МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
КАФЕДРА КОМП'ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
_____ С.В. Казмірчук
«_____»_____ 20__ р.

На правах рукопису
УДК 004.056.5:510.22(043.3)

ДИПЛОМНА РОБОТА

ЗДОБУВАЧА ВИЩОЇ ОСВІТИ
ОСВІТНЬОГО СТУПЕНЯ «БАКАЛАВР»

Тема: Система забезпечення конфіденційності інформації, що передається по локальній комп'ютерній мережі підприємства

Виконавець: І.В. Олійник
Керівник: к.т.н., доцент С.В. Єгоров
Нормоконтролер: к.т.н., доцент С.В. Єгоров

Київ 2021

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет: Кібербезпеки, комп'ютерної та програмної інженерії

Кафедра: Комп'ютеризованих систем захисту інформації

Освітній ступінь: Бакалавр

Спеціальність: 125 «Кібербезпека»

Освітньо-професійна програма: «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ С.В. Казмірчук

«__» _____ 20__ р.

ЗАВДАННЯ

на виконання дипломної роботи

здобувача вищої освіти Олійника Івана Вячеславовича

1. Тема: *Система забезпечення конфіденційності інформації, що передається по локальній комп'ютерній мережі підприємства* затверджена наказом в.о. ректора від « » _____ 2021 р. №_____.
2. Термін виконання: з р. по р.
3. Вихідні дані: проаналізувати існуючі системи та методики аналізу і оцінки ризиків інформаційної безпеки; на основі аналізу виділити вхідні і вихідні параметри, завдяки яким можливо провести порівняння існуючих систем, виявлення їх переваг і недоліків;
4. Зміст пояснювальної записки: аналіз існуючих систем та методик аналізу і оцінки ризиків інформаційної безпеки; розробка методики системи аналізу та оцінки ризиків на основі нечіткої логіки; розробка програмного забезпечення запропонованої системи, верифікація отриманих результатів.

КАЛЕНДАРНИЙ ПЛАН

виконання дипломної роботи

№ п/п	Етапи виконання дипломної роботи	Термін виконання етапів	Примітка
1.	Уточнення постановки задачі	19.04.2021	*Виконано*
2.	Аналіз літературних джерел		*Виконано*
3.	Обґрунтування вибору рішення		*Виконано*
4.	Збір інформації		*Виконано*
5.	Дослідження сучасних систем і методик аналізу та оцінки ризиків інформаційної безпеки		*Виконано*
6.	Розробка методики та структури системи аналізу та оцінки ризиків інформаційної безпеки		*Виконано*
7.	Перевірка на антиплагіат		*Виконано*
8.	Оформлення і друк пояснювальної записки		*Виконано*
9.	Оформлення презентації		*Виконано*
10.	Отримання рецензій від рецензента		*Виконано*

Здобувач вищої освіти І. Олійник

(підпис, дата)

Керівник дипломної роботи С. Єгоров

(підпис, дата)

РЕФЕРАТ

Дипломна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, додатків і має 78 сторінки основного тексту. Список використаних джерел містить 38 найменування і займає сторінок. Загальний обсяг роботи 95 сторінок.

Метою роботи є підвищення рівня захищеності ІКС за рахунок аналізу і оцінки ризиків інформаційної безпеки.

В роботі вирішено задачу побудови системи аналізу і оцінки ризиків інформаційної безпеки на основі експертних думок відповідно до вимог НД ТЗІ та інших нормативно-правових документів, сформованих в умовах нечіткості.

В роботі розроблено алгоритм для аналізу та оцінки ризиків інформаційної безпеки на основі ідентифікації активів та загроз, визначенні значень ключових оцінюючих компонентів та ступеню ризику.

Розроблений метод відносяться до галузі інформаційної безпеки і можуть бути використані для підвищення рівня захищеності.

Можливі напрямки розвитку цієї роботи пов’язані із розширенням моделі і алгоритму програмного забезпечення відповідно до вимог міжнародних стандартів, наприклад ISO 27001, для більш повного аналізу та оцінки ризиків.

Ключові слова: ризик, система аналізу і оцінки ризиків, інформаційна безпека, інформаційно-комунікаційна система, функція належності, нечіткі актив, загроза, оцінюючі компоненти, ступінь ризику.

ВСТУП

Актуальність теми Актуальність досліджуваної проблеми полягає в тому, що з розвитком конкуренції значного поширення набули такі злочини, як викрадання інформації через комп'ютерні мережі і прослуховування ліній зв'язку. Тому знання потенційних загроз, причин та умов скоєння таких злочинів дозволить працівникам підрозділів служб безпеки підприємств у межах своєї компетенції здійснити заходи, що стануть перешкодою на шляху до зло- вмисних замахів на інформаційні ресурси та потоки господарюючого суб'єкта. Запропонована нами система захисту об'єктів інформації комп'ютерних мереж від незаконного відтоку інформації, а також охорони комерційної таємниці ґрунтується на законодавстві України, наукових розробках українських спеціалістів у сфері інформаційної безпеки та набутому підприємствами досвіді.

Об'єкт дослідження – забезпечення конфіденційності інформації, що передається по локальній комп'ютерній мережі підприємства

Предмет дослідження – технології та механізми захисту конфіденційності інформації

Мета роботи – Розробка системи захисту інформації підприємства та їх програмного забезпечення.

Завдання бакалаврської роботи:

- проаналізувати існуючі типи атак на втрату конфіденційності компаній в їх програмних додатках;
- Створення локальной мережі
- Передача данних запропованованим методом
- Передача данних повина відбуватися з використанням шиврування
- виокремити основні технології та механізми захисту комп'ютерних мереж ;

- дослідити можливість поєднання встановлених технологій та механізмів виявлення та протидії атакам у рекомендації, які дійсно допоможуть компаніям не втратити свої кошти та час

Методи дослідження – аналіз експлуатаційної документації, звітів світових конференцій та засад з інформаційної безпеки, теорія машинного навчання, теорія корпоративних інформаційних систем та проведення досліджень з використанням спеціалізованого ПЗ.

Ступінь новизни одержаних результатів. проектування організаційно-функціональної підсистеми інформаційної безпеки підприємства і її ресурсного забезпечення.

Галузь використання – інформаційна безпека.

ЗМІСТ

1 ЗАХИСТ ОБ’ЄКТІВ ІНФОРМАЦІЇ, ІНФОРМАЦІЙНИХ СИСТЕМ ПІДПРИЄМСТВ, УСТАНОВ ТА ОРГАНІЗАЦІЙ ВІД ПРОТИПРАВНИХ ПОСЯГАНЬ

1.1 **Інформаційна система підприємства**

Ефективний працівник компанії (організації) - це те, що неможливо без ресурсів, які можна використати для досягнення мети. З загальної точки зору управлінської літератури поняття ресурсів поширюється не тільки на людей, капітал, сировину, а й на інформацію. Суть об'єктивних показників компанії відсутня у визначенні ключових ресурсів та перетворенні їх на ефективні продукти . Сьогодні, не лише теоретично, а й багаторічна практика, відомо, що природні ресурси та соціальна інформація завжди обмежені.

Потреба в інформації набагато більша, ніж здатність реагувати. Справа в тому, що процес комерціалізації потенційної інформації постійно оновлюється, що означає , що вона є необхідною , щоб скористатися в момент , коли необхідно приймати управлінські рішення, такі , як про укладення в договорі. Для задоволення інформаційних потреб компанії необхідно створити найбільш відповідну структуру з визначенням вимог до інформаційної безпеки. В принципі, важливо, щоб інформаційна структура пропорційна розподілу можливостей компанії, а інформація, необхідна для вирішення проблем, передавалась у відділи не будь-кому, а лише відповідальним. Інформаційна структура повинна бути розроблена з урахуванням потреб усіх рівнів корпоративного управління. Такий підхід дозволяє йому точно і ефективно вирішити проблему створення корпоративної мережі всередині компанії (агентства).

Взаємозв’язана мережа (агентство)- це організація зв’язку інформаційної системи компанії через глобальну мережу мереж, тобто обмін інформацією між кількома комп’ютерами, розташованими на дуже великій відстані один від одного, залежно від локальної мережі. Важливо пам’ятати, що інформація принципово відрізняється від інших типів ресурсів компанії, тобто її дані свідчать про безперебійну поведінку двох компаній і за її межами. Зміст керівництва компанії багато в чому залежить від змісту та способів отримання

інформації. Інформація про сировину, фінансові інструменти , процеси наукової літератури для визначення так званого управління безпекою. З іншого боку, сама інформація є досить специфічним типом , тому для досягнення цієї мети необхідно впливати на процеси збору, зберігання, розповсюдження та використання даних на організаційному рівні за допомогою відповідних механізмів .

У цьому випадку інформація є об'єктом контролю. Багатогранний доступ до джерел інформації вимагає важливого чинника, який слід розглядати як бізнес - функцію в ринкових відносинах та ситуаціях , що є відмінною рисою у боротьбі між незалежністю ринку та управлінням агенціями та виробництвом жорсткої конкуренції. Боротьба за фінансову безпеку - це ринкове право. Забезпечення торгівлі у формі ситуативних ринкових відносин вимагає захисту інформації приватного бізнесу. Література сприймається як умова, що сприяє або створює перешкоду для досягнення практичного результату (прибутку) від економічної діяльності [45, 55-56]. Комерційна інформація, яка створює належні умови для суб'єкта господарювання приймати оперативні рішення та досягати ефективних результатів , вважається корисною. Щоб захистити незнайомця, щоб не втратити сподівання, зазвичай використовується набір технічних та організаційних прийомів . Комерційна інформація існує на ринку конкурентно - діяльність, що здійснюється в рамках діяльності, поділяється на видавничу , технічну , комерційну, фінансову, також має інформацію про потреби та конкуренцію, чинне законодавство, державні злочини , включаючи інформацію про структури, повноваження та методи інформації компанії з мережевої безпеки тощо [75]. Інформація про діяльність компанії зберігається у різних форматах: людська пам’ять, картотеки, книги, комп’ютерні пристрої зберігання даних тощо. Потрібно вирішити деякі питання, пов’язані з використанням практичних методів зберігання, виготовлення , проектування та відновлення даних [60] . Інформаційні структури повинні бути організаційна структура управління, але не обов'язково повинні бути ідентифіковані . Рішення полягає в тому, що метою архітектурних послуг є додавання різноманітних ресурсів, а система інформаційного потоку лише досягає своїх цілей. Важливим напрямком технологій управління є інформаційний центр - потенційне джерело інформації, необхідне для успіху його діяльності. Існують суміжні технології, що

діють (технологія виробництва), але вони відрізняються своїми характеристиками .

Технологія управління забезпечує спосіб управління компанією (агенцією) . Поглиблено розуміючи технологію управління, важливо наголосити на її складових. До них належать: інформація, функціонування та методи управління асиміляцією, технологія, праця, обладнання , структура [55]. Важливо пам’ятати, що підрозділи, які є частиною бізнес-інфраструктури компанії, взаємопов’язані через рішення щодо житла та обслуговування. В цілому , структурна цілісність його змісту є змістом для компанії в зв'язку з необхідністю , щоб отримати інтегровану в технічний процес. На наш погляд , пояснення в цих ситуаціях важливі з точки зору пояснення важливості інформаційної безпеки в корпоративній мережі, оскільки велика кількість компаній має доступ до Інтернету. Це, безумовно, добре, з одного боку, а з іншого боку, усі країни світу мають доступ до мережі місцевих компаній. Найсучасніше обладнання - це управління комп’ютерними технологіями та комп’ютерні методи зв’язку. До них належать: • Технічні методи обробки даних та захисту ланцюгів (запис, передача, пошук, обробка даних); • Інформатори - об'єкти, що передають інформацію. Близьке до поняття інформації місцеположення в телекомунікаційній компанії , тобто, частина з bay'adeeda і здібності, за допомогою використання або контролю значень, для управління інформаційними системами, включаючи можливі оновлення системи. Однак сферу комунікацій компанії можна значно розширити за рахунок інтеграції з іншими інформаційними системами (наприклад, Інтернетом). Слід зазначити, що сьогодні технологія управління інформацією не має реальної альтернативи зберігання магнітної інформації . Інформаційні системи, основні об'єкти, що є комп'ютером, основна інформація зберігається на жорстких магнітних дисках . Він розташований на жорсткому диску (HDD), де операційна система зберігає та передає оперативну пам’ять на комп’ютер, дані обробляються під час її використання та видаляються користувачем. Одним з найбільш важливих показників - Енергетична незалежність робить жорсткий диск без зміни ефективна і в протягом тривалого часу для зберігання великих обсягів даних. Машини

для зберігання на жорсткому диску широко відомі як жорсткі диски. Слід зазначити, що в наш час велика кількість інформації зберігається, обробляється та передається електронними засобами і як така супроводжується електромагнітним випромінюванням .

На даний момент операційна система комп’ютера не працює самостійно . На окремих комп’ютерах інформація обробляється та зберігається, а також окреме підключення або підключення до Всесвітньої павутини та передача даних (обмін інформацією). Локальна мережа виконує всю роботу з інформацією : зберігання, обробка та передача. Персональний комп’ютер є центральним ланкою в системі обробки інформації автоматично і привертає увагу конкурентів, злочинців та спецслужб [54, 20-24]. Для отримання цінної інформації вони використовують усі існуючі інструменти та методи , включаючи різні типи аналітиків ліній електропередач. Таким чином, більшість вимог безпеки строгих даних повинні бути встановлені для комп'ютерів в локальній мережі, все які мають елементи , пов'язані з системою кабелем (як правило , захищеними або не пов'язаної парою). Зараз неможливо використовувати локальну комп’ютерну мережу самостійно без взаємодії з іншими мережами. .

1.2 Загальнотеоретичні характеристики окремих напрямів захисту від перехоплення інформації, що обертається у локальних та корпоративних мережах установ і підприємств

Розвиток і використання в них комп’ютерних технологій у багатьох сферах економіки в даний час є однією з основних причин її ефективності. Однак досягнення в галузі інформаційних технологій створили потенційні загрози у вигляді нових розробок та змін та методів, які раніше називали науковим шпигунством, що дозволяють швидко отримати доступ до необхідної інформації з комп'ютера .

Збір інформації про розвиток високих технологій завжди був і залишається головним пріоритетом у світі інтелекту. Тому все частіше використовуються методи отримання інформації, перевірені на практиці учасниками науково-практичної конференції, організаторами виставки та кадровою службою .

Шифрування конфіденційної інформації, яка обробляється за допомогою комп’ютерних технологій і передається по лініях клієнтів , здійснюється за допомогою портативних патрульних радіостанцій і забезпечує безліч режимів прийому, доступних у різних напрямках та на різних хвилях. інший. Ця форма радіодосліджень є більш поширеною [89, 70]. Хоча слід зазначити, що арсенал конкретних технічних методів і прийомів, що використовуються для викрадення інформації з інформаційних систем компаній, установ, корпорацій, досить широкий. Ви можете знайти інформаційну цінність у конкуруючих компаніях , підключившись до комп’ютерної системи (включаючи зображення та аудіофайли) за допомогою спеціальної програми - токенів для передачі секретних даних у отриманих файлах. Програма дозволяє не тільки безпечно приховати факт передачі повідомлення, але і зберегти його за допомогою алгоритму. Такі профілактичні методи, як контрацепція, мають певний інтерес у захисті конфіденційного екрану монітора за допомогою електромагнітних хвиль випромінювання, що виникають під час фундаментальної роботи [28]. Якщо інспектор не завжди може увійти в офіційну відео , тому що він встановлений, ви не можете бачити екран, і очей для отримання інформації по - , як і раніше можливо, але від інспектора з світлового випромінювання .

Екран відеомонітора з безліччю оглядів з різних аспектів (стіни, стелі, меблі та інші предмети) може переходити до спеціального пристрою, що дозволяє перемикати потік інформації у світлі

відео. Поєднання символів, задіяних у відеомоніторі Сонце, є перешкодою, наприклад, зображення випускника на всій фігурі. Однак такі дослідження займає більш тривалий час , іноді тижні. Фахівці, що спеціалізуються на дослідженнях існуючого проектування та розробки, беруть участь у мріях "примусити" комп'ютер передавати інформацію, коли це необхідно для збереження секретності.

Суть ідеї вчених полягає в тому, що для зараження комп’ютера потрібна певна позначена програма («троянський кінь») у кожній з так званих вірусних технологій, зокрема за допомогою дискети. Драйвери, і якщо комп'ютер підключений до локальної мережі, то таким же чином . В комп'ютерних інформаційних мережах значна частина інформації зберігається на жорстких дисках. Тому програма маркування для пошуку необхідної інформації для них, пристроїв з різними факторами випромінювання, не є розумною для електромагнітних коливань у просторі. За допомогою цієї програми ви можете додавати вбудовані сигнали до відеосигналу разом із короткими повідомленнями. При цьому користувач комп'ютера, наприклад, граючи в комп'ютерні карти, не може візуально визначити, чи містять вони також певну інформацію у вигляді зашифрованих текстових повідомлень [81].

Для забезпечення профілактика в суворому випромінюванні від екрану і вибору необхідних сигналів є ефективною, необхідно знайти оглядове притулок (найпростіший спосіб - різні ТВ стандарту). Освітні експерименти, проведені в різних країнах, підтверджують можливість отримання даних шляхом отримання радіоактивних насіння з відеомонітора. Результатами всіх цих досліджень стала технологія SOFT TEMPEST - технологія передачі даних через секретні радіаційні канали електромагнітного вузла за підтримки програми. Зверніть увагу на ці основні основи, як історію інтелектуальної технології TEMPEST, яка призначена для збору інформації про роботу локальних комп’ютерних мереж та захисту інформації від витоків через димові канали та перешкоди. Слід зазначити, що серед експертів було створено два аспекти цієї технології, які розглядалися TEMPEST, з одного боку, метод атаки (розвідки), а з іншого - метод захисту.

У 1918 році Герберт Ярдли зробив принциповий висновок, що для відновлення із записаними повідомленнями можна використовувати електронні пристрої, що містять різноманітну конфіденційну інформацію, яка належить паразитичним викидам . З метою забезпечення безпеки зв'язку (COMSEC), Канадське товариство захисту зв'язку (CSE) було створене в 1946 р. У нашій країні також проводиться робота з захисту потоку інформації про маршрути випромінювання - PEMVN (електромагнітна інструкція). Європа та Канада використовують слово "TEMPEST" для використання електронних форм для управління електронними формами - радіаційними пошкодженнями, а в Америці - за допомогою абревіатури Департаменту секретної оборони Міністерства оборони США для виготовлення логотипів проти потоку інформації в електронній формі , розповідь та випромінювання. Лікування увагу на захист даних, відповідно з вказівками Президента України, на основі величини з державних відносин Служби української безпеки в 1999 році і Департаменту спеціального захисту систем зв'язку Інформація для по безпеці служби . З України було створено . Це найбільша в країні основа для захисту технічних і технічних даних. Використання та управління електронною документацією та, як правило, існуюче управління створює
можливість доступу до заборонених комунікацій . Розкриття обмеженої інформації, яка має реальну цінність, безпосередньо пов'язане з очікуваними результатами . Це може серйозно зашкодити інтересам власника інформації. Тепер розглянемо випадок вилучення жорсткого диска із забороненої інформації .

Хто не знає , що в той час комп'ютера іноді виходить з системи електронної та модифікованого пристрій , деякі з них можуть являти собою магнітні жорсткі диски до роботи. У відповідності до чинного правлінням закону про відносинах між клієнтами і виробниками продуктів і продуктів по різним видам власності , виробник гарантує нормальну роботу виробу, в тому числі компонентів, при створенні гарантійного терміну в відповідно до закону, і в його відсутність - контракт . Гарантійні зобов'язання, викладені в цій Угоді, передбачають заміну жорсткого диска, але лише за умови виконання пломб та дотримання правил експлуатації комп'ютера. Деякі

користувачі комп’ютерів, надсилаючи проблему з жорстким диском до сервісного центру, часто не видаляють інформацію, що міститься в ньому. Тому інформація, включаючи конфіденційну інформацію, автоматично передається постачальнику комп’ютерів. Слід зазначити , що вітчизняні постачальники комп'ютерної техніки закуповуються з підрозділів в зарубіжних компаніях - виробниках та їх представників. Для того , щоб замінити собою дефектний диск з відповідним якістю жорсткий диск, він вирушає до іноземним проксі . Незвична поведінка користувача ПК зрозуміла. "Протилежна" технологія забезпечує ухадалкедью чутливий час і встановлені водійські права з гарантією та безпекою обслуговування суперечливого стану. Порушення звичайної діяльності в комп'ютерних комп'ютерах споживачів, а також тиск, властивий адміністрації, який потрібно швидко усунути, щоб позбутися проблеми, сила впливу на природу людини, часто складна, стає належним виконанням службових обов'язків, запобігає критичній оцінці. І буває. Необхідну інформацію потрібно знищити . У цьому випадку використовують звичайні операції. Інтерфейс комп’ютера повідомляє користувача про видалення файлу. Фактично дані все ще зберігаються на жорсткому диску і можуть бути оновлені. Відсутні лише його контакти в папці та графік розташування файлів. Отже, проблема полягає у правильній утилізації відходів інформації. До речі, цікаво розглянути технологію розповсюдження інформації в базах даних. Виявляється, що збережена інформація зберігається на жорстких або сухих дисках, які можна роздрукувати (з’являється у списку). Як відомо, робота на жорсткому диску заснована на принципі магнітного запису, тобто показань і міток на обертовому диску, які не покриті робочим магнітним шаром . Читаючи шматок диска з різною намагніченістю, перемістіть його під верхню частину магніту і відображайте електромагнітні сигнали, перетворені в цифрові дані. Сучасний жорсткий диск Обладнання складається з: пакета (ів), плит, машина двигуна - диск приводу обертання , читання / запис голови пакети , розширення - головки і PCB кнопки управління - з електронними схемами . Знищення ліцензії на виробництво для використання, на думку експертів, і особливо "Епопеї", яка дозволяє Департаменту приватних систем зв'язку та інформаційної безпеки Української

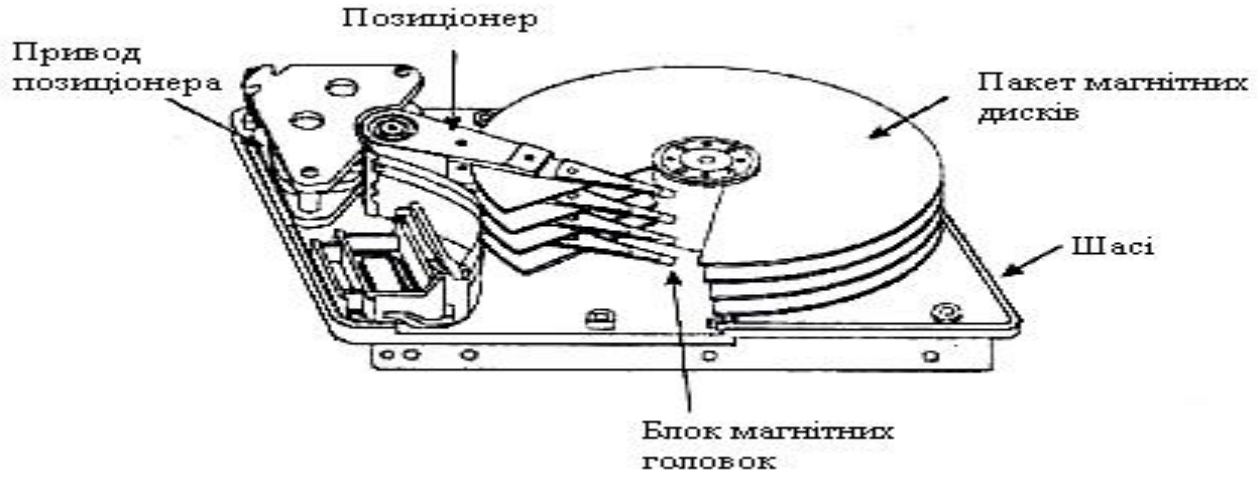
служби безпеки, було досягнуто під час реєстрації. Файл знищується іншою інформацією, а потім знищується через операційну систему. На це є спеціальні плани, особливо один із них - у будівлі туалету Нортона. Для старої було написано нову інформацію, яку було видалено. Повторіть запис послідовності аварій (подібний звук) із знищенням даних у зоні пошкодження магнітної конструкції лише на ділянках дороги, де зберігаються дані. Відновлення - це некласифікований процес запису даних у пам'ять, який зберігав раніше конфіденційні дані . За рекордний час ємність даних на жорсткому диску, якщо він пошкоджений, повністю зберігається. Дані не можна безпечно видалити на старому жорсткому диску. Методи знищення даних поділяються на програмне вплив, технічне, фізичне та використання HDD

пристроїв:

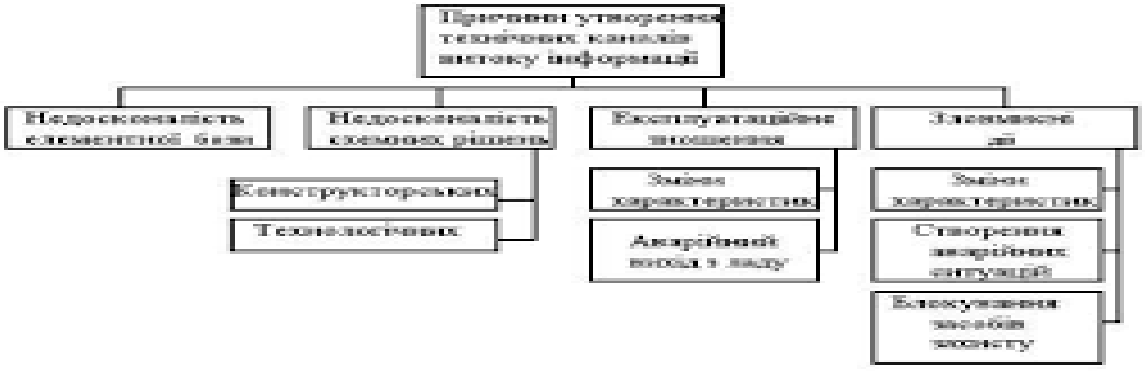
• без руйнування структури і поверхні жорсткого диска;

• Відключення жорсткого диска.

Технічні методи видалення інформації на жорсткому диску за допомогою методу впливу на носій поділяються на механічні, термічні, піротехнічні , металеві , хімічні випромінювання . Ви можете знищити інформацію, піддаючи дошки сильним постійним або тимчасовим зонам (руйнуючи магнітну структуру на робочій поверхні). Знищення даних користувачами магнітних носіїв викликає занепокоєння, тому в літературі існує інтерес до ландшафтів . Знищення даних на магнітних носіях - саме така зміна магнітної структури даних неможливо прочитати в звичайному режимі зберігання і відновити втрачені дані, що зберігаються на жорстких дисках за допомогою спеціальних методів , економічно неможливо



1.3. **Захист інформації від відтоку через канали побічного електромагнітного випромінення і наведень комп’ютера**



У зв'язку з швидким розвитком мережевих комп'ютерів , локальних і глобальних , методів розвідки (бізнес - шпигунство) і призначена для інтеграції даних для обробки, передач, мережі зберігання даних , і локального зміни , а також [45]. Сьогодні важко відповісти - розвідувальні служби , вони дуже залучені в бізнесі або уряді, конкуруючи з компаніями. Відповідно , журнальні методи контролюють інтелект для швидкого вдосконалення . Слід зазначити, що доступ до локальної мережі будь-якої організації може здійснюватися лише відомим методом

налагодження всього мережевого відділу (кожного окремого комп’ютера) системним адміністратором. Якщо сходинками є логотипи, що запобігають проникненню несанкціонованого локального комп’ютера, а також додаткові програми та інструменти для належного впровадження засобів мобілізації,

необхідних для своєчасного виконання, шпигун змушений знаходити нові способи та засоби отримання інформації. Це не випадково , що останні методи завантаження даних через електромагнітне випромінювання і навчання (PEMVN) на локальних ПК мережевих об'єктів [80] для забезпечення інформаційної безпеки в компаніях, в компаніях, локальних обчислювальних та інших автоматизованих систем є в даний час особливо актуальна [19] . Інженери та технічні групи серйозно ставляться до захисту мережевого середовища корпорації. Згідно зі статистикою, найбільшу загрозу безпеці корпоративної мережі як і раніше представляють користувачі закону. Тому необхідно посилити пильність в організації технічного захисту організаційної інформаційної мережі , включаючи:

• захищати цілісність ділової інформації компанії, особливо конфіденційної;

• Забезпечувати безперервну роботу обладнання.

Розголошення або втрата інформації може призвести не лише до фінансової шкоди, але й до репутації та конкурентоспроможності компанії . Це також важливо для безперервної роботи пристрою - відмова пакета відстежує повернення та припинення обслуговування клієнтів, тобто менший прибуток. Конфіденційна інформація та пошкоджене обладнання можуть витікати або втрачатися

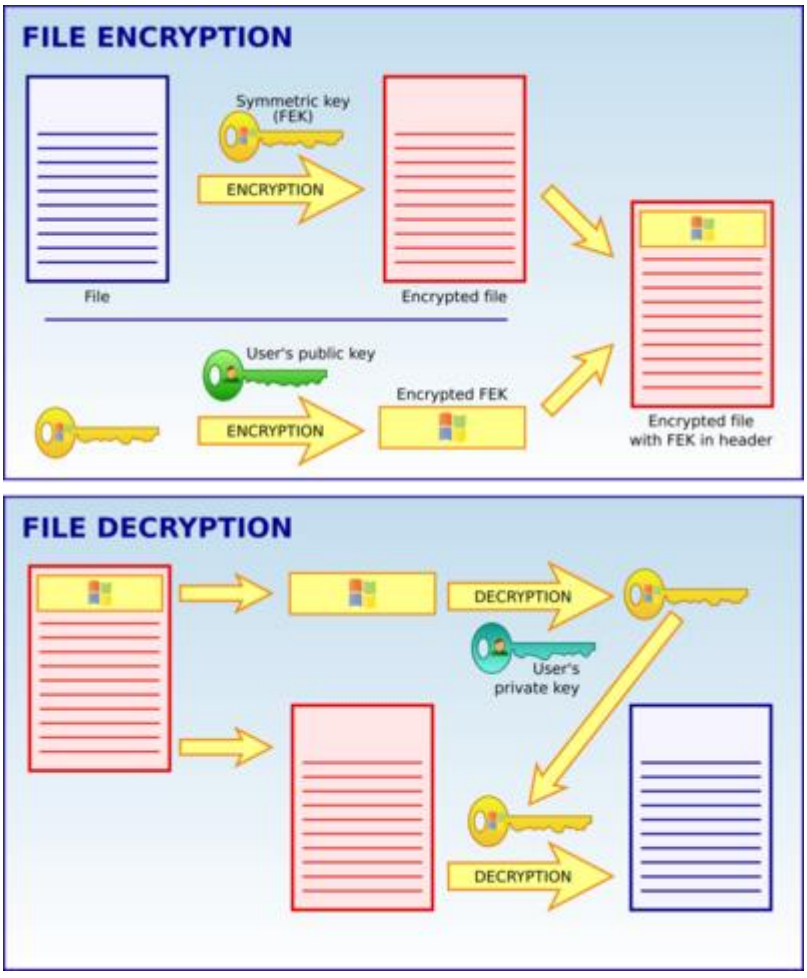
• Помилки користувачів. Я не можу погодитися між собою

• навмисне зловживання користувачами;

• Таємне введення в програму маркування вірусів троянських коней, глистів тощо. [48].

Велика кількість важливої інформації зберігається не тільки на файловому сервері, але і в робочих центрах користувача (комп’ютерах). Цю інформацію можна легко загубити або розкрити, якщо не вжити відповідних заходів. По-перше, рекомендується використовувати характеристики файлової системи NTFS

системи Diskiga, яка забезпечує ще кілька особливостей захисту та безпеки між конфіденційною інформацією через канали PAMVN, однією з особливостей такого контролю доступу. Ви можете використовувати список управління доступом (ACL) для обмеження доступу користувача до комп'ютера з використанням як в індивідуальному і групу користувачів . Наприклад, один користувач не зможе прочитати вміст файлу, інший може редагувати, і ніхто інший взагалі не може отримати доступ до файлу . Це необхідно , якщо є кілька користувачів на одному комп'ютері , і Інтернет - бізнес НЕ встановлювати обмеження реєстру - і будь-який користувач , який має фізичний доступ до комп'ютера , може зареєструвати його. Windows 2000 використовує п'ятий тип файлової системи NTFS. Одним із нововведень є система шифрування файлів (EFS), яка дозволяє обмежити доступ до файлів і папок.



Локальна мережа не може працювати на добровільних засадах без взаємодії з іншими мережами. Кожна організація , будь то приватна компанія чи державна установа, хоче бути представленою у Всесвітній павутині - на власному веб-сайті, публічній електронній пошті, доступі до інформації про широкий світ Інтернету . Це необхідно для підтримання вимог щодо інформаційної безпеки . Справа в тому, що взаємодія певних мереж може становити різні загрози для організації. Для цілей цього Голокосту була порушена найбезпечніша небезпека з усіх можливих небезпек при підключенні до Всесвітньої павутини . Найбільш поширеним виразом кібер-знущань є заміна існуючих посилань на посилання на оголені сайти. Це шкодить іміджу власника сайту та призводить до додаткових витрат на відновлення всіх посилань. В мережевому комп'ютері в провінції української інформації, цікавому для іноземних компаній , буде активно приймати комп'ютерний бій. Їх не можна розділити, але разом вони дають дуже важливу інформацію. Таким чином, у світлі інтеграції комп’ютерних мереж державних установ, компаній, науково-дослідних інститутів та організацій у глобальну мережу - слід очікувати, крім аукціонів, Інтернет та право входу в корпоративну мережу додаткових агентств. [41]. (Компанія - це та, що належить кожній компанії). Попередити, що це дуже важко . Тому Інтернет повинен бути ізольований зсередини, де зосереджені спільні дані. Looga відрізняє одну міжнародну комп'ютерну мережу , а ряд методів , використовуваних , щоб захистити лугів, запобігає огляд етнічної, в зокрема , коливання електромагнітного випромінювання з допомогою комп'ютера .

Інформаційні мережі , які не мають обмежений доступ, в поодинці, часто досить , щоб використовувати в маршрутизатор з фільтром , який служить стіною, в якості шлюзу до джерел даних в компанії «и внутрішньої мережі . Захист брандмауера можна забезпечити лише через брандмауер. Повна безпека гарантується лише в тому випадку, якщо Інтернет локальний від мережі go'anyahay додому . Якщо необхідно запобігти зовнішньому інтелекту, це обґрунтована оцінка. рішенням Кабінету Міністрів України від 12 квітня 2002 року Україна заборонила міжнародні відносини в мережі комп'ютерних персональних мереж, які обробляють і зберігають обмежену кількість інформації, що належить уряду [6]. Якщо будівля

фізично відключена від мережі, ви повинні звертати увагу на захист інформації, що просочується в каналах PEMVN.

Часто інформаційний працівник з обмеженим доступом повинен це робити. Доступ до Інтернету для забезпечення цієї можливості два комп'ютери встановлені на робочому місці , один підключений до локальної мережі, а інший -. Інтернет в цьому випадку має проблеми з тим фактом, що кабелі до приватної мережі, які захищають дані, а не відкритий Інтернет, важко надіти. тому інформаційний шлях, що циркулює в локальній мережі , а також все паразитне випромінювання від комп'ютерів, які забезпечували мережевий кабель до локальної мережі, можуть бути забезпечені відкритим Інтернет-кабелем. Піктограма - це відкрита мережа , яка іноді є частиною набору дроти, що кадр не дуже швидко, а антена за межами поля кордонів повинна бути захищена. Тому інформація доступна не лише шляхом зупинки випромінювання, але і безпосередньо шляхом підключення відкритих мережевих кабелів [61].

Можливість доступу до інформації за допомогою автоматизованих засобів, щоб уникнути багатьох людей серйозно сприймати радіацію . Цей результат може бути людсько-психологічним (різні позиції, часто неправильні). Люди , як правило , не хочуть вони , щоб повірити , що вони бачать своїми очима. Однак досвід показує в багатьох країнах, що успішних спроб отримати інформацію шляхом запобігання електромагнітного випромінювання вона ніколи не виявляла . Важливо зрозуміти, як захистити інформацію Looga, пролиту через переходи векторного випромінювання, і почути дискусію про комп'ютери Looga за допомогою широко відомого радіотехнічного ефекту "мікрофонів". Він призначений для розміщення електронних пристроїв під впливом акустичних коливань .

Для вирішення проблем з точки зору захисту фактичної технічної інформації часто використовують два основні методи: динамічний та непрямий. [58] Активний підхід передбачає використання бар'єрів для масової комунікації. Втручання надходить із джерел, що перебувають поза коливаннями активних електромагнітних камер . Шумові бар'єри використовуються для створення активних збурень. Відповідно до принципу генерації існує шум і прямі

шумові порушення . Прямі шумові перешкоди - це постійний струм шуму на дуже великій кількості частот. Така сила явно не вказує кількість і частота провідної сили втручання є рівним для розділити всі частини в шумових збурень , так що цей тип втручання є ефективним. Частина шуму, що виник, може бути більшою мірою від розширення шляху доступу до менш професійного одержувача опитування. Активний підхід до профілактики радіо дуже корисно , тому що вони загрожують не тільки поширенню інформації через переходи з комп'ютера випромінювання вектора , а й запобігти використанню слухових апаратів під час обговорення в середині електромагнітного пристрою - це радіо - реліз пристрій . Захисна кімната [58]. При оцінці ефективності цього методу мети і завдання процесу для обох повинні бути прийняті до уваги . Це пов’язано з тим, що дві різні установи, одна з яких займається розвідувальними технологіями, а інша - технічним захистом інформації, порівнюють подібні заходи, щоб побачити останні результати . Добре відомо , що при будь-якому способі з даних захисту технологій , експерт, безсумнівно , зіткнеться свої переваги і недоліки.

Метод активної оборони має наступні недоліки. По-перше, сильне випромінювання від джерела використовується , який вважається шкідливим для здоров'я.

По-друге , присутність радіоактивного матеріалу прихованого в програмах повітря кімнаті був обладнаний профілактичних заходів, які важко використовувати систему для вивчення радіо , щоб виявити витік інформації через вектор випромінювальних переходів в . Для того , щоб оцінити активний метод з даних захисту , вона прямо залежить від можливості профілактики з використанням приймача електромагнітних коливань і прослуховуванням комп'ютера розмови з одержувачем з невеликим досвідом розслідування . Аналіз виступів є , що успішне застосування методів і погроз Looga лічильник лікування для пролиття інформації залежить від правильного вибору, в разі , якщо якийсь - або , відповідне обладнання, інструменти, матеріали, і стояти в технічних вимогах до утвердження зі сторони технічне оснащення, як ми знаємо, це можливо, якщо гарантується правова цілісність, безпека, шкода, етика та

соціальна мораль. Дивовижний погляд на недоліки та переваги системи захисту даних може призвести до серйозних втрат при розробці технічних рішень щодо захисту інформації для корпоративних мереж компаній. Це особливо важливо відзначити , що відмова, на перший погляд, до спроб перехоплення від - електромагнітних хвиль, з використанням комп'ютерів та електронної розвідки для виявлення збоїв великих консультацій призводять до висновку , що існує таємна організація , захована в одній професії стандарту .

Це залежить від індивідуальних особливостей будівельної структури мережі iskuwareego довідкової інформації, разом з активними і Looga уникнути проливаючи над у радіаційному вектор з обманюючи комп'ютер приходить непряме ВЕ реалізовано .

Методом тимчасового захисту інформації для запобігання журналам, захищеним від випромінювання, є шафа, оснащена комп’ютером . Екранування можна досягти наступним чином: Покладіть металеві листи на двері, стіну, підлогу,

стелю .

1.4. **Превентивні дії на захист інформаційних ресурсів підприємства від посягань зловмисників**

Останнє десятиліття характеризується бурхливим розвитком ділової активності в Україні. Багато компаній активно використовують нові методи управління. Персональні комп'ютери та сучасні системи зв'язку широко використовуються для реалізації систем управління. Пошук, обробка та передача інформації зазвичай здійснюються на персональному комп'ютері. Технологія управління, а також робота з унікальними ресурсами організації - інформацією, забезпечує доступ до управління бізнесом. Результатом різних управлінських втручань є управлінські рішення , які замінюються передачею певної інформації. Таким чином, за умови належної організації в системі взаємодії, наприклад зовнішнього середовища бізнесу , може бути досягнута зміна об'єктивних відносин управління . Я погоджуюся з думкою, висловленою в літературі, що базується на всіх заходах щодо участі у візитах у зв'язку з так званим спілкуванням.

Питання про роль людини в інформаційному процесі в управлінських технологіях полягає не в поглинанні, передачі та розповсюдженні інформації, в складному процесі, який впливає на людей для досягнення мети [31]. Я можу погодитися з А. Додоновим, Є. С. Горбачиком, М. Кузнєцовим в інформаційному суспільстві, роботі та багатьох системах, підтримка рішень - це технічні проблеми вразливості до помилок у цих системах, спрямованих на тих працівників та рівень, спрямований назовні. Проблемою стає соціальний захист та держава "* . * Додонов А. Г., Є. С. Горбачик, М. Д. Кузнєцова. Питання безпеки для громадської інформації // Інформаційна безпека:. Наочно-паркет . Колекція . "Справа 1." технічний захист інформаційних систем " - За : ТОВ " ТІД " ДС ", 2003. - 216 с . . потреба в захисті даних часто пов'язано з економічним переходом до ринкових відносин в Україні більшість робіт по забезпеченню інформаційної безпеки підприємництва в Україні, він зазначив , що для забезпечення ефективного здійснення заходів безпеки вимагає спеціального знання [61, 65-76]

В Останніми роками спостерігається суттєва різниця між можливостями застосування різних дисциплін (кібернетика, теорія інформації, радіотехніка,

електротехніка, експерти-криміналісти тощо) для захисту інформації та стану розробки методів та заходів щодо прав комерційного компанії. проблема захисту ділової інформації була вирішена правильно. література не має визначення кінцевої безпеки в компанії даних . немає достатньо досліджень - глибина таких понять, основних, таких як безпека інформації , методи забезпечення безпеки , які використовуються для досягнення цієї мети, а також інтегрована захисту [56]. ідея загального захисту ділової інформації не розроблена [20]. сприяння захисту ділової інформації, необхідної їм у розробці наукових рамок і методів, поради Ю. Теми , методи та прийоми забезпечення безпеки бізнесу .

Успішні рішення цієї проблеми в основному передбачають поєднання результатів досліджень комп'ютерних даних та того, що призначене для інтелектуальної власності (розголошення, конфіденційна інформація, банківська справа, комерційна таємниця), залежно від способу захисту. Ділова інформація [76].

Проблема захисту ділової інформації в науці та літературі значною мірою охоплюється загальними теоретичними характеристиками її особистих аспектів. М. Алещенков, Б. Радіонов, А. Хоров, А. Задворний, Д. Халяжин, В. Ярочкін, В. Ліпкан, П. Біленчук, М. Гуцалюк, В. були чудовим інструментом для розуміння проблеми захисту даних. Герасименко , В. Попович, Л. Гофман, А. Додонов, В. Цимбалюк. Робота, а також презентація досвіду авторів, використовує засоби літературних ресурсів для захисту даних, розроблених за допомогою комп’ютерних технологій та переданих у мережу, побудовану на їх основі

[70

Ми поділяємо думки більшості учасників розвитку щодо питань інформаційної безпеки; зазвичай необхідність захищати інформацію виникає:

• якщо документи є конфіденційними, а робота конфіденційною;

• під час обробки традиційних документів;

• При обробці інформації в автоматизованих системах;

• При обробці інформації, що зберігається в локальних мережах і передається; • При передачі інформації за каналами зв'язку;

• При проведенні конфіденційних переговорів.

Використання різних видів комерційного шпигунства і бізнес - структура стало одним з найбільш ефективних методів для вирішення проблеми отримання вигоди від незаконної атмосфери конкуренції і отримати максимально можливі вигоди. Багато року доступу до економічних і промисловим секретам конкурентів і конфіденційної ділової інформації послідовно були показані бути ефективним способом використовувати достовірну інформацію у всіх секторах ринкової економіки. Досягнення цієї мети стало можливим завдяки стратегічному стандарту та дії з доступу до інформації в обмежених ситуаціях . Злочинна діяльність характеризується використанням різних методів та сучасних інформаційних

технологій, що впливають на захист ділової інформації та вимагають адекватних заходів [79].

Метод вирішення проблеми захисту інформаційного бізнесу призводить до проблеми використання наукових та сучасних методів захисту інформації, що зберігається в приватних ЗМІ [77]. Сьогодні не можна стверджувати, що цю проблему можна вирішити, незважаючи на її загальновідомі успіхи, такі як використання найсучасніших технологій та інструментів для захисту секретів єдиної проблеми компанії. Це, звичайно, нічого не коштує, на перший погляд, інформація з великими обсягами забезпечує перехід від кількості до якісної ідентифікації та аналітичної обробки. Забезпечення успіху кожної компанії не тільки захищає конфіденційну ділову інформацію , але також включає збір, аналіз, оцінку та прогнозування.

Система збору даних дозволяє наукові методи , щоб пояснити природу відповідного процесу про відповідної конкурентної економічної ситуації , з коментарями про вплив ситуації на увазі , щоб розробити прогностичні моделі найкращої практики [35 12 - 19] В. Воно повинно слід зазначити, що інформація цінна лише в тому випадку, якщо вона може бути використана споживачами. Приватне місце в кеші конфіденційної інформації, яке охоплює управління організацією, має інфраструктуру системи захисту інформації. З огляду на це , то це необхідно пояснити , що це вважається інформація безпеки чинників . Як і всі, розроблені для досягнення цієї мети, методи обробки інформації у вигляді автоматизованих, безпечних та традиційних засобів, як правило, включають технічну ефективність та інформаційні технології , обмежені ресурси, клієнтів та працівників. Про інформаційну безпеку. На відміну від інших функцій, об’єктом захисту тут є джерело інформації, тобто інформація про фізичні носії, яка включає, наприклад, технічні документи, документи, бази даних тощо. Власник має право отримати доступ до законодавчо встановленого джерела інформації . , Порядок також регулює доступність, використання, зберігання та

передачу інформації. View, не- неіснуючі матеріал безпеки даних може не тільки матеріальний об'єкт, але і послуги , такі як конкретні дані про продуктивності і конфіденційних документів на , надання доступу до конфіденційної інформації, доступ до компанії конфіденційної реєстраційної інформації і так далі. Основи інформаційної безпеки включають її концептуальні рамки та структуру, внутрішня структура відображає структуру системи інформаційної безпеки бізнесу та, що найголовніше, загальні принципи створення та функціонування системи інформаційної безпеки. Про суб'єкта господарювання. Для визначення інформаційної безпеки, то різні концепції принципів , запропонованих багатьма вченими , які складають основу їх знань на концептуальному рівні інформаційної безпеки діяльності мають важливе значення . "Захист ділової інформації є гарантією захисту прав інтелектуальної власності цінної особи, пов'язаної з власністю", - сказав прем'єр-міністр Клименко. Конфіденційність стає методом захисту даних . Інформація про керівних напрямних, організаціях і методах сучасної захисту даних », підготовленої групою C.H. Tifaftireen Valid проаналізований для управління бізнес - послугами на момент захисту інформації . Автори назвали відсутність порушення конфіденційності та цілісності інформації.

Інформаційна безпека виявляється, що визначення інформаційної безпеки відображає його особистість, що найбільш важливо і розташування в компанії безпеки . на цій основі ми можемо також виявити зміни в ситуації безпеки бізнесу щодо інформаційної безпеки та інформаційних даних, Tikniyoolajiyada Sameysmahooda та використання, а також звичайний потік інформаційних транзакцій, який полягає у виключенні порушень конфіденційності та повноти даних . з урахуванням потенційних ризиків інформаційної безпеки обговорювалися може перевірити діяльність інформаційного саду процесу різноманітні. відомо, що джерелом

навмисного використання різних технологій, що використовуються в обробці інформації, є останній випадок [36, 34-36]. Подумайте про партійну систему, враховуючи пріоритети ризику , всі елементи безпеки даних. Вибір порушень є тим чи іншим способом з огляду на інформаційні технології останньої обробки інформації з метою порушення . Слід пам’ятати, що вибір винуватця шахрайства є випадковим, але часто залежить від мотиву злочинця, рівня підготовки та здібностей злочинця, передбачуваного середовища, в якому йому доведеться діяти [60]. Аналізуючи зв’язок незаконної єресі в галузі конфіденційної інформації в реальній владі людей, які хочуть зберігати комерційну таємницю, і дозволяє виявити конкретні типи злочинців, які загрожують безпеці ділової інформації. На наш погляд, ними можуть бути:

• працівники служби безпеки комерційного підприємства;
• працівники компанії, які мають доступ до певних важливих будівель;
• Людина виходить з-під контролю, створюючи організоване закриття, оснащене техніками спостереження, небезпечні межі для безпечних районів ,
• контрольована територія, але нам не потрібні ніякі засоби;
• Той, хто має доступ і працює у відведених місцях.

Адекватне розуміння загроз інформаційної безпеки та видів злочинців дозволяє співробітникам служби безпеки компанії вживати відповідних заходів, щоб захистити їх від можливих "атак" на засоби інформаційної системи. Під час їх розвитку не можуть бути враховані основні характеристики, наприклад: елементи захисту інформації та типи правопорушників (їх здібності, поведінка,

місцезнаходження). Аналіз має таку необхідну умову, опис матеріального змісту основних особливостей структурних елементів, цільової системи зростання для захисту циклічної інформації в організації від зовнішнього середовища. Найбільш важливі елементи в інформації безпеки структури в системі , пов'язаної з відносинами між двома сторонами може розглядатися в якості підходу захисту наступним чином :

• фізично;

• управління;

• Аксесуари для обладнання;

• Програмне забезпечення;

• сигналізація;

• Доказ системи комп’ютерної безпеки. Застосовується для досягнення наступних цілей:

• Заборонити доступ до комп’ютерних документів та інформації за допомогою апаратного забезпечення, створеного апаратним та програмним забезпеченням комп’ютера

• запобігати знищенню або несанкціонованому зміненню даних; • Запобігання конфіскації конфіденційної інформації в матеріальних каналах (розкрадання зразків продукції, копіювання, ксерокопіювання документів, фотографій);

• запобігти отриманню даних переданою командою;

• Запобігання несанкціонованому доступу до конфіденційної інформації за допомогою візуальних, акустичних каналів [58, 289-294]. Останнім часом приділяється увага корпоративній інформаційній безпеці, мережевим платіжним мережам та іншим автоматизованим системам. Фізичний підхід до захисту інформаційних систем може відрізнятися, і їх вибір залежить від завдань, які вони вирішують, типу передавача даних, методів, що використовуються для доступу до обмеженої інформації, та каналів даних. Система фізичного захисту зазвичай використовується для забезпечення виконання таких заходів: протипожежного захисту в місцях, де обладнання знаходиться в системі обробки даних або в комп'ютерному центрі; Запобігання проникненню злочинців у будинки, визначені ЦК, шляхом посилення дверей, вікон, електричних заборон на будівлю Центральної ради, центр обробки інформації та пошкодження об’єктів, що охороняються; Обмеження доступу персоналу до будівлі Центральної ради або Центру обробки інформації; Контроль за захистом державних службовців, встановлений компанією. Спеціальне програмне забезпечення Softwerk є частиною інформаційного процесу розробки програмного забезпечення, запобігаючи несанкціонованій мережі передачі даних або Інтернету з місцевих причин TEMPEST, а також запобігає появі знаків між інтегрованою головкою. TEMPEST - Атака здійснюється шляхом "зараження" комп'ютера спеціальною програмою розмітки ("троянський кінь") або іншими способами (наприклад, за допомогою технології побудови комп'ютерних вірусів: використання компакт-диска для відтворення, цікава програма за допомогою, комп'ютерний диск з драйверами, а якщо персональний комп'ютер підключений до локальної мережі, то це шлях) [85]. Фонова програма дозволяє передавати інформацію за допомогою комп’ютеризованого програмного

забезпечення для контролю випромінювання, а головне - програма розмітки здійснює пошук інформації, необхідної для диска, за допомогою різних комп’ютерних засобів, що призводить до появи неінвазивного випромінювання. Випромінювання процесора через інтелектуальний приймач дозволяє йому отримувати інформацію безпосередньо через інтерфейс комп'ютерної системи. Найпоширеніше програмне забезпечення включає антивірусні програми, пристрої для зменшення випромінювання, особливо шрифти Tempest. Методи захисту інформаційних технологій є частиною програми захисту Tempest, яка використовується для запобігання завантаженню конфіденційної інформації за допомогою методів фарерської електромагнітної комп'ютерної діагностики. Для цього зазвичай використовують непрямий метод для запобігання відстеженню процесів для електронної обробки даних.

Емоційна система - це поєднання захисного чохла та особистих речей на комп’ютері з використанням вдосконалених фільтрів для досягнення високого рівня точності. Проблема запобігання можливості електромагнітного випромінювання в інформаційних системах , приміщенні комп’ютера, вирішується головним чином спеціальними джерелами шуму , робота яких не дозволяє використовувати пристрої. прослуховування. Відомий як активний метод захисту даних). Іншим варіантом захисту даних є захист комп’ютеризованих джерел випромінювання для зниження рівня випромінювання на робочому місці. Лікарі рекомендують розміщувати його в металевій шафі або в приміщенні. В даний час комп’ютери розробляються як форма захисту інформації за допомогою каналів PAMVN. Особливо важливою для захисту інформації в локальних мережах є технологія, заснована на розбризкуванні спеціальних матеріалів на корпус комп’ютера для зменшення сигналу, що випромінюється з робочого місця [39, 104–108].

Сьогодні існує безліч інструментів, а електронні, електронні, апаратні, конструкторські та технічні рішення для глобального журналу запобігають появі інформаційних технологій через коридори персональних комп’ютерів. Ось деякі з

них: Захист дротів зв'язку для запобігання додатковій інформації про вилучення електроенергії та землі; Використання контрольних фільтрів, що зменшують перешкоди при передачі від зовнішніх та внутрішніх джерел перешкод; Уникнення наслідків електричних коливань у мережевих комп’ютерах, що використовують інструмент координації мережі електропостачання, однією з функцій якого є фільтрація коливань частоти ланцюга захисту землі у випадку комп’ютера; Вибір та використання такого рішення для створення комп’ютерної системи, яка відповідає вимогам безпеки і не порушує характеристик всіх захищених матеріалів, на яких розповсюджена локальна мережа тощо. Звичайно, використання технічного захисту інформації жодним чином не замінює експертні функції моніторингу, знайдені у відповідних пристроях, у разі порушення прикордонної безпеки.

Слід зазначити, що практичне застосування організаційних заходів щодо захисту ділової інформації нереально без вирішення кількох ключових питань, серед яких:

• доступ до інформації вважається конфіденційним у бізнесі;

• створити надійний захист конфіденційної інформації з власником або ліцензійним агентством;

• Повний контроль над інформаційною безпекою компанії.

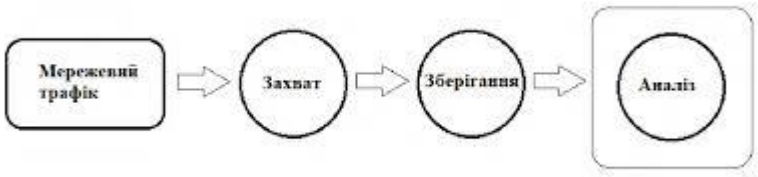
Робота компанії з захисту даних часто пов'язана з відмовою у доступі до несанкціонованої інформації методами збору даних.

Пояснимо це на прикладі.

Коли двоє співробітників компанії ведуть ділову розмову в приватній кімнаті, усний обмін інформацією між ними відбувається по повітрю. Зрозуміло, що в’язні, перебуваючи поза кімнатою, вони обирають найкраще місце для спостереження, наприклад, за вікном люди розмовляли. Таким чином, за допомогою оптичних приладів для поліпшення зору (за рахунок збільшення губ) вони можуть отримати потрібну інформацію. Надійна передача інформації за різними каналами, схоже, пов’язана лише з основним

способом поширення сигналів, що містять інформацію. Насправді, крім основного середовища , яким є повітря, існує кілька універсальних середовищ. Наприклад, існує так званий вібраційний ефект віконного скла з частотою дзвінків. Існування вібрації важливо для вибору конкретного методу перетворення вібрації в техніку тривалого діалогу. Виникає запитання: чи існує зв’язок між симптомами остеопоротичних симптомів, що виникають під час обговорення в кімнаті, та способами отримання інформації? Розглядайте розмноження як процес отримання інформації, яка передається у формі остеомаркерів і без істотних змін у навколишньому середовищі. Під час цього процесу джерелом інформації є як людина, так і технічна система, яка дозволяє зчитувати вібрацію через вікна і перетворювати її на розмову. Слід зазначити, що в даний час для прослуховування в приміщенні використовуються лазерні мікрофони. Тому кольорова точка вже видно у вікні, яке відображає лазерне світло в нагрівачі, при використанні фотодіодного приладу перетворює коливальний світловий цикл в електричний. На практиці вирішення питань організації різних систем захисту конфіденційної ділової інформації компаній вимагає створення захисних меж поза контрольованими зонами. Існуючими у таких країнах захистом, як правило, є операційні, кімнати - зберігання комп'ютерних даних, особливо важливі приватні кімнати, в яких зберігається база даних тощо. [82]. Використання прикордонних систем для захисту ділової інформації не випадкове, а завдяки тому, що це дозволяє освоїти різні технології складної обробки інформації за допомогою спільного контролю. Традиційний суб'єкт даних - це документ, який адміністративно визначається як об'єкт з інформацією, що змінює техногенну передачу з часом. За способом обробки інформації документи поділяються на текст, відео, фотографії, пунктуацію, документи та фільми. Письмові - усі рукописні нотатки та рукописні документи, зроблені з використанням різних друкарських та перукарських інструментів. Зображення включають зображення, плани, схеми, креслення, графіки, карти. Фотодокументи - аудіозаписи інформації, які широко

використовуються для підготовки протоколів конференцій, конференцій, конференцій тощо. Відомо, що інформація передається людям за допомогою органів чуття: зору, слуху, смаку. Важливою характеристикою інформації є її доступ як до людей, так і до комп'ютерів. Люди отримують більшу частину інформації в аудіо- чи відеоформаті. Відповідно до сучасних уявлень, інформація завжди виражається матеріально та енергійно. Справа в тому, що обмін інформацією будується на всіх видах управлінської діяльності і відбувається за допомогою різноманітних фізичних явищ і методів. З управлінської точки зору ці методи називаються методами комунікації. Зверніть увагу, що кожна форма обміну даними має своє власне базове середовище. Існує побічне середовище, вони зберігають інформацію, яка відображається, тобто джерело інформації. По-перше, нам важливо зрозуміти взаємозв'язок між первинним та верхнім середовищами обміну інформацією . Давайте розглянемо приклад персонального комп’ютера користувача. Відомо, що інспектор призначений представляти інформацію візуально. Користувач ПК отримує інформацію у вигляді змішаного сигналу від монітора, який замінюється певною серією електричного та магнітного полів. Інформація візуально відображається на екрані монітора. Не Важко зрозуміти, що в цьому випадку основним інформаційним обміном є видима частина електромагнітного коливання. Як ми вже згадували раніше, коли екран працює, існує побічне середовище, яке включає відображену інформацію. Подивіться на них докладно.



Під час роботи монітора електронні схеми випромінюють електромагнітне випромінювання в діапазоні від 100 МГц і в результаті катодного про меня крана. Рентген - це електромагнітні хвилі. За своїми симптомами вони близькі до видимого випромінювання, але більшість з них не видно людському оку. Радіація

Електромагнітні зіткнення відеомоніторів та елементів, що містять конфіденційну інформацію, можуть перехоплюватися радіорозвідкою та радіо в кримінальних структурах та в комерційній конкуренції [58, 244]. Інтеграція та перешкоди електромагнітного випромінювання, що генеруються комп'ютерними компонентами, такими як монітори та комп'ютери, створює серйозну загрозу захисту комерційної таємниці завдяки автоматизованій обробці даних. Питання управління системою захисту даних приватної компанії, яка складається з електронних пристроїв та комп'ютерного обладнання - служби безпеки. Слід зазначити, що сьогодні робота із захисту даних між комп'ютерами та комп'ютерними мережами ведеться за чотирма основними напрямками:

• Запобігання несанкціонованому доступу до інформаційного потоку компанії через програмне забезпечення та значення інженерної розвідки;

• Зручність в організаціях та організаціях та технічна обробка конфіденційної інформації для запобігання крадіжки, пошкодження;

• Несанкціонований доступ до зберігання та обробки інформації за допомогою комп'ютерного обладнання, яке передає лінії зв'язку клієнта;

• Запобігання змінам несанкціонованої інформації.

Жоден з них не може оскаржити літературну думку про те, що ділова інформація має багато архівів, а найпопулярнішими є людська мова, документи, верстати (жорсткі драйвери). Це призвело до використання різних методів, включаючи передачу, зберігання та обробку. Організовуючи захист обмежених даних, що обробляються на персональних комп'ютерах, необхідно враховувати деякі фізичні характеристики, що характеризують комп'ютерні методи зберігання. В залежності від фізичної природи джерела і навколишнього середовища , в якому передаються і модернізоване випромінювання, технічна інформація про шляхи , які випускаються з комп'ютерної мережі діляться на електромагнітний, обсяг і потужність [39, 104-108]. Загальновідомо, що сегрегація - це перший крок у правових знаннях. У подальших дослідженнях із загальної теорії інформаційної

безпеки основна передумова дослідження веде до більш глибокого розуміння літературних положень у часи лише відділення влади від технічних каналів, через які надходить інформація. П’ять-шість років тому це мало посилити почуття ідей та важливих питань, пов’язаних з інформаційною безпекою, яка обробляється в електронних обчисленнях. Вони з'являються в інформації та посиланнях, що розповсюджуються в цій книзі "Організація та сучасні методи захисту даних ", а також у працях С. Казневського, А. Моршова, С. Прокопенка, А. Правозіна, С. Чеховського, Л. Козленко. І т. Д. [39, 104-108]. У діях, пов'язаних з проблемою інформаційної безпеки, особлива увага приділяється відновленню та знищенню гарантій даних, що зберігаються на жорстких дисках, та запобігає потоку інформації через електромагнітне випромінювання та керівництву при роботі на персональному комп'ютері. Однак питання про характер стратегії вибору ефективних заходів для боротьби з втручаннями в мережеві комп'ютери , достатньо конкретних інструментів і прийомів, які може використовувати порушник, не розроблено, на наш погляд, не залишило уваги експертів . Експерт з цих питань. Оцінюючи можливість вибору конкретного методу, що означає, що необхідно контролювати комп’ютерне випромінювання і запобігати потоку інформації, яка працює, вона не може відхилятися від значення в логічному процесі змісту фізичних явищ, що виникають при каналах з'являються. . Тільки інші, без особливого значення, дозволяють правильно це вирішити. Сюди входять загальні вимоги щодо розумного використання існуючих технічних можливостей та проблем, що впливають на ефективність захисту даних у системах із комп'ютерним ядром. Рішення щодо використання операції у спеціальних методах та засобах для визначення та позначення взаємодії секретним інформаційним маркуванням не обмежується точними знаннями, пов'язаними з фізичним вираженням різних типів зберігання інформації для цілей електронно-обчислювальних методів. , Але також визначте конкретні методи, що використовуються для блокування сигналів "ризику" та блокування доступу до інформаційних каналів. Проблема незаконного доступу до конфіденційної

інформації конкурента через технічний підхід є навмисною. Це пов'язано, зокрема, з тим, що всі технічні методи пошуку інформації створюються не тільки радіаційним та електромагнітним наведенням, які замінюються сигналами, що з'являються на комп'ютері під час інформаційного процесу. Існує також створення технічних посібників з розповсюдження інформації по установці радіо сигналів (сигналів) на комп'ютері або мережі живлення або шляхом повторного застосування їх. Наприклад, лінії за межами зони управління, спричинені електропроводкою, комп’ютерним та віддаленим режимами, називаються контактними в ряді струмів. Високочастотні хвилі, що передаються через матеріал, опосередковано призводять до збільшення об'єднаних хвиль і придбання конкретного пристрою. Крім того, коливання електронного пристрою управління для прийому інформаційних знаків вже існують у робочому комп’ютері. Особливо важливим є той факт, що лише комп’ютери здатні обробляти та зберігати інформацію. При підключенні комп’ютера до локальної мережі або глобальної мережі Інтернет проводяться всі види інформаційної роботи: її зберігання, обробка та передача.

Слід зазначити, що сьогодні комп’ютери в основному використовуються в локальній мережі. Отже, необхідно вирішити проблему захисту комп’ютерів від витоку інформації через електромагнітне випромінювання та канали. Давайте тепер розглянемо питання про виникнення «небезпечного» комп’ютерного випромінювання.

Сучасні уявлення про комп’ютери як продукт технічного захисту інформації повністю пояснюють це явище. Наявність деталей персонального комп'ютера різного призначення обумовлена під час їх роботи побічним випромінюванням. Оскільки це канали інформаційного потоку, створені комп’ютерною мережею, використовуйте непряме електромагнітне випромінювання і керуйте більшістю компонентів комп’ютера - принтером, комп’ютером, блоковою системою, акустичною системою, монітором. Всі компоненти локальної мережі підключені до проводів та кабелів живлення. А як

щодо кабельної мережі? По-перше, він грає роль незаконної випромінювальної антени на комп'ютерах і серверах. Крім того, електромагнітні коливання вивільнили комп’ютер через проводку кабельної системи, яка вивільняє пристрої на комп’ютерах, що працюють в локальній мережі, і може спричинити накопичення додаткового повітряного випромінювання. Майте на увазі, що кумулятивне накопичення створюється внаслідок впливу випромінювання двох комп’ютеризованих елементів на елементи, вузли, блоки непрямого перетворення з декількома довжинами хвиль. Розглянемо цільові обставини, які допомагають створити шляхи для проходження інформації через електромережі. Для роботи з комп'ютером зазвичай використовують заводську мережу змінного струму - 50 Гц. Типове електричне обладнання - це поворотний фільтр і постійне джерело енергії. Пристрій розподілу живлення Персональний комп'ютер, ізольований, має унікальні функції, які будуть реалізовані наступним чином. Електроживлення звукозаписуючого обладнання, принтера, акустичної системи здійснюється через перехідники та автономні пристрої. Адаптер використовується для перетворення 220В змінного струму в 12В змінного струму. На додаток до адаптера тільки , є перемикачі , які працюють на електричній схемі комп'ютера. Клітини системи, комп’ютери та двигуни працюють із пристроєм змінного струму на частоті 50 Гц та напругою 220 вольт з потужним водопостачанням.

Конструктивно верхній електричний блок побудований з металевого контейнера, розміщеного в системному блоці з механікою для обробки та зберігання. Принтер живиться від свердловини (220 вольт, 50 Гц) через електричний фільтр або джерело безперебійного живлення. Для того щоб знизити рівень електромагнітного випромінювання , який падає на потужність до ПК «з мережею , використовуються ослаблення шуму , мережеві фільтри. Зверніть увагу, що в промисловій мережі 50 Гц при напрузі 220 вольт, яка використовується для живлення окремих комп’ютерів, спостерігаються зміни напруги, які називаються відключеннями мережі. Під час другої електричної роботи клітинної системи випромінювання виникає у вигляді

електромагнітних коливань. Електрична схема складається з багатьох конструктивних елементів - ланцюгів, ланцюгів живлення, моніторів, магнітних проводів. Багатокомпонентна електрична складова в ланцюзі живлення ПК є загальним джерелом системного блоку та регіонів. Блок живлення багатоканальний, вбудований в системний блок корпусу, отримує харчування безпосередньо з в мережі . Зверніть увагу, що джерело живлення служить нейтральним з'єднанням між джерелом живлення та компонентами комп'ютера, тому вони повинні бути тими, які повинні бути фільтрами, тобто не передавати мережеві перешкоди навантаженню. Слід зазначити, що під час роботи тверді речовини та конструкції, які перетворюють змінний струм - 220 вольт у постійну напругу 12 вольт - утворюють паразитні ланцюги. Наприклад, перетворювачі для самостійного виготовлення створюють такі схеми, як: базова мережа - приймальний адаптер, вихід адаптера - завантаження; І вбудовані перетворювачі: основна мережа - перетворення - зарядний пристрій. Пам'ятайте, що додатковий цикл паразитів створює енергетичний цикл для принтера. Всі паразитні цикли різних пристроїв мають спільну точку підключення до пристроїв, що знаходяться поза зоною управління через основний електричний ланцюг. Обладнання для обчислювальної техніки кумбуюутаррада створило серйозні проблеми шляхів розподілу для вектора рішення. Фактори, що спричиняють розповсюдження радіоактивного випромінювання, знаходяться в електричному ланцюзі окремих комірок комп’ютерної системи і є дуже важливими кабелями, що забезпечують напругу змінного струму 220 В з частотою 50 Гц. Причинами несправності комп'ютерних пристроїв є: можливість передачі та зв'язку між інтегральними схемами силових ланцюгів та заземлювальними ланцюгами; Системи комутації, що виникають при заміні транзисторів - трансформаторів - від 220 вольт до 12 вольт постійного струму; Перетинає напрямок між сигнальними лініями через паразитичні та обсерваторські сили; Інструкції з електромагнітних полів. Електричні збурення в комп’ютерній схемі вважаються непрямим електромагнітним випромінюванням

від джерела порушень поглинання, доступним двома способами: передачею, наприклад, ланцюгами, та повітряним випромінюванням. Проміжне поширення електромагнітних перешкод: простір з непрямим електромагнітним випромінюванням; Металеві деталі для огорож, вузлів і блоків; Збільшення циклів паразитів; Паразити в розподільчих камерах; Проміжні продукти дросельного фільтра; Різні з'єднувальні дроти; Електроенергія та земельний потік; Електричні схеми.

У сучасній фізиці відомо, що всі закони регулюються чотирма типами взаємодій:

• електромагнітні;

• Сила тяжіння;

• Слабкий;

• Сильний

Ніхто не може зрозуміти фізичну природу каналів інформаційного циклу комп'ютерних мереж та комп'ютера, не розуміючи радіаційної картини комп'ютерних компонентів, радіаційні хвилі пов'язані з високими хвилями, мікрофоном і викликають симптоми, що викликають - негативні наслідки потоку інформації.

Серед вимог до розробки технічних способів інформації, що виходить з електричного кола, можна відзначити такі умови: недостатня кількість циклів паразитів, наявність загальної точки циклів паразитів, що забезпечує непрямий електромагнітний обмін; Багато видів з багатоканальних коливань .

Також майте на увазі, що сторону коливань можна змінювати, по-перше, сигнали, що генеруються під час комп'ютерної обробки інформації на комп'ютері, а по-друге, інформацію про акустичне поле як деяку структуру електричного обладнання. Вони мають ефект мікрофона. Це означає, що виправлені бічні коливання можна встановити не тільки шляхом вибору інформації, яка працює на комп'ютері, але і в залі для прослуховування. Визначаючи умови, що сприяють формуванню шляхів передачі інформації, необхідно враховувати багатогранні

фактори, що впливають на потенціал електромагнітного випромінювання в комп'ютері. Справа в тому, що кожне фізичне явище відповідає ряду обмежень, дисперсія яких визначає екологічні характеристики інформації, що обмінюється. У разі будь-якої загрози безпеці ділової інформації повинні застосовуватися різні засоби для запобігання доступу до Ліги конфіденційної інформації.

Виходячи з вимог безпеки збереженої інформації, необхідно вживати заходів із використанням різних технологій та методів захисту. Знайдіть електронний спосіб покрокового запису незаконної інформації:

• Дослідження відповідно до умов служби безпеки компанії, яка працює на об'єктивних даних;

• перевірка радіо за межами будівлі;

• Перевірка внутрішнього радіоконтролю з використанням непрямих областей вздовж частот між 0,1-2000 МГц;

• моніторинг комп'ютерів, телефонів, електрообладнання через приймачі;

• Перевірте стіни кімнати, використовуючи опитування або індикатори місця;

• огляд меблів та інших предметів у приміщенні за допомогою радіологічного обладнання;

• Перевірте телефонні та електронні лінії за допомогою сканера 99. Серед доступних на даний момент методів захисту інформаційних систем ви можете отримати конкретний перелік: технічний, моніторинг, контроль, ідентифікація та інші. Технічна підтримка захисту конфіденційної інформації включає:

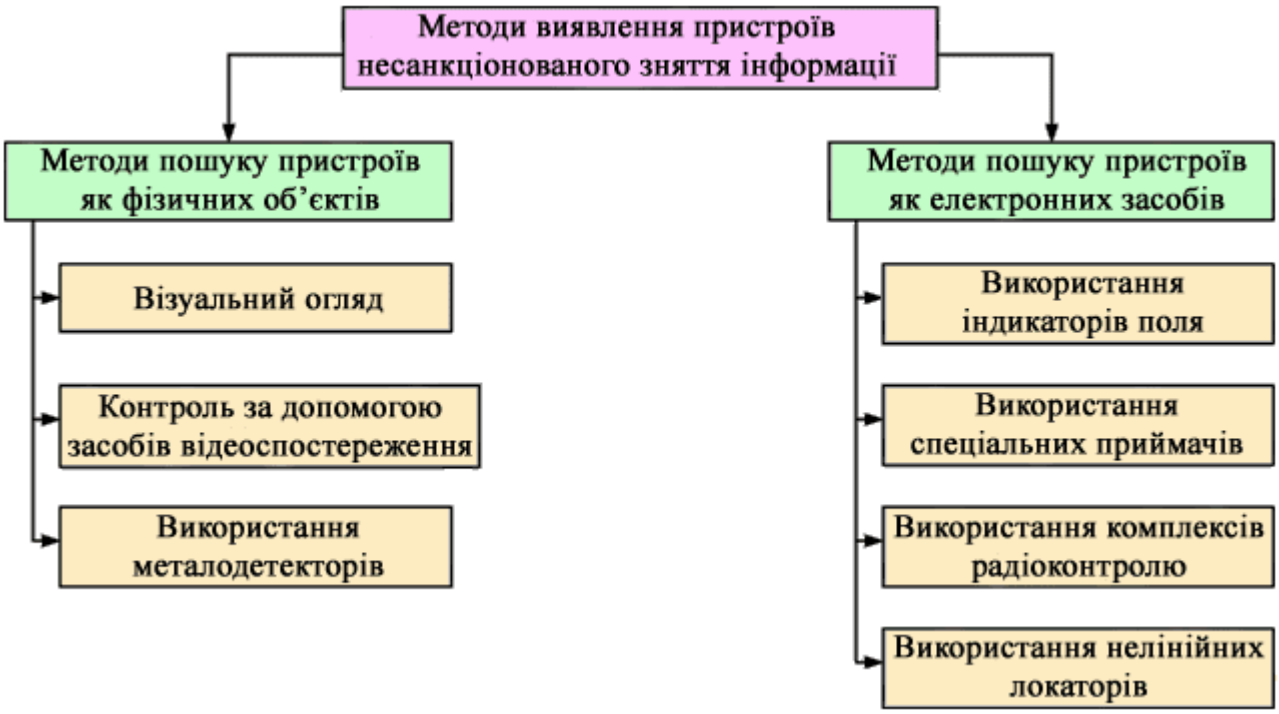
• сортування об'єктів у комп'ютерній системі;

• Нагляд за послугами інформаційної безпеки компанії за програмами комп'ютерних технологій (служби захисту інформації для компаній, організацій,

організацій, у тому числі: керівник організації, менеджер системи або менеджер програми, керівник служби безпеки компанії, бухгалтери, інформація експертів систем);

• Доказ системи комп'ютерної безпеки для забезпечення відповідності стандартам захисту інформації;

• Технічний контроль спеціального обладнання, що використовується для забезпечення безпеки та конфіденційності інформації.



2 НОРМАТИВНО-ПРАВОВИЙ І ОРГАНІЗАЦІЙНИЙ АСПЕКТИ ДІЯЛЬНОСТІ СУБ'ЄКТА ГОСПОДАРЮВАННЯ СТОСОВНО ЗБЕРЕЖЕННЯ КОМЕРЦІЙНОЇ ТАЄМНИЦІ

2.1. Законодавча база у сфері захисту комерційної таємниці

Законодавчий захист можна вважати правовою, організаційною системою. Законодавство - це фізична форма правових норм і норм та різних норм, що регулюють споріднену групу. Юридичний аналіз у сфері комерційної конфіденційності дозволяє зупинитися на окремій галузі - Законі про підприємництво.

Вивчення правовідносин, що виникають у процесі підприємницької діяльності, як відомо, стосується предмету підприємницького права. Види соціальних норм

(соціальні норми - це правила поведінки, встановлені суспільством і є стандартами соціальних відносин) Відомі організаційні правила (правила громадських організацій, встановлені законом). Положення закону про приватні компанії стосуються зовнішніх форм юридичних осіб.

Ці правила базуються на загальних правилах і застосовуються лише до відносин, що виникають у компаній. Це правила внутрішньої поведінки. Юридично збір та використання нелегальної комерційної таємниці належить до однієї з груп, яка демонструє недобросовісну конкуренцію. У разі недобросовісної конкуренції необхідно посилатися на спеціальний закон, зокрема - на український закон "Про захист від недобросовісної конкуренції" [7]. Поглиблене дослідження недобросовісної конкуренції є дуже важливим для розкриття змісту комерційної таємниці. Код. 505 Цивільного кодексу України визначає значення терміна "комерційна таємниця" [4].

Це конфіденційна інформація повністю або частково, а загальний зміст її компонентів невідомий і недоступний, тому вона має комерційну цінність і вважається належним кроком для захисту конфіденційності, прийнятої для особи, яка керує нею на законних підставах. інформація.

Способи захисту прав учасників на передачу інформації такі різноманітні, як:

• усунення бар’єрів у здійсненні прав;

• відновлення прав було порушено з будь-якої причини;

• Відповідальність за впровадження порушує законодавство.

Закон не тільки захищає особисті права на інформацію, але також захищає комерційну таємницю, конфіденційну інформацію, що охороняється державою. включає заходи щодо захисту прав та законних інтересів громадян в умовах безладного управління та зловживання владою, при цьому особливе місце займає спікер . Вам слід звернути увагу на деякі питання, пов’язані з використанням (у тому числі незаконним) торгових марок та послуг, а також торгових марок. Відносини в результаті придбання та перевірки товарних знаків та послуг регулюються Законом України від 15.12.93 № 3689-XII "Про захист права на товарні знаки товарів та послуг". Порядок використання товарного знака регламентується спеціальним законом, який є підзаконним актом компанії, затвердженим ЦВК і РНК 22 червня 1927 р. Товарним знаком є товарний знак, розміщений на промисловій та комерційній продукції (або

упаковці) . У разі реєстрації Міжнародним бюро Світової організації інтелектуальної власності для маркування продукції та послуг, що відповідають міжнародним стандартам класифікації, повинна бути доведена справжність міжнародної реєстрації. Предметом злочину, згаданим у ст. 229 Кримінального кодексу України (незаконне використання товарного знака), може бути: а) знак іншої особи, тобто ярлик, характерний для товарів та послуг, які вони мають державний патент; Б) маркування товару. Незаконне використання товарного знаку іншої особи навмисно з метою отримання прибутку.

2.2. **Характеристика суб'єктів і об'єктів охорони комерційної таємниці**

Як у 231 Кримінального кодексу України про відповідальність за комерційний шпигунство, так і у ст. 232 Кримінального кодексу України про видачу комерційної таємниці призначений для захисту купців. Тільки інформацією, що має комерційну таємницю, можна зловживати при розголошенні комерційної таємниці, комерційному шпигунстві. За розголошення нелегальної комерційної таємниці передбачається покарання лише за спеціальні суб'єкти господарювання , тобто особи, з якими комерційна таємниця пов'язана з їх професійною чи службовою діяльністю, і юридично зобов'язані захищати цю інформацію.

Податкові інспектори, банки, правоохоронні органи та інші, які мають законне право на доступ до конфіденційної інформації або мають доступ до такої офіційної інформації, можуть бути ідентифіковані як перевізники та капуста. Закон України від 25 березня 1992 р. № 2229-XII "Про Службу безпеки України" говорить: "... інформація, що містить державну таємницю, офіційну та комерційну, а також конфіденційну інформацію не може розголошуватися. Це може завдати шкоди країні національної безпеки України, поваги до людини або порушення її законних прав ... "[48]. Український закон від 4 грудня 1990 р. "Про регіональну податкову службу України" із змінами від 24 грудня 1993 р. Запроваджує обов'язки податкових інспекторів.

Для захисту службової таємниці [6]. З теоретичної точки зору такий злочин розголошення комерційної таємниці охоплює діяння, вчинені умисно громадянами України, іноземцями, особами без громадянства, і є порушенням умов розголошення такої інформації (без дозволу її власників). Бізнес-шпигунство - це умисний злочин. Мета може бути прямою або

непрямою. Оскільки захист комерційної таємниці полягає у забезпеченні фінансових інтересів компанії, відповідно, безпека та інформація про сечу компанії переплітаються.

2.3. **Розроблення системи захисту інформації з обмеженим доступом, що може бути предметом комерційної таємниці суб'єкта господарювання: технологічний і методичний аспекти**

Юридична обробка соціальних мереж у галузі комерційної таємниці передбачає розуміння здатності суб'єкта володіти правами та обов'язками комерційної таємниці, що вплине на необхідні характеристики логотипу - обов'язки та дозволи - права. Правова база правовідносин у галузі охорони комерційної таємниці включає такі речі, як правові звичаї, правовідносини, юридична відповідальність, правосвідомість тощо.

Емітенти прав інтелектуальної власності так чи інакше реагують на умови та дозволи, що містяться в законі. З огляду на такий підхід, неможливо визначити можливі організації для вжиття заходів щодо захисту конфіденційності певних підприємств, але також вимагає проведення (передачі контактів) від деяких інших людей, які взяли на себе контрактні зобов'язання. Збережіть надану їм інформацію. Майте на увазі, що правовий статус власника комерційної таємниці

визначається законом, він визначає позицію питання власності на комерційну таємницю стосовно держави, її органу та інших.

До повноважень СБУ входить подання органу державної влади пропозиції про обов’язковий перегляд. Щодо національної безпеки України, в тому числі призупинення роботи , пов'язаної з державною таємницею здійснюється в порушення встановлених правил (стаття 25 пункт 2 українського закону від 25 березня 1992 № 2229-XII «Про Службу безпеки України» Конфіденційна інформація передається до Департаменту приватних комунікацій та захисту інформації Служби безпеки України, а також до Ліцензійного центру України (рекомендації щодо умов нагляду, видачі, імпорту, експорту, продажу та використання IPO , а також служби захисту даних).

Зараз ми звернемося до деяких теоретичних питань, які є ключовими для створення системи юридичної охорони комерційної таємниці компанії. По-перше, процес узгодження придбань компаній, державних установ та адміністративних установ, українських партнерів та Компанії, замовників, підрядників, конкурентів із захищеною інформацією. Оскільки державна та приватно-приватна системи базуються на одних і тих же принципах, але мають свої юридичні характеристики, важливо розуміти організаційні та правові аспекти роботи, пов’язаної з отриманням ліцензій на доступ до бізнесу.

У світлі вищесказаного необхідно вивчити діяльність цих компаній, установ, неурядових організацій та управління ними, виходячи з права власників використовувати фінансові ресурси свого майна та принципів самоврядування. Українське законодавство надає приватному бізнесу в економіці, який не бере участь у вирішенні проблем регіональної безпеки, право встановлювати власну систему заходів щодо захисту конфіденційної інформації задля конфіденційності бізнесу.

Доступ до захищеної інформації повинен базуватися на принципі "потрібно знати". Право на економічну структуру бізнесу, ведення бізнесу, роботу з інформацією відповідно до законодавства України може бути віднесено до категорії "комерційна таємниця", воно повинно бути юридично забезпеченим документами, що стосуються формату. Тільки після додавання необхідних елементів до учасника та інших документів, офіційно наданих компанії, ви справді перевіряєте право на комерційну таємницю. Зокрема, слід викласти

положення, що вказують на те, що компанія має право торгувати з конфіденційністю та захистом. Як правило, порядок захисту інформації, що містить комерційну таємницю, встановлюється керівником компанії. Документи будуть включені, а відповідні пункти можуть включати :. Альянс, Угода про самоорганізацію, Колективний договір розробляють ці правила, але норми комерційної таємниці та приватного права не включені в документи компанії. Відповідно до Трудового кодексу України та українського Закону "Про спільні переговори" (1 липня 1993 р. № 36), колективний договір повинен бути укладений з власником компанії або кваліфікованим органом та колегами, незалежно від форми власності ферми з використанням працівника та законних повноважень. час зміст спільних підприємств значно розширився, і багато з них включають положення про торговельну таємницю. Детально описаний порядок обробки ділової інформації, визначено спільну відповідальність керівництва та персоналу та відповідальність за невиконання ділової таємниці бізнес-системи. Особлива роль колективного договору в правовідносинах через суворість комерційної таємниці полягає в тому, що керівництво зобов’язане надавати консультації персоналу, що займається питаннями конфіденційності компанії, необхідними правилами та будівельними ресурсами.

Звичайні бали визначають відповідальність за порушення системи логотипів, що зберігаються в комерційній таємниці, це вдосконалення прав управління кордонами, наприклад, може бути покладено на злочинців з дисциплінарною відповідальністю, як він описав Трудовий кодекс в Україні. Крім того, суть контракту полягає в тому, щоб забезпечити персонал навчанням правилам ведення бізнесу, пов’язаним з приватністю бізнесу. В основному система приватного життя бізнесу відрізняється від державної. Коли державна таємниця розкрита, держава зазнає матеріальної або моральної шкоди. Якщо розкриття інформації пов’язано з помилкою, допущеною працівниками компанії, працівники зазнали економічної шкоди, а в деяких випадках компанія може збанкрутувати. Загальні умови найму працівників з комерційною таємницею, викладені в колективному договорі, поширюються на всі колективи, а не лише на працівників, які мають доступ до конфіденційної інформації.

Підприємці повинні зберігати конфіденційність під час трудової діяльності, пов'язаної з державною конфіденційністю. Відповідальність за розголошення

державної таємниці покладається на самого працівника, а іноді і на його керівництво, яке належним чином не контролює свою діяльність. Права корпорації, корпорації вимагати відшкодування збитків у разі пошкодження та збитків у разі розголошення конфіденційної ділової інформації через їх помилку з'являться лише в тому випадку, якщо умови асоціації мають підстави та законодавчі вимоги. Компанії, створені та діють на основі угоди про асоціацію, в якій відсутні нормативні акти, включають право на торгівлю, зокрема, передбачене законом, шляхом подання відповідних нормативних актів. Слід зазначити, що компанії мають право добровільно консолідувати свою виробничу та господарську діяльність, якщо це не суперечить антимонопольному законодавству в Україні. Відповідно до чинного законодавства підрядниками можуть бути асоціації, компанії, кооперативи, корпорації, утворені у формі принципів, простору та інших принципів [66]. У регіонах компаній, зареєстрованих в Україні, можуть бути компанії з інших регіонів. Організації діють на підставі договору або угоди, затверджених їх засновниками або власниками. Українські компанії та інші уряди, які є частиною інституційної структури прав юридичних осіб. Важливо визнати можливість того, що кожен засновник приєднається до організації із власною політикою конфіденційності. Всі засновники або ряд мають право здійснювати спільну діяльність з охорони та збереження комерційної таємниці. Закон надає засновникам асоціації право вирішувати питання спільної власності на комерційну таємницю відповідно до угоди про асоціацію. У цьому випадку кожен засновник оцінює можливість незалежності та відповідну точку зору. Для засновника або власника компанії, який має намір забезпечити конфіденційність бізнесу та забезпечити його захист, він повинен чітко представляти значення та обмеження, їх фактична реалізація може допомогти запобігти витоку конфіденційної інформації. Закон передбачає право організації вживати правових заходів для забезпечення охорони комерційної таємниці, що має відображатись у нормах трудового законодавства, які вимагають не лише працівників, а й адміністрації. Керівництво прагне:

• створити умови, необхідні для дотримання Компанією правил доступу до конфіденційної ділової інформації та дотримання всіма працівниками

встановлених правил для забезпечення безпеки інформації з обмеженим доступом (включаючи конфіденційну інформацію та пов’язаний бізнес) ;

• отримати посадову інструкцію працівника, щоб прийняти рішення щодо кожного працівника щодо необхідності охорони комерційної таємниці та навчитися запобігати можливій конфіденційній інформації;

• Пропонує інструкцію щодо правил, що стосуються доступу - до інформації, що стосується конфіденційності торгової конфіденційності (при бухгалтерському обліку в державах, пов’язаних із переведенням на іншу посаду);

• Інструкції щодо ступенів потенційних клієнтів Правильні в'їзні собаки Особисті зобов'язання щодо збереження комерційних секцій "Мирної Гококобми Лімітед". Розробка Larkin реалізує комплекс організаційних, інших неверно технічних заходів, попередню інформацію про комерційну комунікацію.

• Контролювати повідомлення про дотримання працівниками встановлення вимог комерційної конфіденційності.

МЕТОДИ ІНФОРМАЦІЙНОГО ШПИГУНСТВА ТА ПРОТИДІЯ ЙОМУ

3.1. **Приховування правопорушником передачі розвіданої інформації, що опрацьовується в комп'ютерній мережі**

Методи злому комп'ютерної мережі, спрямовані на подальший викрадення даних, різні, і найбільш ефективним є встановлення програми розмітки системи. Це залежить від мети, наприклад, програма маркування може відображати пароль користувача або доступну інформацію, необхідну для дисків, відповідно до конкретної політики .

Усі адміністратори вживатимуть відповідних заходів, щоб запобігти спробі логотипу надіслати попередньо зібрану електронну адресу порушнику. Це змусить хакерів винаходити нові способи злому комп'ютерної мережі. Найскладнішою частиною розвідувальної роботи порушника є дві речі:

• Створення власної програми ("Троянський кінь");

• Передача інформації за допомогою інтелекту пошкоджує велику кількість сигналів та інформації.

Поки існує людство, існує проблема обміну інформацією. З одного боку, люди, які хочуть спілкуватися та ділитися інформацією, з іншого боку, вони намагаються приховати від незнайомців природу та реальність передачі. Таким чином, людство постійно вдосконалює механізми профілактики та її охоплення. використовує криптографічні прийоми та візуальні прийоми для приховування інформації.

Криптографія - це логотип, який модифікує дані, щоб ви могли зрозуміти їх лише на початку.

Стеганографія - це метод перетворення інформації, щоб приховати існування секретного повідомлення. Слово "стеганографія" походить від слова "стеганографія" - секретна "графіка" - запис, що буквально означає "прихований запис" .

Застосування криптографії дозволяє зовнішньому монітору легко встановити правдивість передачі конфіденційних повідомлень, а застій - більше приховування для посилення захисту, може зашифрувати Всесвітню організацію охорони здоров'я ще більше конфіденційно.

Стагнографія припускає, що реальність будь-якого обміну даними не приховується, хоча повідомлення слід вважати цензурою. Таким чином, приховування факту існування секретного повідомлення означає не тільки (можливо, не багато) те, що курсор не може ідентифікувати повідомлення, коли бачить інше приховане повідомлення, але й те, що надіслане повідомлення не викликає підозр курсора. Приховане повідомлення - це секретне повідомлення всередині контейнера. Stagoki - це секретний ключ, необхідний для шифрування інформації. В залежності від числа рівнів безпеки (таких , як створення попередньо написане повідомлення), може бути один або більше Stego-пов'язаних систем .

Стратегія Stegenochannel - це канал для передачі конфіденційної інформації. Stag Container - контейнер з повідомленням всередині. Таким чином, конфіденційне опромінення здійснюється за допомогою подібних методів та процесів. Щоб бути надійним та викликати підозру, повинні бути дотримані певні вимоги, а саме:

• Контейнер сцени містить вбудоване повідомлення. Зовнішній контроль практично не відрізняється від очного контейнера;

• При побудові системи стигматизації слід припустити, що “цензор” (адміністратор системи) має повне уявлення про використовувану стенографічну систему та деталі її впровадження, але цінність розробника стигми не визнається. ;

• що лише власник ключа стига має можливість перевірити наявність конфіденційного повідомлення;

• Система stigo повинна бути встановлена таким чином, щоб лише власник ключа stigo міг витягнути повідомлення з контейнера stigo.

Приховане повідомлення, вбудоване в образ секретного контейнера повідомлень

1. Комп’ютеризована система діагностики Комп’ютеризована стенограма - це фрагмент стеганографії, який обговорює реалізацію стратегічних систем із використанням комп’ютерних технологій. Цифрова інформація часто передається у вигляді файлів за допомогою комп'ютерної системи стего, інструменту та інструментів, що використовуються для створення секретного каналу передачі

інформації за допомогою контейнера файлів слів та файлу повідомлень. Щоб уникнути підозр іноземців з-за кордону, насправді повідомлення (файл повідомлення) за допомогою жорсткого ключа являло собою "змішаний" контейнер файлу. Це не повинно призвести до змін основних можливостей файлового контейнера, заповненого цифровою інформацією.

2. Між найпростішим використанням комп’ютерної системи Stego та красивою лінією є багато спільного . Ви можете написати кілька рядків секретного повідомлення білими літерами на білому тлі текстового редактора оголошень Microsoft Word, наприклад пральних порошків. Білих букв на білому тлі не видно, і навіть той, хто користується спеціальним комп’ютером, може це показати. Звичайно, надійність такої системи дуже низька. Однак складні розширення комп'ютерної системи вже використовуються зловмисниками, особливо "вірусописателями".

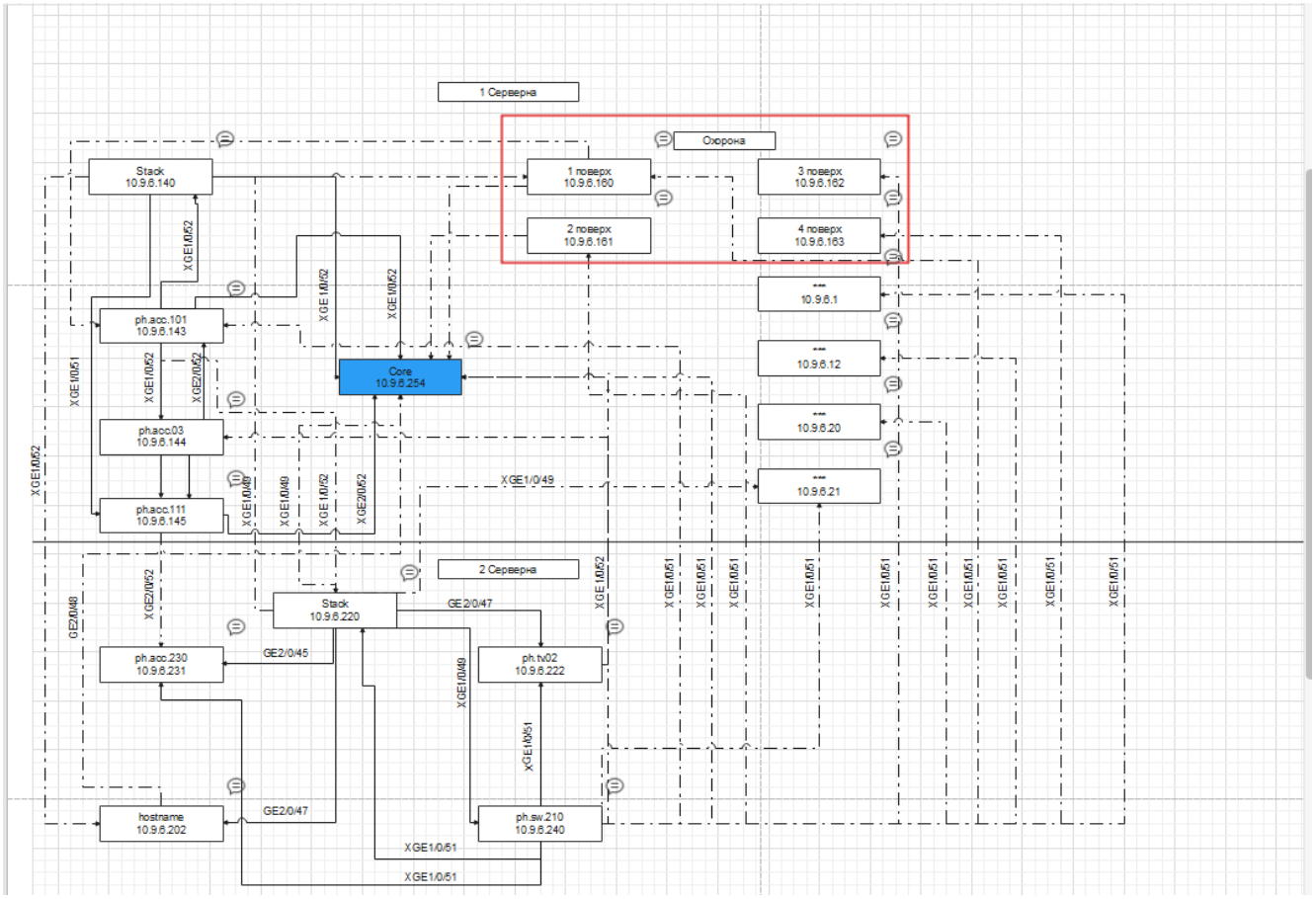
Це відомо, наприклад, як вірус під назвою "W32 / Per Run", він "ховає" своє тіло 18K у файлі jpg і фактично просто додай свій код в кінці файлу jpg. Що стосується стагнації, це дуже вдосконалений формат, але він дає уявлення про те, як створити широкомасштабну комп’ютерну систему «етикетки». Для цього план розмітки потрібно скласти з двох частин.

Розділ для початківців , який шукає лише найважливішу частину програми для позначення інших файлів, як правило, дуже малий, що полегшує встановлення. Однак найважливішою частиною контрольного списку є те, що його розмір може бути дуже великим, а ризик ідентифікації може бути зменшений. Є кілька дуже складних технік маскування. Наприклад, вірус Win 95 CJH встановлюється у файл "EXE" із використанням функцій портативної операційної системи (Windows) (починаючи з Windows 95).

У Windows виконуваний файл EXE може містити не тільки код, але і набагато більше даних - піктограми, інформацію про різні служби, додаткову інформацію, таку як імпортовані та імпортовані служби. Кожен тип даних, що зберігається у

PE-файлі, є унікальним об’єктом. Для зберігання всього матеріалу файл PE розділений на кілька частин фіксованого розміру. Кожен предмет починається з нової частини. Якщо обсяг не містить обсягу всього сегмента, ця частина не використовується і все ще є безкоштовною. Тому вільного місця у файлі PE завжди достатньо. Більшість з них - це перша частина, просто крутий вок (PE-голова), записаний файл . Ви можете приховати багато інформації в порожніх місцях, і жоден з розмірів файлів не зміниться або це не вплине на його продуктивність. Ця технологія маски дозволяє приховати встановлення програми розмітки вашого комп’ютера. Оцінка результатів програми - Файли знайдені. Можливості сучасних методів комп’ютеризованої стенограми можна виявити, проводячи експерименти, наприклад, рівномірно розподіляючи стереограмму. Однією з найпопулярніших в історії, яка може приховувати графічну інформацію (GIF. У форматі BMP) та аудіо (у форматі WAV), є програма S-Tools E. Brown. Це дозволяє не тільки приховати повідомлення, але й зберегти його за допомогою чутливого алгоритму, який забезпечить як таємну передачу секретного повідомлення, так і його стабільність.

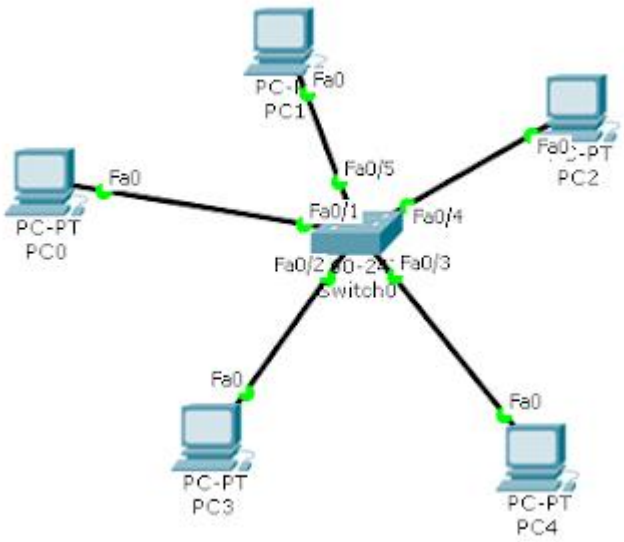
3.2. **Реализація локальной мережі та шифруваня інформації**



Створення з'єднання зірка

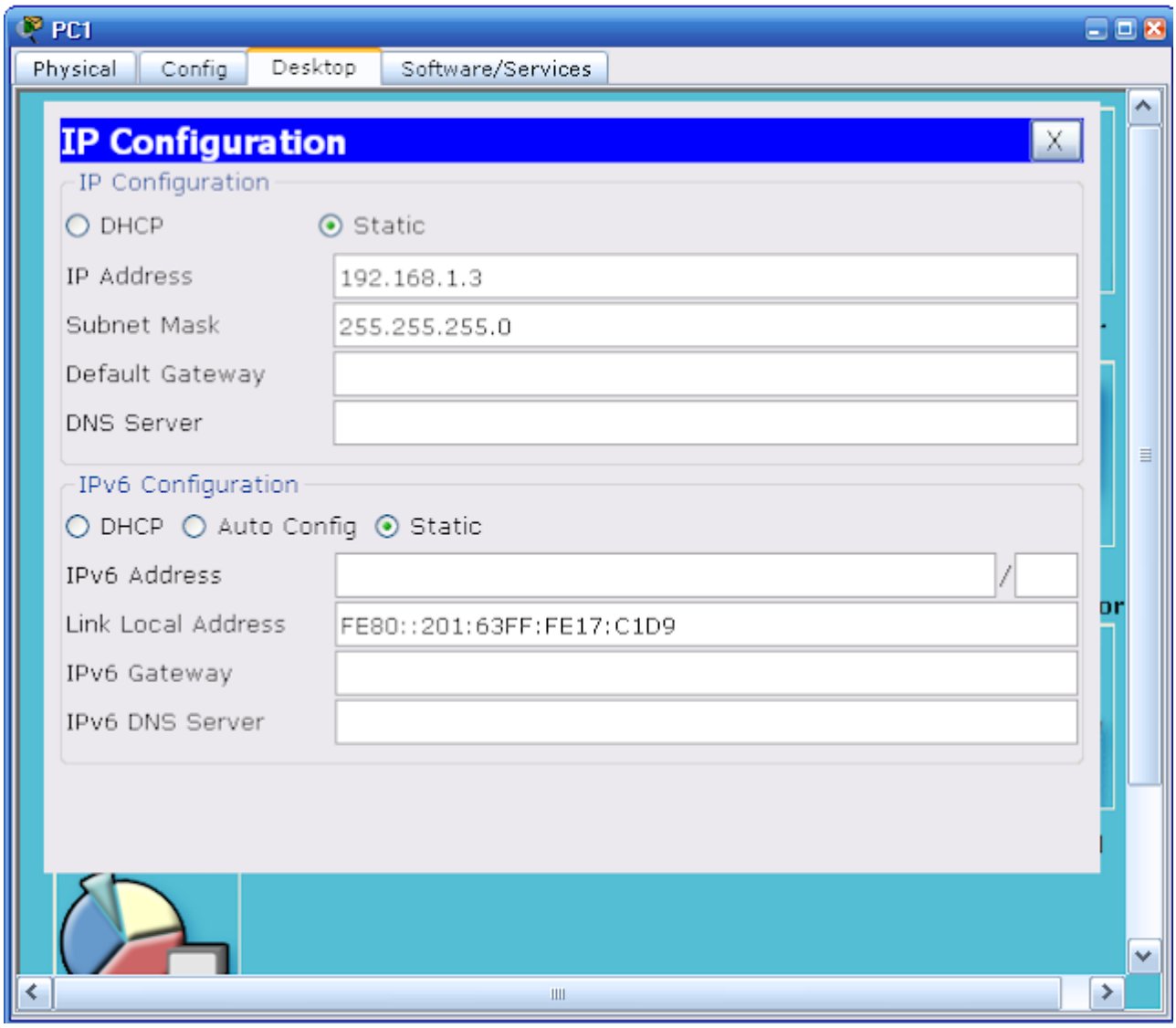
Для почтатку розташуємо всі елементи на формі. Розташуємо комутатор та 5 комп'ютерів.

Після цього з'єднаємо комп'ютери з комутатором кабелем типу вита пара.

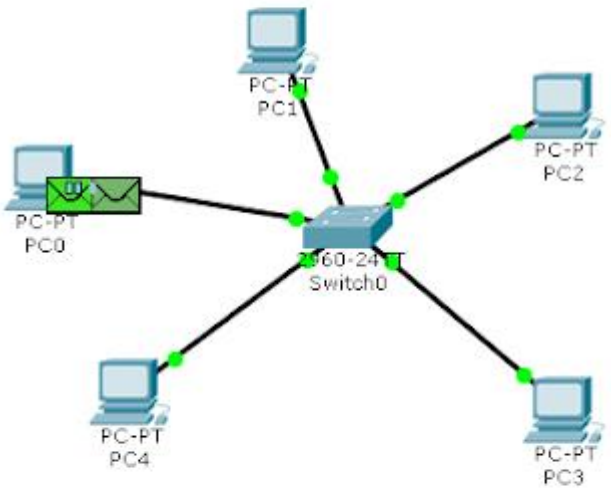


Спочатку при з'єднанні індикатори на кінцях кабелю зі сторони комутатора будуть мати оранжевий колір. Через деякий час коли комутатор сам налаштується індикатори на кінцях кабелів мають світитись зеленим.

Наступним кроком буде встановлення IP-адрес у комп'ютерах мережі. Оберемо інтервал 192.168.1.2 - 192.168.1.6. Маску встановимо 255.255.255.0. Зробити це можна перейшовши на вкладку "Desktop" і обравшт пункт IP Configuration.

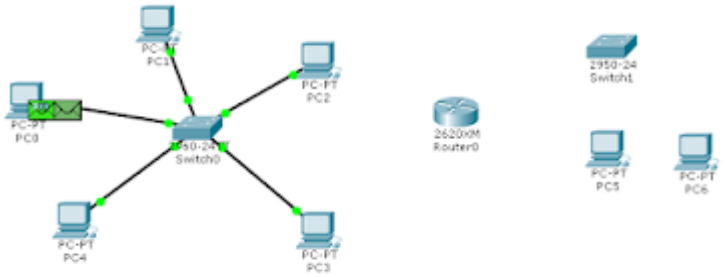


Після цього мережа буде здатна передавати пакети. Виконати це можна у режимі симуляції.

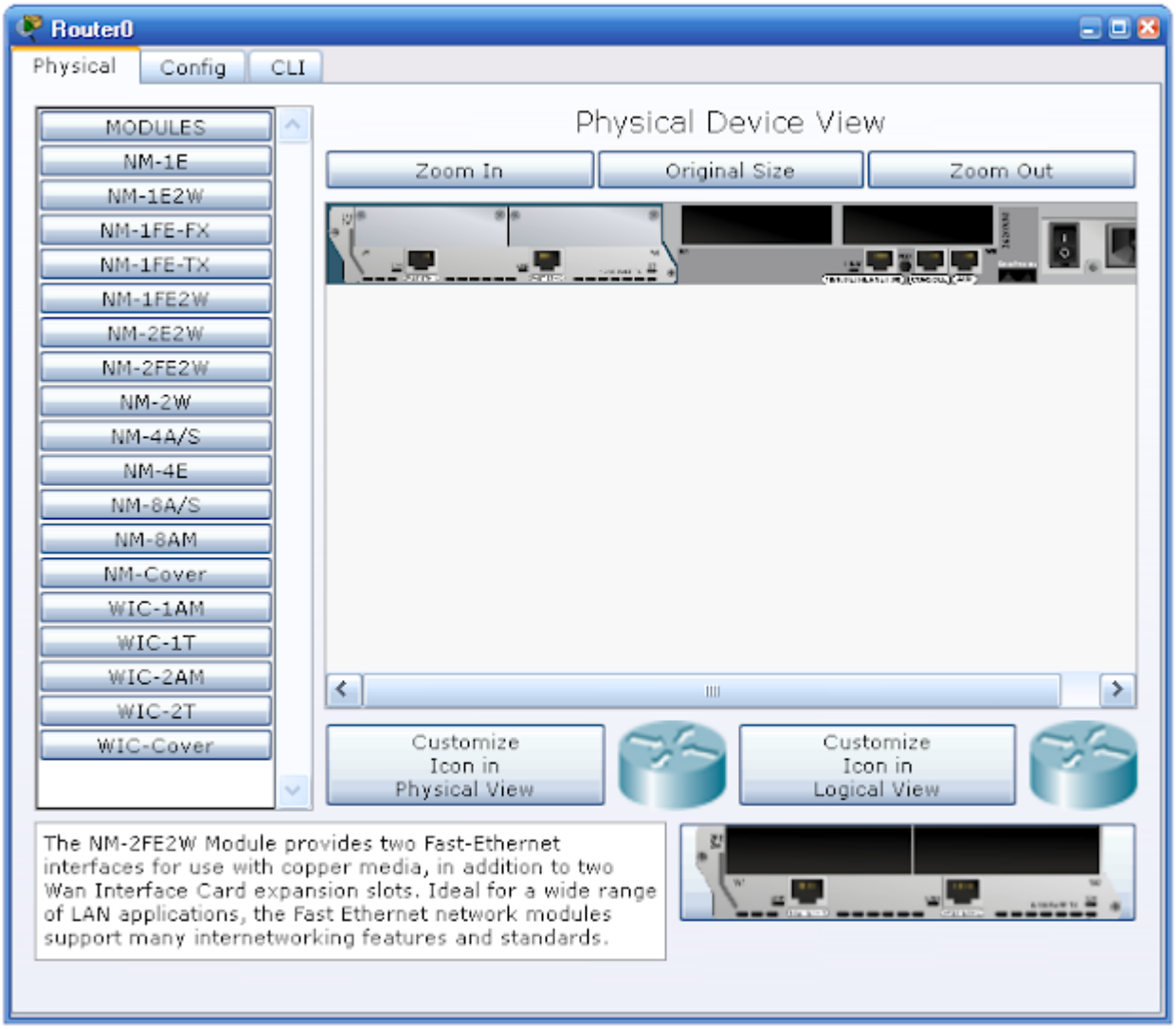


Додавання іншої мережі та з'єднання двох мереж роутером

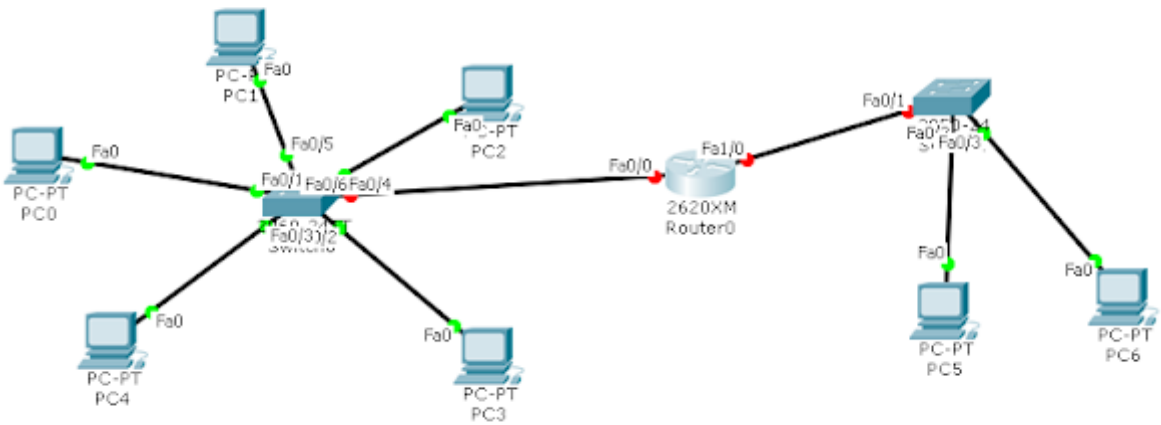
Додамо маршрутизатор та елементи іншої мережі.



Натиснемо на роутер і вкладці "Physical" вимкнемо маршрутизатор та додамо до нього модуль NM-2FE2W, який надає нам два порти FastEthernet. Не забудемо увімкнути маршрутизатор.

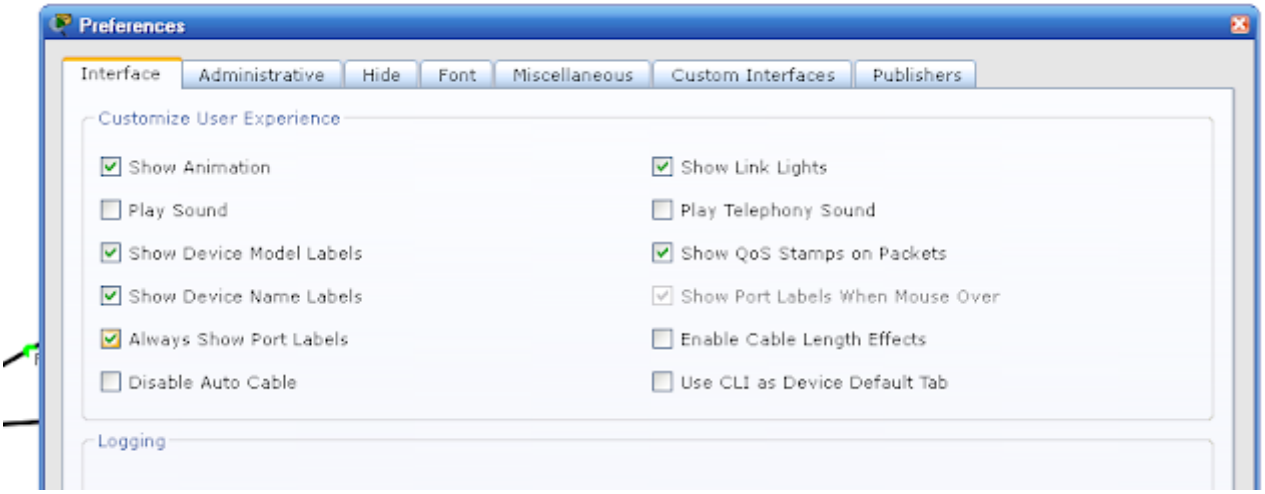


З'єднаємо елемнти витою парою через порти FastEthernet.

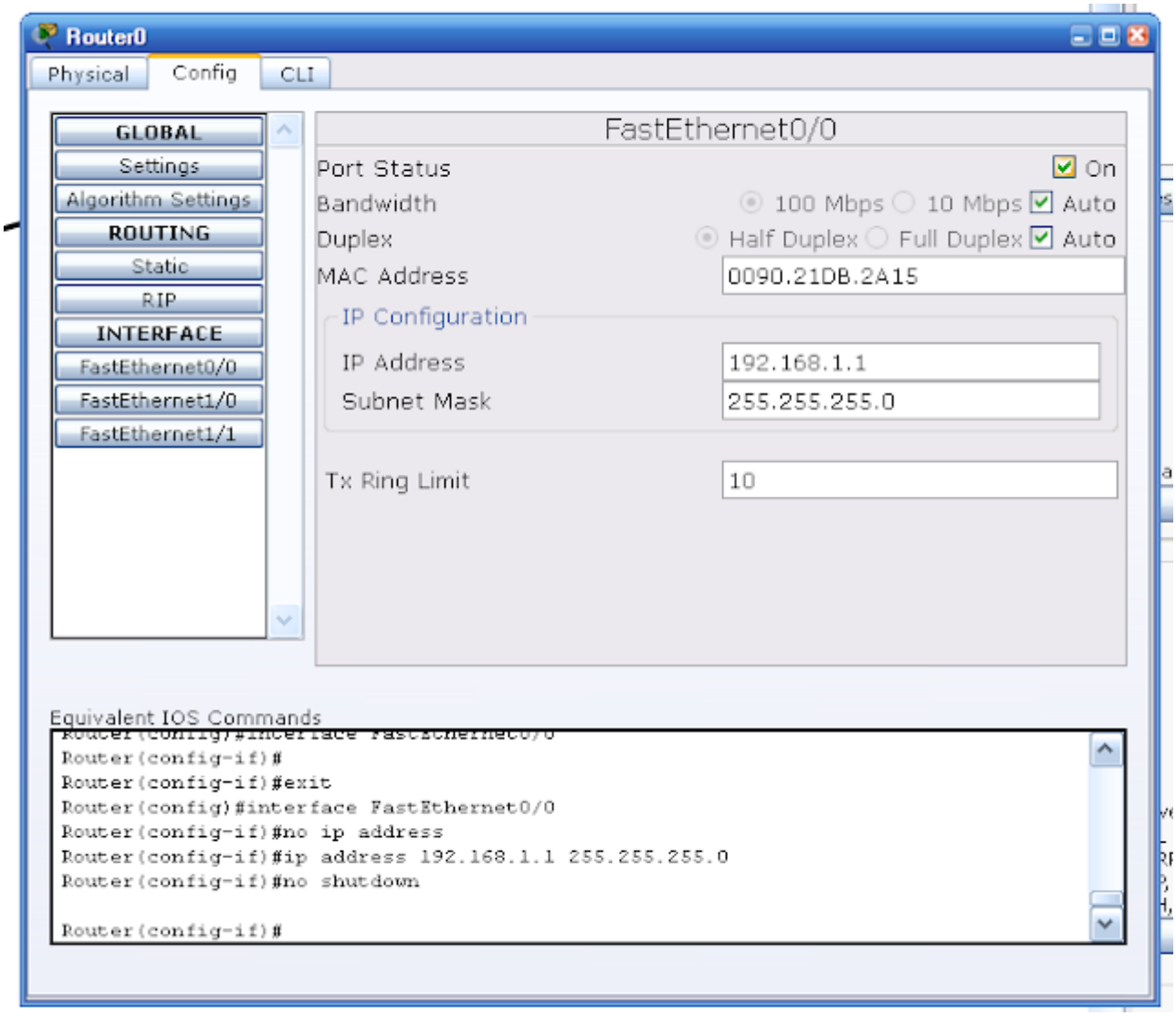


В даному випадку індикатори кабелів роутера будуть червоними, на відміну від комутатора.

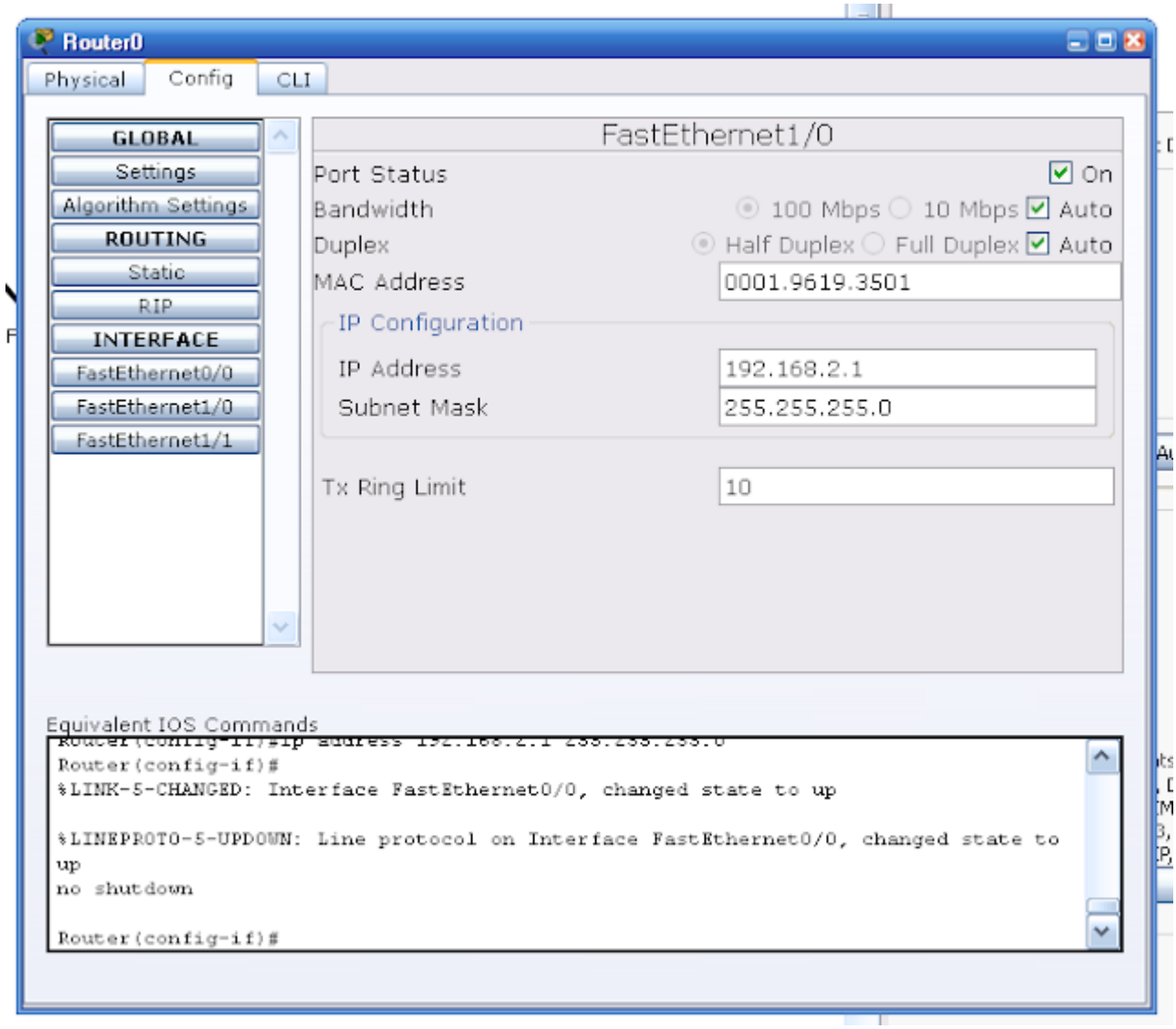
Налаштуємо інтерфейси. Для полегшення роботи з інтерфейсами увімкнемо відображення назв портів у пункті меню "Preferences" (Always show port labels).



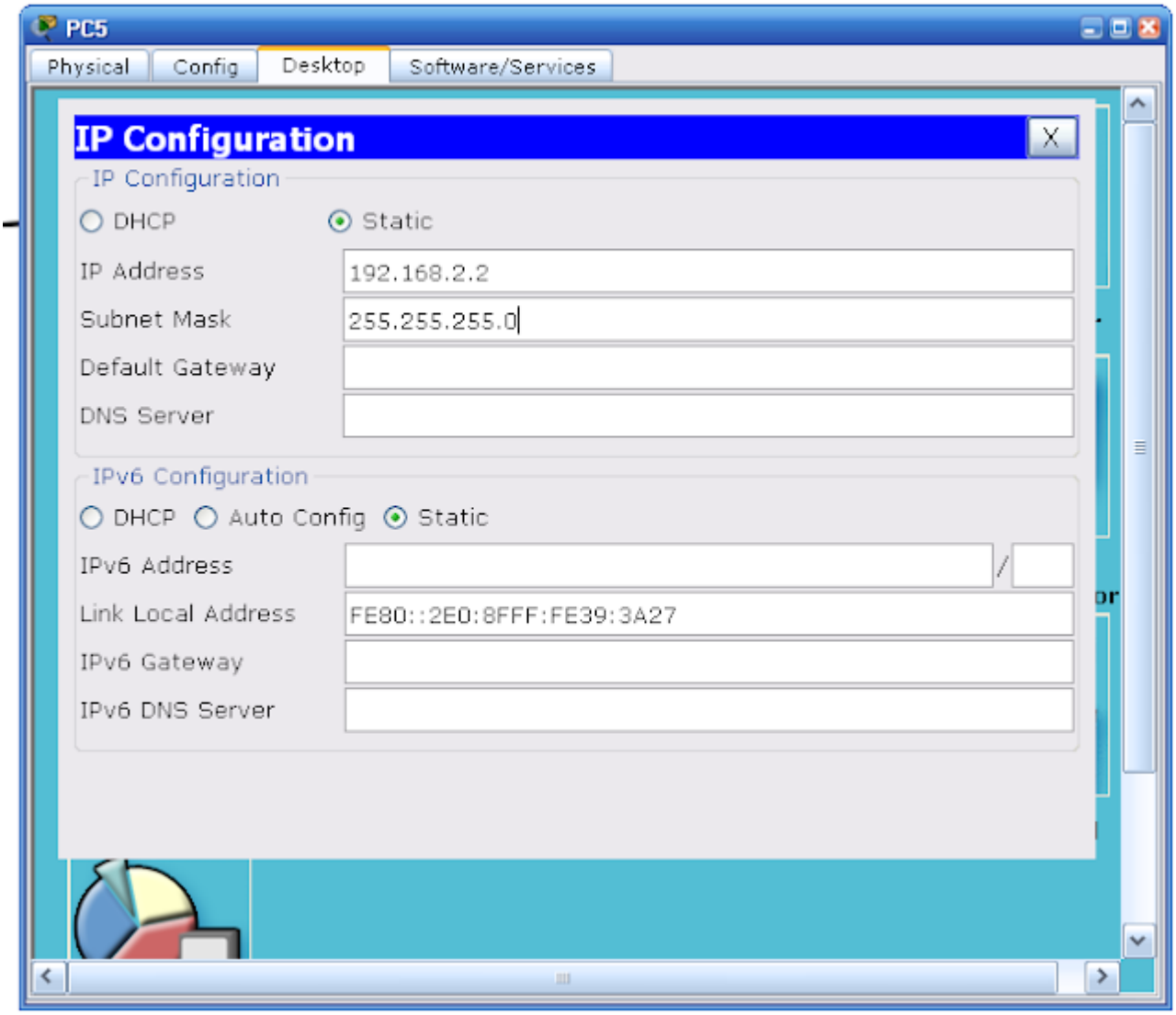
Після цього клацнемо на роутер та перейдемо у вкладку "Config" до інтерфейсу "FastEthernet0/0". Увімкнемо його. Та задамо IP-адресу 192.168.1.1, маску - 255.255.255.0.



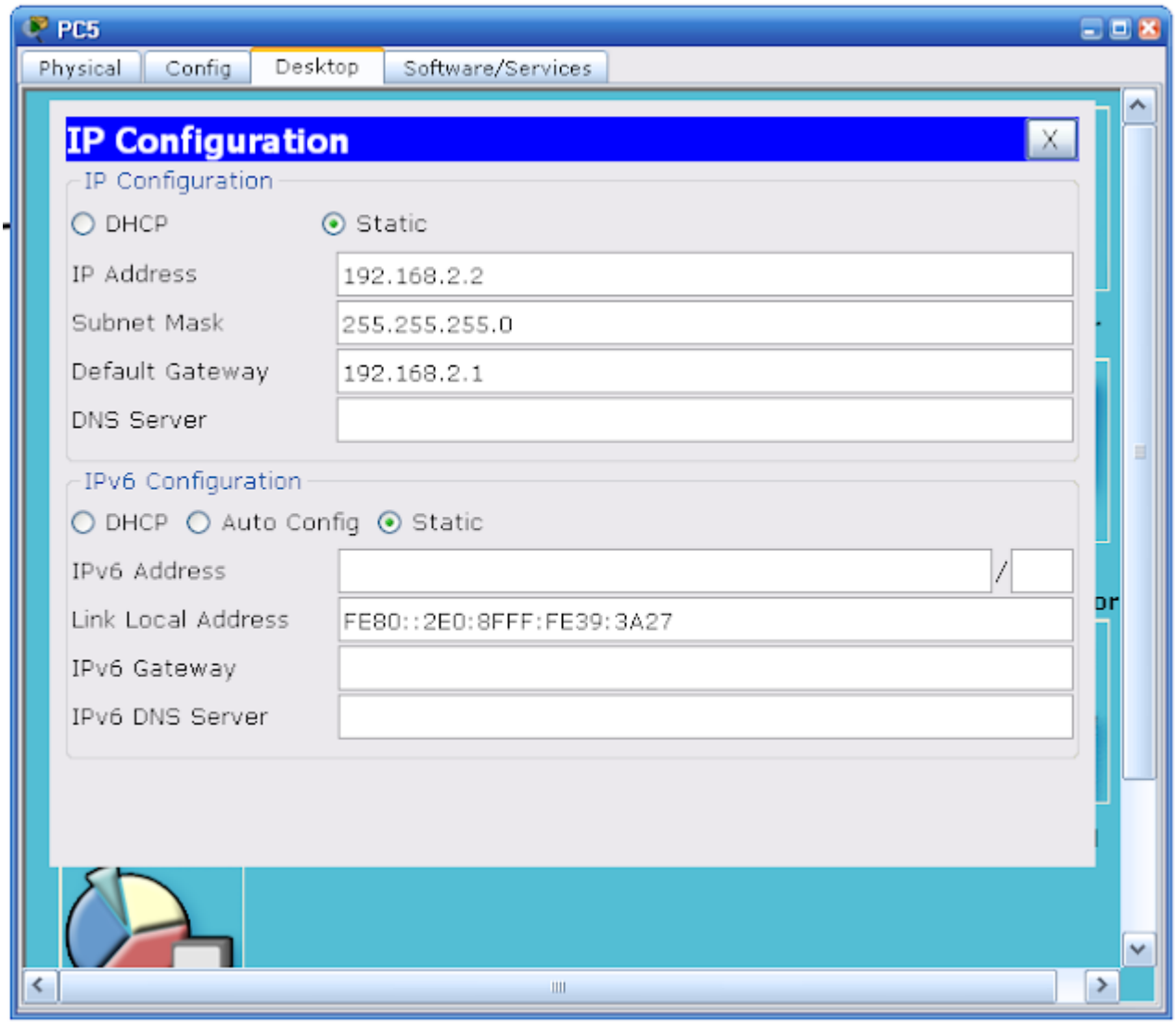
Інтерфейс "FastEthernet1/0" також увімкнемо та задамо IP-адресу 192.168.2.1, маску - 255.255.255.0.



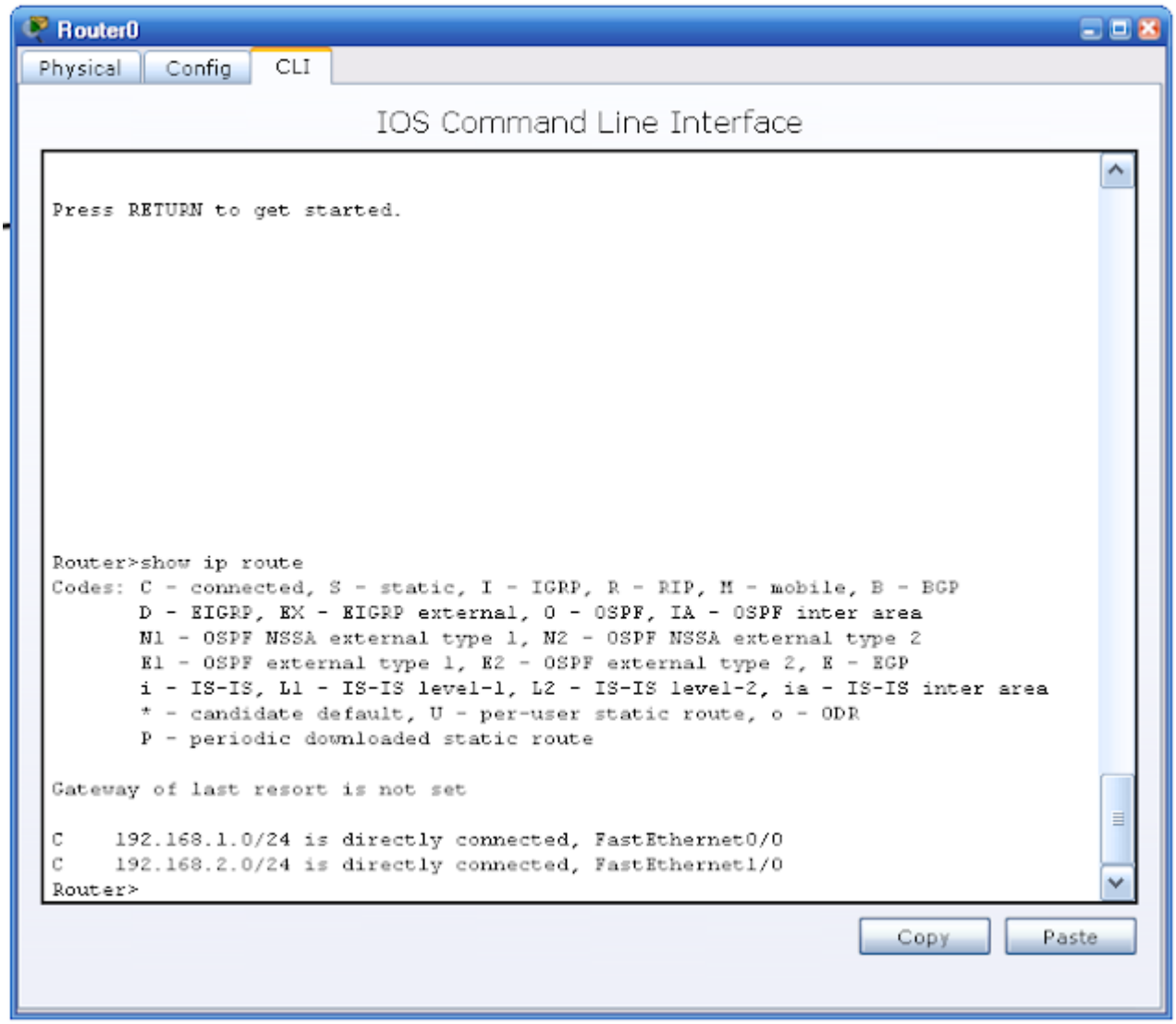
На комп'ютери правої мережі встановимо IP-адреси 192.168.2.2-192.168.2.3.



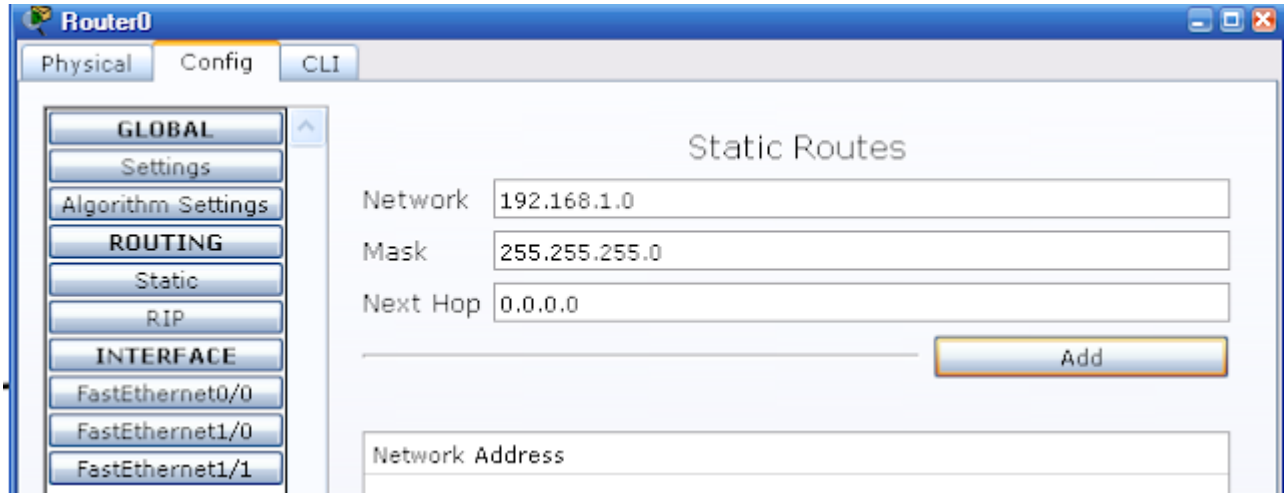
У IP-налаштуваннях всіх комп'ютерів допишемо "Default Gateway", який буде відповідати IP-адресі роутера з відповідним інтерфейсом, тобто для лівої мережі це буде значення 192.168.1.1, а для правої - 192.168.2.1.



Для певності, що маршрутизатор вірно передаватиме повідомлення можна переглянути його таблицю маршрутизації. Це виконується у вікні "CLI" командою "show ip route".



Також в деяких випадках варто задавати статичну маршрутизацію. Це виконується на вкладці "Config" у пункті "Static".



Мережі готові до використання. Результат тестування:

Successful	PC0	PC6	ICMP		0.000	N	0	(edit)	(delete)
Successful	PC5	PC1	ICMP		0.000	N	1	(edit)	(delete)
Successful	PC4	PC5	ICMP		0.000	N	2	(edit)	(delete)

3.3. **реалізація шифрування данних**

Блок схема шифрування та дешифрування інформації що передається по локальній мережі підприємства

Реалізація коду

```
private static readonly byte[] rgbKey = Encoding.UTF8.GetBytes("Ni=9OE=$i+62eprIuDr@ewOu5I9r34Ro"); // подмена под собственный ключ

private static readonly byte[] rgbIv = Encoding.UTF8.GetBytes("to$eO_e!maI*o3ut"); // подмена под свой вектор инициализации
public static string Encrypt(string originalString)
{
    if (string.IsNullOrEmpty(originalString))
    {
        throw new ArgumentNullException(
           "originalString",
           "The string which needs to be encrypted can not be null.");
    }

    using (var cryptoProvider = new RijndaelManaged())
    using (var memoryStream = new MemoryStream())
    using (var encryptor = cryptoProvider.CreateEncryptor(rgbKey, rgbIv))
    using (var cryptoStream = new CryptoStream(memoryStream, encryptor, CryptoStreamMode.Write))
    using (var writer = new StreamWriter(cryptoStream))
    {
        writer.Write(originalString);
        writer.Flush();
        cryptoStream.FlushFinalBlock();
        writer.Flush();
        return Convert.ToBase64String(memoryStream.GetBuffer(), 0, (int)memoryStream.Length);
    }
}

public static string Decrypt(string encryptedString)
{
    if (string.IsNullOrEmpty(encryptedString))
    {
        throw new ArgumentNullException(
           "encryptedString",
           "The string which needs to be decrypted can not be null.");
    }

    using (var cryptoProvider = new RijndaelManaged())
    using (var memoryStream = new MemoryStream(Convert.FromBase64String(encryptedString)))
    using (var decryptor = cryptoProvider.CreateDecryptor(rgbKey, rgbIv))
    using (var cryptoStream = new CryptoStream(memoryStream, decryptor, CryptoStreamMode.Read))
    using (var reader = new StreamReader(cryptoStream))
    {
        return reader.ReadToEnd();
    }
}
```

ВИСНОВОК

Сучасний етап розвитку бізнесу в Україні, питання, що стосуються комерційної таємниці та захисту, інфраструктури інформаційної безпеки, привертає увагу багатьох вчених та аналітиків з точки зору бізнесу. Креативна інформаційна безпека є важливою частиною національної інформаційної безпеки. Для вирішення питань інформаційної безпеки підприємства повинні мати стратегію інформаційної безпеки. В Україні спостерігається значне збільшення кількості комп'ютерних злочинів, пов'язаних із використанням інформаційних технологій та сучасних банківських операцій, незаконної діяльності, пов'язаної з використанням комп'ютерів. Наприкінці 1970-х років із інформаційною безпекою виникла ще одна проблема: невідома кількість електронних листів, що дивляться вниз? Мені надіслали запит, який зламав мій комп'ютер і погрожував знищити переваги електронної пошти. 1. Розслідування кримінальних справ за несанкціоноване втручання даних показує, що цього не можна зробити, не потрапивши незаконно в комп'ютерну мережу. Ці злочини стали звичайним явищем в місцях і банках: • перериванням від роботи у вигляді комп'ютерних банків і мереж на Інтернет - доступ до конфіденційної інформації, методи порушення безпеки правил ;

• відмивання грошей за допомогою електронних грошей;

• Шахрайство на рахунках клієнтів комерційних банків із використанням підроблених магнітних пластикових карток у міжнародній платіжній системі.

2. Захист інформації в терористичних мережах , пов'язаних з фінансовим, банківським, бізнесом та іншими фінансовими секторами вимагає впроваджень ефективних систем інформаційної безпеки , які відповідають реальному рівню ризики. Система захисту даних - це сукупність методів та інструментів,

організованих проблемами безпеки даних загалом для вирішення загальної проблеми, наприклад, забезпечення більш систематизованого рівня необхідного рівня захисту джерел інформації. Цілі інформаційної безпеки: інформація, що зачіпає юридичні, офіційні, комерційні, інтелектуальні та особисті інтереси, а також процеси обробки та передачі та інфраструктуру.

3. Захист інформаційних технологій - це складна система, яка є інформаційною безпекою. Основним захистом та юридичним захистом фінансової таємниці фінансової установи та захистом інформаційних технологій є штучні організаційні структури, що мають зв'язки та обміни в рамках функціонування єдиного рівня системи безпеки підприємства. Метою технічного захисту інформації, що міститься в комерційній таємниці, є запобігання розголошенню або пошкодженню цілісності інформації обмеженим доступом. Цього можна досягти шляхом створення механізмів для запобігання зловживанню комп'ютерними системами та мережами, автоматизовані системи можуть спричинити спотворення або руйнування даних чи носіїв інформації.

СПИСОК ВИКОРИСТАННИХ ДЖЕРЕЛ

1. Конституція України // Відомості Верховної Ради Украї- ни. — 1996. — № 30.
2. Господарський кодекс України // Відомості Верховної Ради України. — 2003.
3. Господарський процесуальний кодекс України // Відо- мості Верховної Ради України. — 1991. — № 6.
4. Цивільний кодекс України // Відомості Верховної Ради України. — 2003.
5. Закон України "Про оперативно-розшукову діяльність" від 18.02.1992 № 2135-XII (із змінам та доповненнями) // Відомості Верховної Ради України. — 1992. — № 22.
6. Закон України "Про державну податкову службу в Ук- раїні" від 04.12.1990 № 509-XII // Відомості Верховної Ради України. — 1991. — № 2.
7. Закон України "Про захист від недобросовісної конкурен- ції" від 07.06.1996 № 236/96-ВР // Відомості Верховної Ради України. — 1996. — № 36.
8. Закон України "Про банки і банківську діяльність" від 07.12.2000 № 21231-III // Відомості Верховної Ради Ук- раїни. — 2000. — № 42.
9. Постанова Кабінету Міністрів України "Про перелік відо- мостей, що не становлять комерційної таємниці" від 09.08.1993 № 611 // Зібрання Постанов Уряду України. — 1993. — № 12.
10. Указ Президента України "Про заходи щодо забезпечення підтримки та подальшого розвитку підприємницької діяльності в Україні" від 15.07.2000 № 906/2000 // Офіційний вісник України. — 2000. — № 7.
11. Наказ Міністра внутрішніх справ України "Про затверд- ження інструкції про порядок видачі суб'єктам підприєм- ницької діяльності ліцензій на надання послуг по охороні колективної і приватної власності, а також охороні гро- мадян, монтажу, ремонту і профілактичному обслугову- ванню засобів охоронної сигналізації" від 28.02.1994
№ 112.

12. Наказ Ліцензійної палати України і СБУ “Про умови і пра- вила провадження підприємницької діяльності (ліцензій- ні умови) з розроблення, виготовлення і реалізації спе- ціальних технічних засобів (в тому числі іноземного виробництва) для зняття інформації з каналів зв’язку, ін- ших засобів негласного отримання інформації та контроль за їх дотриманням” від 07.04.1999. — 30/76.
13. Абрамов В., Радомисельский М. Підприємництво, малий бізнес і ринкова конкуренція // Економіка України. — 1995. — № 11. — С. 27–35.
14. Андрощук Г., Крайнев П. П. Економічна безпека підпри- ємства: Захист комерційної таємниці. — К.: Вид. дім “Ін Юре”, 2000. — 398 с.
15. Андрощук Г., Работягова Л. Н. Патентное право: правовая охрана изобретений. — К., 2001.
16. Андрощук Г. О. Правове регулювання захисту комерційної таємниці в Україні // Адвокат. — 1997 — № 4 (7). — С. 49– 53.
17. Афанасьев В. Г. Системность и общество. — М.: Политиз- дат, 1980. — 95 с.
18. Барановский А. Экономическая безопасность государства
// Финансовая Украина. — 1996. — № 22. — С. 32–36.
19. Безопасность бизнеса: Справочное пособие / Под ред. Ю. И. Когута. — К.: Журналист, 1993. — 102 с.
20. Вус М. А., Морозов В. Л. Информационно-коммерческая безопасность. — М.: Общество “Знание”, 1993. — 57 с.
21. Винокуров Ю., Прутник Е. Комерційна таємниця банку та правове забезпечення її функціонування та захисту. — Донецьк: Донбас, 1999. — 235 с.
22. Гаврыш В. Практическое пособие по защите коммерчес- кой тайны. — Симферополь: Таврида, 1994. — 72 с.
23. Гасанов Р. М. Шпионаж и бизнес. — М.: Международные отношения, 1993. — 119 с.
24. Гладишенко М. І. Правові та організаційні аспекти діяль- ності підприємця для захисту комерційної таємниці // Персонал. — 2005. — № 3. — С. 51–55.
25. Горячева К. Фінансова безпека підприємства, сутність та місце в системі економічної безпеки // Економіст. — 2003. — № 8. — С. 23–28.

26. Гримблат С. О., Кузнецов С. А. Безопасность предприни- мательской деятельности: Учеб.-практ. пособ. — Харьков: Наука и жизнь, 1998. — 93 с.
27. Гурин А. А., Гурин С. А. Экономическая безопасность орга- низации. — СПб.: Питер, 2002. — 160 с.
28. Домарев В. Каналы утечки информации // Бизнес и безо- пасность. — 1997. — № 1. — С. 17–25.
29. Єрмаков І. Б. Економічна безпека як об’єкт менеджменту // Бізнес і безпека. — 2002. — № 4. — С. 11.
30. Дячук І. В. Розвиток інноваційного підприємництва як стратегічний фактор безпеки бізнесу // Галицькі контрак- ти. — 2005. — № 5. — С. 13–17.
31. Економіка підприємства / За ред. С. Ф. Покропивного. — К., 2000. — С. 526.
32. Задірака В. К. Методи захисту фінансової інформації. — Тернопіль: Збруч, 2000. — 460 с.
33. Зубок М. І. Безпека підприємницької діяльності: Норма- тивно-правові документи комерційного підприємства, бан- ку. — К.: Істина, 2004. — 144 с.
34. Зубок М. І. Безпека банківської діяльності: Навч. посіб. — К.: КНЕУ, 2002. — 190 с.
35. Ильяшенко С. Н. Составляющие экономической безопас- ности предприятия и подходы к их оценке // Актуальні проблеми економіки. — 2003. — № 3. — С. 12–19.
36. Кабірова Н. Мовчання ягнят: як примусити персонал зберігати секрети фірми // Галицькі контракти. — 2004. — № 45. — С. 34–36.
37. Клеков О. Банківська безпека. — К.: Бліц-інформ, 1997. — 83 с.
38. Козакевич Б. Т., Кочев Н. В. Предпринимательство в опас- ности: способы защиты. — М.: Юрфак МГУ, 1992. — 154 с.