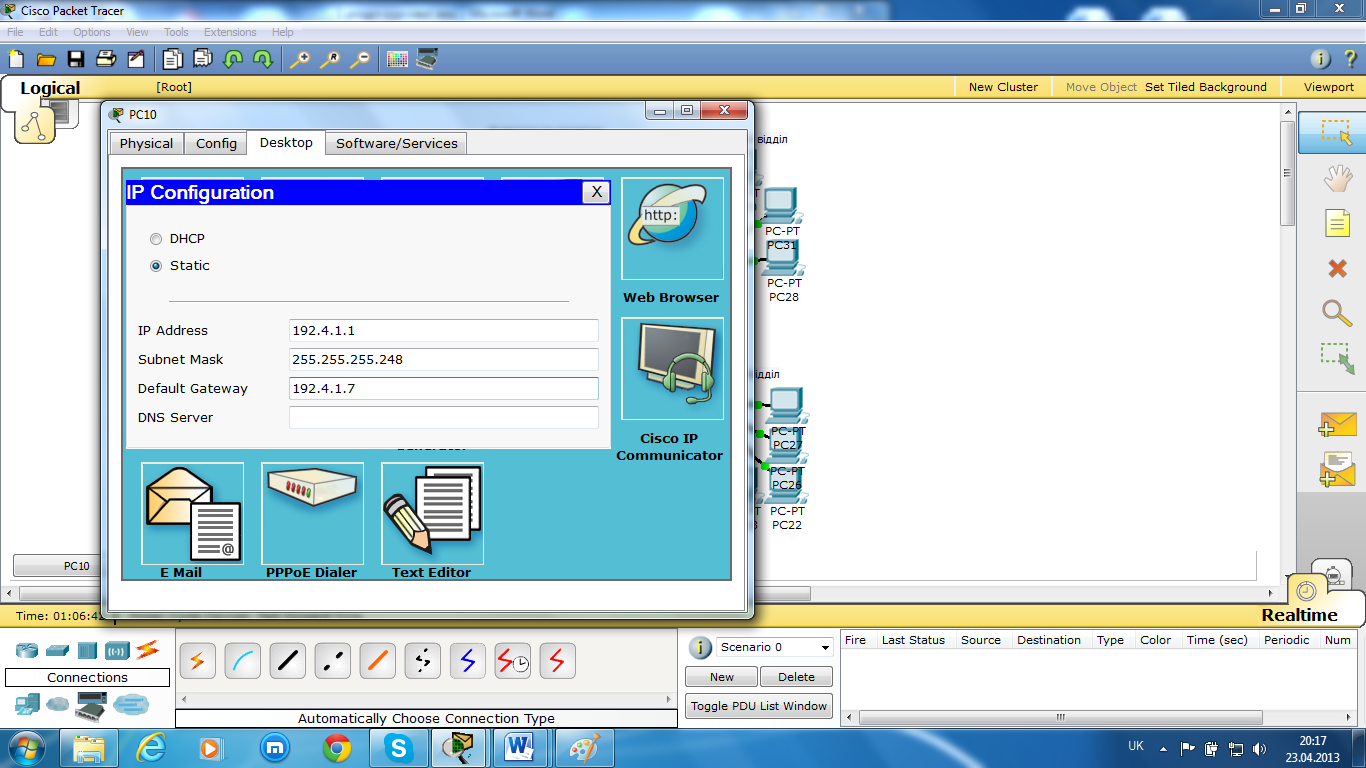


Рисунок 3.3 – Присвоєння ІР-адреси та маски під мережі для комп’ютерів

Таким же чином присвоюються ІР-адреси та вказуються маски зміної довжини для кожного комп’ютера, що знаходиться в підмережі. Кожному порту маршрутизатора присвоюється ІР-адреса та маска зміної довжини, того сегмента під мережі, який під’єднаний до даного порту маршрутизатора.

Отже, змоделювавши мережу та встановивши всі необхідні налаштування для коректної роботи мережі, переходимо до аналізу алгоритму шифрування інформації, яка буде передаватися по даній комп’ютерній мережі та до програмної реалізації.

# ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОМП’ЮТЕРНОЇ МЕРЕЖІ

Постійний розвиток, розширення та підвищенням навантаження на об'єкти комп’ютерних мереж викликає необхідність в адекватних та сучасних засобах моніторингу їх технічного стану для забезпечення гарантоспроможності. У зв’язку з розвитком технологій електронних платежів, "безпаперового" документообігу та інших, збій локальних мереж може паралізувати роботу цілих корпорацій і банків, що призводить до відчутних матеріальних втрат.

Захист даних у комп'ютерних мережах стає однією з найгостріших проблем. На сьогодні сформульовано три базові принципи інформаційної безпеки: цілісність даних - захист від збоїв, що ведуть до втрати інформації, а також неавторизованого створення або знищення даних; конфіденційність інформації; доступність для всіх авторизованих користувачів.

Модель апаратних загроз комп'ютерної мережі виглядає таким чином: збої кабельної системи; перебої електроживлення; побічні випромінювання збої дискових систем; збої систем архівації даних; збої роботи серверів, робочих станцій, мережевих карт і т. д..

## Аналіз застосовуваних методів

Аналіз методів показав, що найбільш ефективним є моніторинг функціонування мережі. Система моніторингу повинна забезпечувати постійне спостереження за станом вузлів комп'ютерної мережі: виконувати перевірку доступності мережевих ресурсів і служб, стежити за роботою серверного і комунікаційного обладнання; у разі порушення нормальної роботи повідомляти адміністратора, використовуючи різні засоби оповіщення.

Крім відправлення повідомлення адміністратору, система моніторингу може бути налаштована таким чином, щоб проводити обробку подій, тобто відмов у роботі елементів мережі та вживати заходів щодо їх усунення шляхом перезапуску будь-якої програми, виконання заданого сценарію і т.п. Ще один аспект - планування розвитку мережі. Корисно мати на руках статистику що відбулися в мережі подій за тривалий період часу. Такого роду дані допомагають у знаходженні вузьких місць, а також дають ясну і вичерпну картину при аналізі і плануванні змін. Детальна інформація про стан сервісів, вузлів, обладнання економить час адміністратора.

## Технічний захист інформації

Також було обрано технічний захист інформації тому, що одним з напрямків захисту інформації в комп'ютерних системах є саме [технічний захист інформації](http://uk.wikipedia.org/wiki/%D0%A2%D0%B5%D1%85%D0%BD%D1%96%D1%87%D0%BD%D0%B8%D0%B9_%D0%B7%D0%B0%D1%85%D0%B8%D1%81%D1%82_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97) ([ТЗІ](http://uk.wikipedia.org/wiki/%D0%A2%D0%97%D0%86)). В свою чергу, питання ТЗІ розбиваються на два великих класи задач:

* захист інформації від несанкціонованого доступу ([НСД](http://uk.wikipedia.org/wiki/%D0%9D%D0%A1%D0%94)) ;
* захист інформації від витоку технічними каналами.

Для того, щоб забезпечити ТЗІ був створений [комплекс технічного захисту інформації](http://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D0%BB%D0%B5%D0%BA%D1%81_%D1%82%D0%B5%D1%85%D0%BD%D1%96%D1%87%D0%BD%D0%BE%D0%B3%D0%BE_%D0%B7%D0%B0%D1%85%D0%B8%D1%81%D1%82%D1%83_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97), що є складовою КСЗІ.

Під НСД звичайно розуміється доступ до [інформації](http://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%8F), що порушує встановлену в [інформаційній системі](http://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0) політику [розмежування доступу](http://uk.wikipedia.org/w/index.php?title=%D0%A0%D0%BE%D0%B7%D0%BC%D0%B5%D0%B6%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F_%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF%D1%83&action=edit&redlink=1). Під технічними каналами розглядаються канали побічних [електромагнітних випромінювань](http://uk.wikipedia.org/w/index.php?title=%D0%95%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BC%D0%B0%D0%B3%D0%BD%D1%96%D1%82%D0%BD%D1%96_%D0%B2%D0%B8%D0%BF%D1%80%D0%BE%D0%BC%D1%96%D0%BD%D1%8E%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F&action=edit&redlink=1) і [наводок](http://uk.wikipedia.org/w/index.php?title=%D0%9D%D0%B0%D0%B2%D0%BE%D0%B4%D0%BA%D0%B8&action=edit&redlink=1), акустичні канали, оптичні канали та інші.

Захист від НСД було здійснюватися в складових інформаційної системи:

* [прикладне](http://uk.wikipedia.org/wiki/%D0%9F%D1%80%D0%B8%D0%BA%D0%BB%D0%B0%D0%B4%D0%BD%D0%B5_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BD%D0%B5_%D0%B7%D0%B0%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%BD%D1%8F) та [системне](http://uk.wikipedia.org/wiki/%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%BD%D0%B5_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BD%D0%B5_%D0%B7%D0%B0%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%BD%D1%8F) [ПЗ](http://uk.wikipedia.org/wiki/%D0%9F%D0%97) (рис. 4.1).



Рисунок 4.1 Класифікація програмного забезпечення.

* апаратна частина [серверів](http://uk.wikipedia.org/wiki/%D0%A1%D0%B5%D1%80%D0%B2%D0%B5%D1%80) та [робочих станцій](http://uk.wikipedia.org/w/index.php?title=%D0%A0%D0%BE%D0%B1%D0%BE%D1%87%D0%B0_%D1%81%D1%82%D0%B0%D0%BD%D1%86%D1%96%D1%8F&action=edit&redlink=1).
* [комунікаційне обладнання](http://uk.wikipedia.org/w/index.php?title=%D0%9A%D0%BE%D0%BC%D1%83%D0%BD%D1%96%D0%BA%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B5_%D0%BE%D0%B1%D0%BB%D0%B0%D0%B4%D0%BD%D0%B0%D0%BD%D0%BD%D1%8F&action=edit&redlink=1) та [канали зв'язку](http://uk.wikipedia.org/w/index.php?title=%D0%9A%D0%B0%D0%BD%D0%B0%D0%BB%D0%B8_%D0%B7%D0%B2%27%D1%8F%D0%B7%D0%BA%D1%83&action=edit&redlink=1).
* [периметр](http://uk.wikipedia.org/wiki/%D0%9F%D0%B5%D1%80%D0%B8%D0%BC%D0%B5%D1%82%D1%80) інформаційної системи.

Також було розроблено ТЗІ від НСД на прикладному і програмному рівнях. Для захисту інформації на рівні [прикладного](http://uk.wikipedia.org/wiki/%D0%9F%D1%80%D0%B8%D0%BA%D0%BB%D0%B0%D0%B4%D0%BD%D0%B5_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BD%D0%B5_%D0%B7%D0%B0%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%BD%D1%8F) та [системного](http://uk.wikipedia.org/wiki/%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%BD%D0%B5_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BD%D0%B5_%D0%B7%D0%B0%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D1%87%D0%B5%D0%BD%D0%BD%D1%8F) ПЗ нами використовуються:

* системи розмежування доступу до інформації;
* системи ідентифікації та [автентифікації](http://uk.wikipedia.org/wiki/%D0%90%D0%B2%D1%82%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D1%96%D0%BA%D0%B0%D1%86%D1%96%D1%8F);
* системи [аудиту](http://uk.wikipedia.org/wiki/%D0%90%D1%83%D0%B4%D0%B8%D1%82) та [моніторингу](http://uk.wikipedia.org/wiki/%D0%9C%D0%BE%D0%BD%D1%96%D1%82%D0%BE%D1%80%D0%B8%D0%BD%D0%B3);
* системи [антивірусного захисту](http://uk.wikipedia.org/w/index.php?title=%D0%90%D0%BD%D1%82%D0%B8%D0%B2%D1%96%D1%80%D1%83%D1%81%D0%BD%D0%B8%D0%B9_%D0%B7%D0%B0%D1%85%D0%B8%D1%81%D1%82%D1%83&action=edit&redlink=1).

Для захисту інформації на рівні апаратного забезпечення було використано:

* [апаратні ключі](http://uk.wikipedia.org/w/index.php?title=%D0%90%D0%BF%D0%B0%D1%80%D0%B0%D1%82%D0%BD%D1%96_%D0%BA%D0%BB%D1%8E%D1%87%D1%96&action=edit&redlink=1).
* системи [сигналізації](http://uk.wikipedia.org/w/index.php?title=%D0%A1%D0%B8%D0%B3%D0%BD%D0%B0%D0%BB%D1%96%D0%B7%D0%B0%D1%86%D1%96%D1%8F&action=edit&redlink=1).
* засоби [блокування](http://uk.wikipedia.org/wiki/%D0%91%D0%BB%D0%BE%D0%BA%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F) [пристроїв](http://uk.wikipedia.org/wiki/%D0%9F%D1%80%D0%B8%D1%81%D1%82%D1%80%D1%96%D0%B9) та [інтерфейс](http://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%82%D0%B5%D1%80%D1%84%D0%B5%D0%B9%D1%81) [вводу-виводу інформації](http://uk.wikipedia.org/w/index.php?title=%D0%92%D0%B2%D1%96%D0%B4-%D0%B2%D0%B8%D0%B2%D1%96%D0%B4_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97&action=edit&redlink=1).

Для ТЗІ на мережевому рівні було використано такі засоби мережевого захисту інформації (рис. 4.2):

* [міжмережеві екрани](http://uk.wikipedia.org/wiki/%D0%9C%D1%96%D0%B6%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D0%B5%D0%B2%D0%B8%D0%B9_%D0%B5%D0%BA%D1%80%D0%B0%D0%BD) ([англ.](http://uk.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0_%D0%BC%D0%BE%D0%B2%D0%B0) Firewall) — для блокування атак з зовнішнього середовища. Вони керують проходженням мережевого [трафіку](http://uk.wikipedia.org/wiki/%D0%A2%D1%80%D0%B0%D1%84%D1%96%D0%BA) відповідно до правил захисту. Як правило, міжмережеві екрани встановлюються на вході мережі і розділяють [внутрішні (приватні)](http://uk.wikipedia.org/wiki/VPN) та зовнішні (загального доступу) мережі.
* [системи виявлення втручаннь](http://uk.wikipedia.org/w/index.php?title=IDS&action=edit&redlink=1) ([англ.](http://uk.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0_%D0%BC%D0%BE%D0%B2%D0%B0) Intrusion Detection System) — для виявлення спроб несанкціонованого доступу як ззовні, так і всередині мережі, захисту від атак типу [«відмова в обслуговуванні»](http://uk.wikipedia.org/w/index.php?title=%D0%92%D1%96%D0%B4%D0%BC%D0%BE%D0%B2%D0%B0_%D0%B2_%D0%BE%D0%B1%D1%81%D0%BB%D1%83%D0%B3%D0%BE%D0%B2%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%96&action=edit&redlink=1). Використовуючи спеціальні механізми, системи виявлення вторгнень здатні попереджувати шкідливі дії, що дозволяє значно знизити час простою внаслідок атаки і витрати на підтримку працездатності мережі.
* [засоби створення віртуальних приватних мереж](http://uk.wikipedia.org/wiki/VPN) ([англ.](http://uk.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0_%D0%BC%D0%BE%D0%B2%D0%B0) Virtual Private Network(VPN)) — для організації захищених каналів передачі даних через незахищене середовище. [Віртуальні приватні мережі](http://uk.wikipedia.org/wiki/%D0%92%D1%96%D1%80%D1%82%D1%83%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0_%D0%BF%D1%80%D0%B8%D0%B2%D0%B0%D1%82%D0%BD%D0%B0_%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D0%B0) забезпечують прозоре для користувача сполучення [локальних мереж](http://uk.wikipedia.org/wiki/%D0%9B%D0%BE%D0%BA%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0_%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D0%B0), зберігаючи при цьому [конфіденційність](http://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BD%D1%84%D1%96%D0%B4%D0%B5%D0%BD%D1%86%D1%96%D0%B9%D0%BD%D1%96%D1%81%D1%82%D1%8C) та цілісність інформації шляхом її [динамічного шифрування](http://uk.wikipedia.org/w/index.php?title=%D0%94%D0%B8%D0%BD%D0%B0%D0%BC%D1%96%D1%87%D0%BD%D0%B5_%D1%88%D0%B8%D1%84%D1%80%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F&action=edit&redlink=1).
* [засоби аналізу захищеності](http://uk.wikipedia.org/w/index.php?title=%D0%97%D0%B0%D1%81%D0%BE%D0%B1%D0%B8_%D0%B0%D0%BD%D0%B0%D0%BB%D1%96%D0%B7%D1%83_%D0%B7%D0%B0%D1%85%D0%B8%D1%89%D0%B5%D0%BD%D0%BE%D1%81%D1%82%D1%96&action=edit&redlink=1) — для аналізу захищеності [корпоративної мережі](http://uk.wikipedia.org/wiki/%D0%9A%D0%BE%D1%80%D0%BF%D0%BE%D1%80%D0%B0%D1%82%D0%B8%D0%B2%D0%BD%D0%B0_%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D0%B0) та виявлення можливих каналів реалізації загроз інформації ([Symantec Enterprise Security Manager](http://uk.wikipedia.org/w/index.php?title=Symantec_Enterprise_Security_Manager&action=edit&redlink=1),[Symantec NetRecon](http://uk.wikipedia.org/w/index.php?title=Symantec_NetRecon&action=edit&redlink=1)). Їх застосування дозволяє попередити можливі атаки на корпоративну мережу, оптимізувати витрати на захист інформації та контролювати поточний стан захищеності мережі.

Захист інформації від її витоку технічними каналами зв'язку було забезпечено такими засобами та заходами:

* використанням [екранованого кабелю](http://uk.wikipedia.org/wiki/%D0%9A%D0%B0%D0%B1%D0%B5%D0%BB%D1%8C) та прокладка [проводів](http://uk.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B2%D1%96%D0%B4) та кабелів в екранованих конструкціях;
* встановленням на [лініях зв'язку](http://uk.wikipedia.org/w/index.php?title=%D0%9B%D1%96%D0%BD%D1%96%D1%8F_%D0%B7%D0%B2%27%D1%8F%D0%B7%D0%BA%D1%83&action=edit&redlink=1) [високочастотних фільтрів](http://uk.wikipedia.org/w/index.php?title=%D0%92%D0%B8%D1%81%D0%BE%D0%BA%D0%BE%D1%87%D0%B0%D1%81%D1%82%D0%BE%D1%82%D0%BD%D0%B8%D0%B9_%D1%84%D1%96%D0%BB%D1%8C%D1%82%D1%80&action=edit&redlink=1);
* побудовою [екранованих приміщень](http://uk.wikipedia.org/w/index.php?title=%D0%95%D0%BA%D1%80%D0%B0%D0%BD%D0%BE%D0%B2%D0%B0%D0%BD%D0%B5_%D0%BF%D1%80%D0%B8%D0%BC%D1%96%D1%89%D0%B5%D0%BD%D0%BD%D1%8F&action=edit&redlink=1) («капсул»);
* використанням екранованого обладнання;
* встановленням [активних систем зашумлення](http://uk.wikipedia.org/wiki/%D0%A1%D1%82%D0%B0%D0%BD%D1%86%D1%96%D1%8F_%D0%B0%D0%BA%D1%82%D0%B8%D0%B2%D0%BD%D0%B8%D1%85_%D0%BF%D0%B5%D1%80%D0%B5%D1%88%D0%BA%D0%BE%D0%B4);
* створенням [контрольованої зони](http://uk.wikipedia.org/w/index.php?title=%D0%9A%D0%BE%D0%BD%D1%82%D1%80%D0%BE%D0%BB%D1%8C%D0%BE%D0%B2%D0%B0%D0%BD%D0%B0_%D0%B7%D0%BE%D0%BD%D0%B0&action=edit&redlink=1).



Рисунок 4.2 – Технічні засоби захисту інформації.

# РЕАЛІЗАЦІЯ ЗАХИСТУ

## Вибір міжмережевого екрана

На сьгоднішній день ринок програмного забезпечення пропонує нам досить великий вибір міжмережевих екранів, тому розглянемо найбільш популярні з них (порівняння наведено в табл. 5.1).

Таблиця 5.1 – Порівняння міжмережевих екранів

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Мережевий  екран  Характеристики | PC Tools Firewall Plus | Agnitum Outpost Firewall Pro | AGAVA Firewall | Comodo Firewall |
| Блокування мережевого трафіку одним клацанням миші, у разі виявлення активного шкідливого коду. | + | + | - | + |
| Веб-фільтр | + | + | + | + |
| Проактивний захист; | + | + | + | + |
| Створення правил мережевого доступу для відомих програм на основі попередніх налаштувань | - | + | - | + |
| Захист від переповнення буфера; | - | + | - | + |
| Захист від несанкціонованого доступу; | + | + | + | + |
| Захист важливих системних файлів і записів реєстру від внутрішніх атак | - | + | + | + |
| Виявлення переповнення буфера, яке відбувається в HEAP пам'яті; | - | - | + | - |
| Захист від спаму |  |  |  |  |
| Захист від інтернет-атак | - | - | + | + |
| Захист від фішингу | + | + | + | - |
| Фільтрація вхідних і вихідних мережевих з'єднань. | + | + | - | + |

Отже, проаналізувавши деякі мережеві екрани можна зробити висновок, що для даного підприємства буде доцільно використати міжмережевий екран Comodo Firewall. Даний програмний програмний продукт містить у собі проактивний захист, що включає в себе HIPS (англ. запобігання вторгнень хост-систем) - система відображення локальних загроз. Завданням HIPS є контроль за роботою додатків і блокування потенційно небезпечних операцій за заданими критеріями. Також значною перевагою даного мережевого екрану є те, що він знаходиться в безкоштовному розповсюдженні і за функціональними можливостями не поступається іншим міжмережевим екранам. Comodo Firewall протестовано сайтом Firewall Chellenge від 30 березня 2008 висунуто на перше місце.

## Аналіз систем виявлення вторгнень

Системи виявлення вторгнення (СВВ) - це системи, що збирають інформацію з різних точок захищається комп'ютерної системи (обчислювальної мережі) і аналізують цю інформацію для виявлення як спроб порушення, так і реальних порушень захисту.

СВВ - це один із засобів хорошою архітектури забезпечення безпеки мережі і багаторівневої стратегії її захисту. Вони мають свої переваги і недоліки, розвинути перші і згладити останні можна, застосовуючи IDS в комплексі з іншими засобами забезпечення безпеки інформації. У IDS є деякі перекриття виконуваних функцій, особливо з міжмережевим екранами, які вже виконують деякі обмежені функції виявлення вторгнень, піднімаючи тривогу, коли «спрацьовує» відповідне правило. IDS унікальні в тому, що на відміну від МЕ, що виконують безліч різних функцій (фільтрація пакетів, аутентифікація користувачів, кешування і т.д.), у них реалізована всього одна функція, але реалізована добре.

Таблиця 5.2. – Порівняльна характеристика СВВ

|  |  |  |  |
| --- | --- | --- | --- |
| СВВ    Характеристики | Snort | [IBM ISS Proventia IDS](http://www-01.ibm.com/software/tivoli/products/security-network-intrusion-prevention/) | [AntiBdoor](http://ru.wikipedia.org/wiki/Bro) |
| Консоль управління, що дозволяє конфігурувати СВВ, спостерігати за станом захищається системи, переглядати виявлені підсистемою аналізу інциденти | - | + | + |
| Підсистему аналізу, призначену для виявлення мережевих атак і підозрілих дій; | - | + | + |
| Не впливають на продуктивність і топологію мережі. | + | + | + |
| Сенсорна підсистема, призначену для збору подій, пов'язаних з безпекою мережі, що захищається або системи; | - | + | + |
| Сховище, в якому накопичуються первинні події та результати аналізу; | + | + | + |
| Ефективне визначення атак і відсутність великої кількості помилкових повідомлень | + | + | + |
| Надійна діагностика використання конкретного інструментального засобу або технології атаки. | + | - | + |

Для підприємства ТОВ «Укроптторг» було обран симу виявлення втогнень [AntiBdoor](http://ru.wikipedia.org/wiki/Bro) - це хостова система виявлення вторгнень (HIDS), вільно розповсюджується з відкритим вихідним кодом. Вона веде аналіз системних логів, перевірку цілісності, спостереження за реєстром ОС Windows, виявлення руткітів, оповіщення в заданий час або, якщо буде виявлено яку - небудь подію. Вона надає функцію виявлення вторгнень для більшості операційних систем, включаючи Linux, OpenBSD, FreeBSD, Mac OS X, Solaris і Windows. Її кроссплатформена архітектура дозволяє легко управляти і спостерігати відразу за декількома операційними системами.

## Аналіз антивірусних програм

Антивірусна програма (антивірус) — [програма](http://uk.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%B0) для знаходження і лікування програм, що заражені комп'ютерним вірусом, а також для запобігання зараження [файлу](http://uk.wikipedia.org/wiki/%D0%A4%D0%B0%D0%B9%D0%BB) вірусом.

На даний момент антивірусне програмне забезпечення розробляється, в основному, для ОС сімейства Windows від компанії Microsoft, що викликано великою кількістю шкідливих програм саме під цю платформу (а це, у свою чергу, викликане великою популярністю цієї ОС, так само, як і великою кількістю засобів розробки, в тому числі безкоштовних і навіть «інструкцій з написання вірусів»). На даний момент на ринок виходять продукти і для інших операційних систем, таких, наприклад, як Linux і Mac OS X. Це викликано початком розповсюдження комп'ютерних вірусів і під ці платформи, хоча UNIX-подібні системи традиційно користуються репутацією більш стійких до впливу шкідливих програм.

Розглянемо порівняльну характеристику антивірусних програм за десятибальною шкалою.

Таблиця 5.3 – Порівняльна характеристика антивірусних програм

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Продукт  Характеристика | Symantec Endpoint Protection | ESET NOD32 | Avast | Norton AntiVirus |
| Кількість успішно проведених тестів VB [100%](http://ua-referat.com/100_%D0%B1%D0%B0%D0%B7%D0%BE%D0%B2%D0%B8%D1%85_%D1%84%D1%96%D0%BB%D0%BE%D1%81%D0%BE%D1%84%D1%81%D1%8C%D0%BA%D0%B8%D1%85_%D0%BF%D0%BE%D0%BD%D1%8F%D1%82%D1%8C) за 2010-2011р | 4 | 10 | 11 | 9 |
| Загальний рівень виявлення шкідливого програмного забезпечення | 91.40% | 97.68% | 94.42% | 95.63% |
| Середній час реакції на нові загроз, годинник | 6-8 | 0-2 | 4-6 | 1-4 |
| Лікування активного зараження | 79% | 69% | 20% | 63% |
| Займана оперативна пам'ять у звичайному режимі роботи, кВ | 6543 | 4500 | 22355 | 7661 |
| Час сканування даних, хв. | 77 | 29 | 25 | 32 |
| Кількість відсканованих даних | 129746 | 126823 | 123724 | 124762 |
| Усереднена по всіх тестів рейтинг антивірусів (чим менше, тим краще) | 7,83 | 2,36 | 4,75 | 3,55 |

За даними таблиці видно, що в одних антивірусів виграшним виявляється один показник, в інших - інший. При цьому [природно](http://ua-referat.com/%D0%9F%D1%80%D0%B8%D1%80%D0%BE%D0%B4%D0%B0), що в своїх рекламних [матеріалах](http://ua-referat.com/%D0%9C%D0%B0%D1%82%D0%B5%D1%80%D1%96%D0%B0%D0%BB%D0%B8) розробники антивірусів роблять акцент тільки на ті тести, де їхні продукти займають лідируючі позиції.

Отже розглянувши порівняльну таблицю антивірусних програм можна зробити висновок, що доцільним для підприємства буде використання антивірусної програми «ESET NOD32».

# ВИСНОВКИ

У ході виконання курсового проекту розглянуто структуру підприємства «Укроптторг», визначено основні відділи та функції кожного з них. Проаналізовано наявність інформаційних ресурсів різного типу, визначено рівні та права доступу до них, створено карту інформаційних потоків організації, визначено матеріальні ресурси організації.

Розглянуто можливі загрози для комп’ютерної мережі даної організації. Для кожного методу описано можливі найбільш дієві методи захисту. На їх основі обирається найкращий, згідно якого і розроблено програмний продукт.

Також описано принцип побудови мережі організації. Для мережі обрано адресу класу С. Адресний простір розподілено за методом із змінними масками, для економії адресного простору. Мережу налаштовано згідно із проведеними розрахунками.

Розроблено захист мережі, який реалізує повний захист підприємства.

* Отже, створено КСЗІ, що дозволяє безпечно зберігати та передавати інформацію в середині мережі і за її межами.

# ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Організація безпеки на підприємстві // http:// www. experts. in.ua/ baza/ analitic/index.php?ELEMENT\_ID=62147
2. Андрончик А.Н. Защита информации в компьютерных сетях. Практический курс\ Андрончик А.Н., Богданов В.В., Домуховский Н.А – Екатеренбург, 2009. - 248с.
3. Романцев Ю.В. Захист інформації в комп’ютерних системах і мережах. Радіо і связь.\ Романцев Ю.В., Тимофеєєв П.А, Шальгін В.Ф., 2001. – 376с.
4. Доценко С.М. Комплексная информационная безопасность объекта: от теории к практике.\ Доценко С.М. , Шпак В.Ф. – «Издательство Полигон», 2000, - 130с.
5. В.Г. Олифер, Н.А. Компьютерные сети. Принципы, технологии, протоколы\ В.Г. Олифер, Н.А. Олифер – ПИТЕР, 2007.
6. Галицкий А. В. Защита информации в сети – анализ технологий и синтез решений.\ Галицкий А. В., Рябко С. Д., Шаньган В. Ф. – М.: ДМК Пресс, 2004. – 616 с.: ил.
7. Норткатт С. Обнаружение вторжений в сеть.\ Норткатт С., Новак Д., Маклахлен Д. – Издательство "ЛОРИ", 2001, – 384 с.
8. Гэри М. Вычислительные машины и турднорешаемые задачи\ Гэри М., Джонсон Д. – Москва: Мир. 1982.
9. T. ElGamal. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. IEEE Trans. Inform. Theory. V. 31. P. 469-472. 1985.