Список літератури

1. *Валиев К.А.* Квантовая информатика: компьютеры, связь и криптография / Валиев К.А. // Вестник РАН. – Том 70. – № 8, 2000. – С. 688–695.
2. Физика квантовой информации: Квантовая криптография. Квантовая телепортация. Квантовые вычисления / *С.П. Кулик, Е.А. Шапиро* (пер. с англ.); *С.П. Кулик, Т.А. Шмаонов* (ред. пер.); *Д. Боумейстер* и др. (ред.). – М. : Постмаркет, 2002. – С. 33–73.
3. *Слепов Н.* Квантовая криптография: передача квантового ключа. Проблемы и решения // Электроника: НТБ. – 2006, №2. – С. 54–61.
4. *Василиу Е.В., Воробиенко П.П.* Проблемы развития и перспективы использования квантово-криптографических систем // Наук. праці ОНАЗ ім. О.С. Попова. – 2006, № 1. – С. 3–17.
5. *Корченко О.Г.* Сучасні квантові технології захисту інформації / *Корченко О.Г., Василіу Є.В., Гнатюк С.О.* // Захист інформації. – №1, 2010. – С. 77–89.
6. *Василиу Е.В.* О надежности квантовых протоколов распределения ключей. I Протоколы с передачей кубитов // Наукові праці ОНАЗ ім. О.С. Попова. – 2007, №1. – С. 5-17.
7. *MagiQ.* Products. QPN Security Gateway. [Електронний ресурс]. – Режим доступу: <http://www.magiqtech.com/MagiQ/Products.html>.
8. *ID* Quantique. Clavis id3000. [Електронний ресурс]. – Режим доступу: <http://www.idquantique.com/products/clavis id3000.html>.
9. *ID* Quantique. Cerberis. [Електронний ресурс]. – Режим доступу: <http://www.idquantique.com/products/cerberies.htm>.
10. *Синельников А.* Шифры советской разведки. [Електронний ресурс]. – Режим доступу: <http://hronos.km.ru/statii/2008/shifr5.html>
11. *Нильсен М., Чанг И.* Квантовые вычисления и квантовая информация. – М. : Мир, 2006. – 824 с.
12. *Wooters W.K., Zurek W.H.* A single quantum cannot be cloned // Nature. – 1982. – V. 299. – P. 802.
13. *Гомонай О.В.* Лекції з квантової інформатики: Навчальний посібник. – Вінниця: О.Власюк, 2006. – С. 62–74.
14. *Shannon C.* Communication Theory of Secrecy Systems, Bell Systems Technical Journal, Vol. 28, pp. 656–715, 1949.
15. *David J.C. MacKay.* Information Theory, Interference and Learning Algorithms. – Cambridge: Cambridge University Press, 2003. – ISBN 0-521-64298-1.

Надійшла 16.03.2010

УДК 681.3 **Сірченко Г.А.**

ЗАДАЧІ ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ТА ДОСТУПНОСТІ ІНФОРМАЦІЙНИХ ОБ'ЄКТІВ В КОМУНІКАЦІЙНИХ МЕРЕЖАХ

Вступ

Задача забезпечення усіх основних функціональних властивостей захищених систем, в тому числі і цілісності та доступності їх інформаційних ресурсів, може вирішуватися як загальносистемними засобами технічного захисту інформації (ТЗІ), так і засобами, які є вбудованими в елементи таких автоматизованих систем (АС). При цьому можна і слід говорити про необхідність забезпечення цілісності та доступності ресурсів по відношенню до кожного з елементів АС, в тому числі по відношенню до телекомунікаційної мережі (ТКМ) АС, та застосування у складі цієї підсистеми певних методів, способів та засобів забезпечення захисту проти загроз цілісності та доступності інформаційних об'єктів.

Аналіз публікації

З матеріалів досліджень, викладених в [1,2,3] витікає, що до складу комунікаційної мережі (КМ) (і, відповідно, засобів захисту кожної з властивостей захищеності інформаційних ресурсів КМ входять засоби забезпечення обміну інформацією (елементи телекомунікаційної мережі) з їх засобами забезпечення відповідних властивостей захищеності в телекомунікаційних мережах КМ (і, зрозуміло, в засобах обміну інформацією локальних обчислювальних мереж, як елементів таких КМ). Це дозволяє сформулювати

висновок про суттєву вразливість стану захищеності КМ як раз через телекомунікаційні мережі, канали обміну інформацією та через їх елементи, а, відтак, це означає актуальність та важливість досліджень та розробок щодо методів, способів, засобів та методик забезпечення властивостей захищеності інформації в таких мережах, каналах обміну інформацією та їх елементах.

В той же час існуючі засоби забезпечення окремих функціональних властивостей захищеності, зокрема в частині контролю, контролю та поновленню цілісності, цифрового підпису інформаційних ресурсів вузлів різних рівнів та в засобах телекомунікаційної мережі не завжди можуть забезпечити потрібну ефективність реалізації деяких з функціональних властивостей захищених ресурсів. Однією з причин такого стану є недосконаліть відомих методів оцінки та забезпечення таких функціональних властивостей.

Мета роботи

Тому основною метою роботи якраз і є розроблення методики оцінки впливу способів організації обміну на характеристики захищеності інформації в ТКМ. Методика включає наступні етапи:

1. Оцінка можливих способів організації та реалізації ефективного захисту інформаційного обміну в телекомунікаційних мережах сучасних ієрархічних КМ з погляду забезпечення цілісності, швидкості обміну та часу доставляння повідомлень (як однієї з кількісних характеристик доступності) та вироблення рекомендацій щодо способів організації обміну, які б забезпечували удосконалення та підвищення рівня захищеності інформаційних об'єктів (інформаційних повідомлень) під час обміну;

2. Оцінка та розроблення можливих варіантів підвищення цілісності та доступності інформації в ТКМ;

3. Оцінка можливої шкоди через неефективну організацію обміну в ТКМ

Останнє пов'язане з тим, що як показано [3], власника КМ турбує не лише можливість забезпечення засобами ТЗІ тієї чи іншої властивості захищеності, а і ефективність цих засобів, тобто якою «ціною» забезпечується досягнення цієї функціональної властивості, то певна увага в роботі приділена оцінці відповідності витрат на захист інформації в ТКМ тому виграшу, який при цьому досягається, тобто оцінці оптимальності захищеності ТКМ з погляду можливих економічних втрат.

Етап оцінки можливих способів організації та реалізації ефективного захисту інформаційного обміну в телекомунікаційних мережах сучасних ієрархічних КМ з погляду забезпечення цілісності, швидкості обміну та часу доставляння повідомлень (як однієї з кількісних характеристик доступності) та вироблення рекомендацій щодо способів організації обміну, які б забезпечували удосконалення та підвищення рівня захищеності інформаційних об’єктів (інформаційних повідомлень) під час обміну передбачає:

1. Оцінку цілісності інформаційних об'єктів в ТКМ при реалізації того чи іншого способу організації обміну. Для оцінки цілісності запропоновано використання такої характеристики як правильність передачі даних (ймовірність правильної доставки повідомлення чи отримання на приймальному боці невикривленої інформації).

2. Оцінку доступності ТКМ, яка здійснюється через такі її характеристики як відносна та абсолютна швидкості обміну інформації в ТКМ та час затримки в доставлянні повідомлень при реалізації того чи іншого способу організації обміну.

3. Оцінку можливої шкоди через неефективну організацію обміну.

Основна частина

З метою отримання рекомендацій щодо практичного вибору ефективних методів та способів організації обміну оцінку характеристик цілісності та здійснено одночасно із порівняльною оцінкою найбільш поширених способів організації обміну в ТКМ. У випадку відсутності однозначності висновків щодо переваг того чи іншого способу організації

обміну запропоновано використання комплексної характеристики ефективності забезпечення в ТКМ цілісності та доступності у вигляді ефективної швидкості обміну.

При цьому слід очікувати, що в загальну інтенсивність потоку загроз для телекомунікаційних мереж (див. рис. 1), які складаються з сукупності вузлів комутації та каналів зв'язку і побудовані на загальних принципах, найбільший внесок дає потік природних впливів.

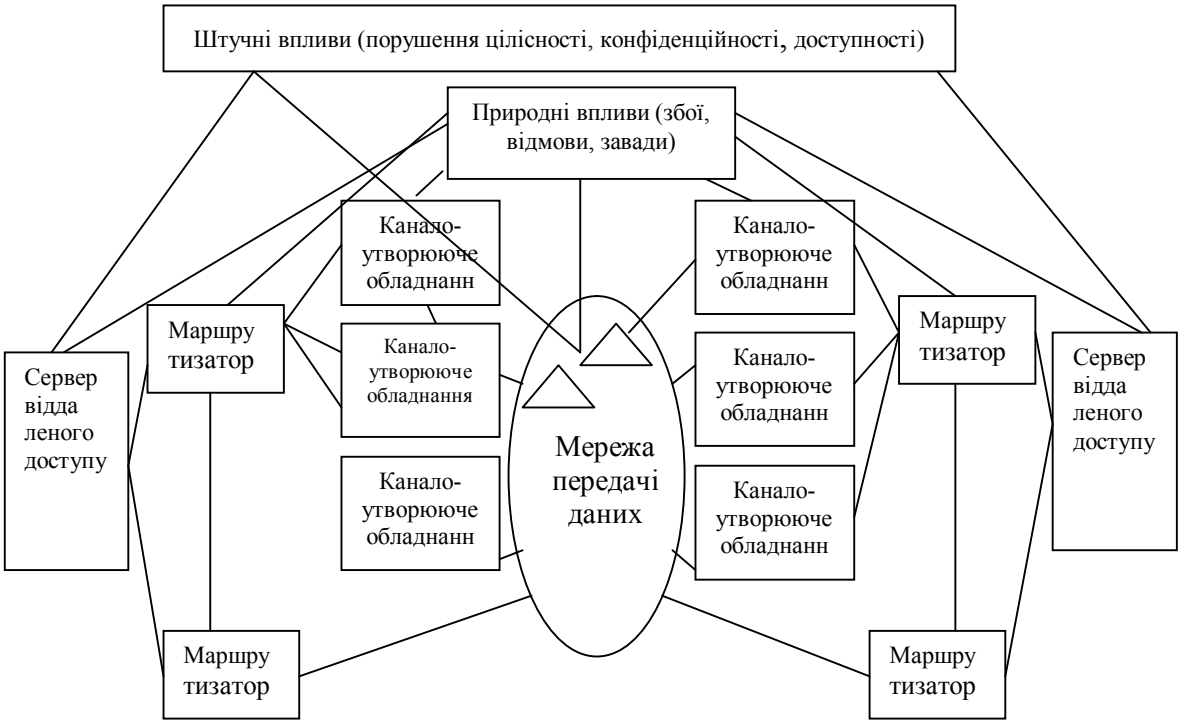

Рис.1. Модель впливів на елементи ТКМ

Тобто природні впливи на елементи ТКМ є найбільш імовірними. Це пов'язано, по-перше, із їх значною інтенсивністю в ТКМ (принаймні в її каналах передачі даних), а по-друге, із підкресленим уже фактом зниження інтенсивності штучних впливів за рахунок їх проріджения засобами управління доступом.

По відношенню до інформації ТКМ слід говорити про те, що первинним наслідком впливів усіх загроз є те чи інше її викривлення - порушення правильності чи цілісності інформації, яке, в свою чергу, може призвести до порушення інших функціональних властивостей інформаційного об'єкта, насамперед, його доступності. Топологія ТКМ при цьому, принаймні для проблеми, що розглядається, принципового значення не має і може бути такою, як це представлено на рис. 2.

Найчастіше під правильністю розуміють стійкість інформації щодо викривлень поодинокого символу чи групи символів в наслідок природних впливів, а під цілісністю - видалення чи модифікацію певної кількості символів чи усього повідомлення в наслідок штучних впливів. Звернемо увагу на те, що ці визначення не завжди відрізняються сутністю, а дуже часто - лише сферою (галуззю) застосування. Тому, з погляду проблематики забезпечення захищеності інформаційних ресурсів, їх доречно звести до поняття цілісності цих ресурсів, хоча при цьому, безумовно, слід враховувати джерело походження загроз цій цілісності. Це є особливо важливим при вирішенні питання щодо механізмів контролю цілісності, оскільки штучні, навмисні викривлення інформаційних об'єктів можуть приховуватися, маскуватися. Окрім того, в даній роботі запропоновано застосувати такі поняття цілісності, які є близькими до понять протоколів

розподілу функцій у відповідності з концепцією взаємного зв'язку відкритих систем та до розподілу способів забезпечення конфіденційності в ТКМ (чи то канальне, чи то абонентське шифрування) [4].

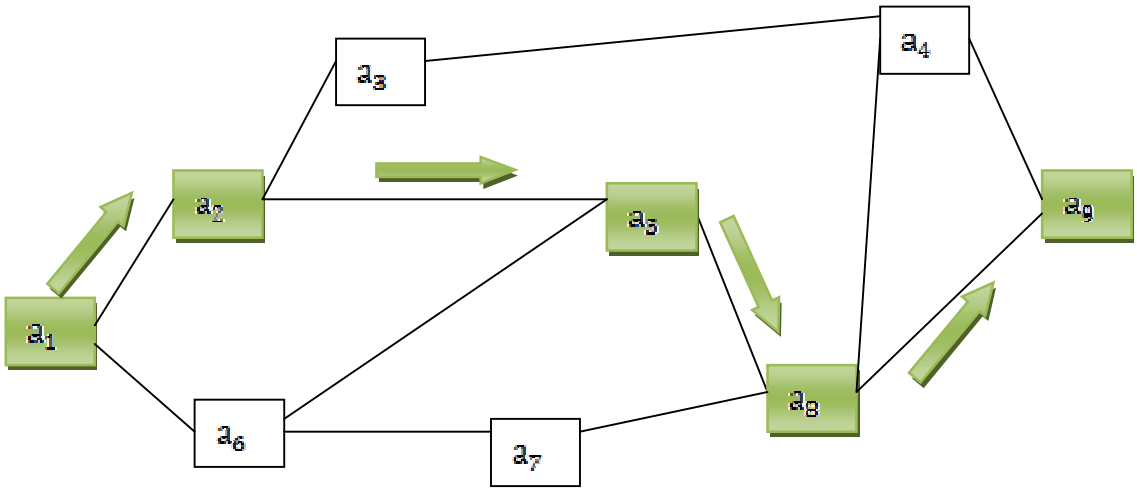

Рис.2. Приклад топології мережі передачі даних

При цьому можна розподілити (в розрізі напрямків даних досліджень) взагалі єдину задачу забезпечення властивостей захищеності ресурсів ТКМ на:

1. *Задачу забезпечення властивостей захищеності ресурсів в каналах*(канальні **цілісність** та **доступність) -** задачі забезпечення правильності та мінімального часу затримки інформації, яка передається в каналах зв'язку по певному маршруту телекомунікаційної мережі між вихідним та вихідним каналоутворюючим обладнанням відповідних елементів КМ у відповідності з протоколами 1 - 4 рівнів (фізичний, канальний, мережний та транспортний). Ця задача вирішується шляхом подолання наслідків природних чи інших впливів на елементи канального та мережного обладнання.

2. Задачу забезпечення властивостей захищеності ресурсів ТКМ вцілому **(абонентські цілісність та доступність**,) — задачу забезпечення цілісності та доступності інформації, яка передасться від одного елемента КМ (абонента — абонентської ЕОМ) до іншого у відповідності з протоколами 5-7 рівнів (сеансовий, .представницький та прикладний), шляхом подолання наслідків усіх штучних впливів та тих природних впливів на елементи ТКМ канального обладнання, які не усунені засобами забезпечення цілісності в елемента канального обладнання.

Модель взаємодії засобів в процесі ТЗІ в телекомунікаційних системах, на думку автора, з урахуванням викладених нижче міркувань, можна уявити так, як це представлено на рис.3, який є трансформацією рис.2. З цієї моделі витікає, що штучні впливи, які генеруються на абонентському рівні з боку передавача з інтенсивністю $\lambda_{шп}$ дають наслідки лише при умові подолання ними системи [4] управління доступом до інформаційних та фізичних ресурсів, тобто тільки в разі їх невиявлення засобами управління доступом. Тоді інтенсивність таких штучних загроз, які впливають на засоби забезпечення відповідної функціональної послуги ТКМ, зменшується (за рахунок проріджения, фільтрації штучних впливів засобами управління доступом) до $\lambda_{шп} P_{уд}$, де, як і в [2]. $P_{уд}$ - ймовірність подолання засобів управління доступом. Ці впливи та штучні ж впливи на канальному рівні, у багатьох випадках, не мають протидії з боку канальних засобів захисту, оскільки відповідають вимогам та умовам формування справжніх повідомлень і тому впливають на відповідні ресурси ТКМ з інтенсивністю ($\lambda_{шп} P_{уд} + \lambda_{шк}$). Цей вплив, скоріше за все, може звестися до зменшення доступності ресурсів ТКМ .

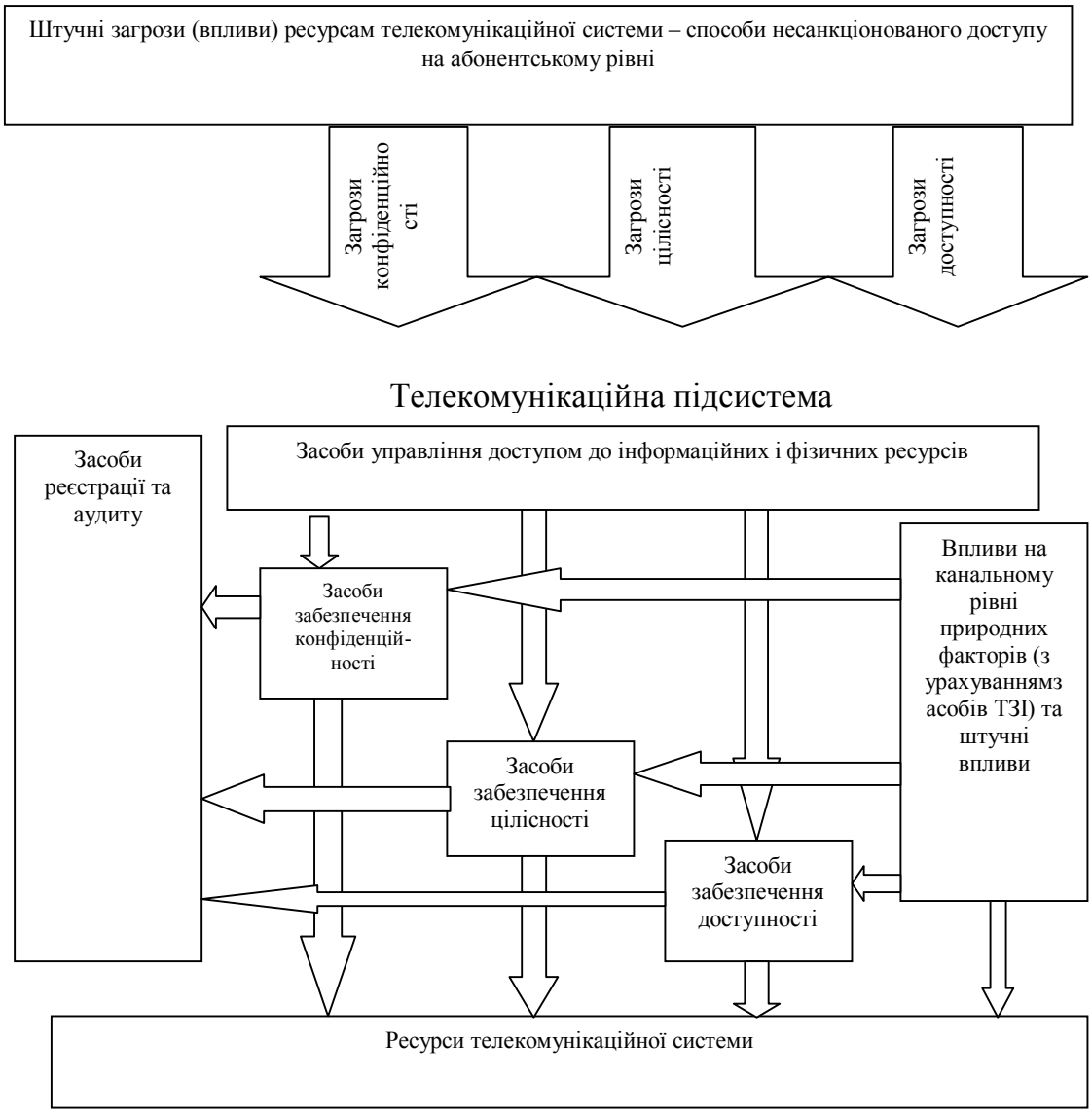

Рис.3. Модель взаємодії засобів в процесі технічного захисту інформації

Природні ж впливи не відповідають вимогам та умовам формування справжніх повідомлень і тому частка ресурсу ТКМ витрачається на їх виявлення та усунення (зменшення доступності ТКМ). На цілісність ресурсів ТКМ вони впливають тільки в разі неспроможності виявити та усунути їх засобами канального забезпечення цілісності. Тобто, інтенсивність природних загроз λ, які впливають на засоби забезпечення цілісності ресурсів ТКМ, також зменшується (за рахунок проріджування, фільтрації природних загроз канальними засобами) до $\lambda P_{кан}$, де, як і в [2], $P_{кан}$ - ймовірність подолання засобів канального захисту інформації телекомунікаційній мережі. Тоді результуюча інтенсивність загроз доступності ресурсів ТКМ $\lambda_{рд}$ може бути розрахованою як

$$\lambda_{рд} = \lambda_{шд} P_{уд} + \lambda_{шс} + \lambda \qquad (1)$$

а результуюча інтенсивність загроз цілісності ресурсів ТКМ $\lambda_{р2}$ може бути розрахованою як

$$\lambda_{рц} = \lambda_{шд} P_{уд} + \lambda_{шс} + \lambda P_{кан} \qquad (2)$$

Зрозуміло, що з цією ж інтенсивністю (вираз (2)) загрози впливають і на засоби захисту абонентського рівня. Тоді, з урахуванням застосування відповідних засобів захисту – засобів

забезпечення цілісності ресурсів ТКМ (на абонентському рівні в ТКМ вузлів центрального, регіонального чи місцевого рівнів АС), імовірність подолання яких - $P_{акц}$, результуюча інтенсивність $\lambda_н$ загроз, не усунутих системою ТЗІ, може бути розрахованою як

$$\lambda_н=\lambda_{рц}P_{акц} = (\lambda_{шд}P_{уд} + \lambda_{шк} + \lambda P_{ккц})P_{акц}. \quad (3)$$

Висновки

Найбільший вплив на ресурси ТКМ, як витікає з виразу (3), слід очікувати від штучних впливів на канальному рівні, оскільки вони не зменшуються (не проріджуються) ніякими засобами, окрім засобів забезпечення цілісності ресурсів ТКМ на абонентському рівні, та особливу необхідність при цьому зменшення ймовірності подолання засобів абонентського контролю цілісності інформації $P_{акц}$, або збільшення ймовірності виявлення та усунення впливу засобами абонентського контролю цілісності інформації (1-$P_{акц}$).

Список літератури

1. *Хорошко В.А.* — Методы и средства защиты информации // Хорошко В.А., Чекатков А.А. — К.: Юниор, 2003. — 504 с.

2. *Ленков С.В.* — Методы и средства защиты информации. В 2-х томах / Ленков С.В., Перегудов Д.А., Хорошко В.А. — К.: Арий, 2008.

3. *Поповский В.В.* — Защита информации в телекоммуникационных системах. В 2-х томах / Поповский В.В., Персиков А.В. — Харьков: ООО «Компания СМИТ», 2006.

4. *Дмитренко А.П.* — Модели безопасного соединения с удаленными объектами / Дмитренко А.П., Сирченко Г.А., Хорошко В.А. // Захист інформації, №1, 2010. — С.53-57.

Надійшла 27.01.2010

УДК 621.396 **Дмитренко О.П.**

СИНТЕЗ ЗАГАЛЬНОЇ ТОПОЛОГІЧНОЇ СТРУКТУРИ МЕРЕЖІ І ПЕРЕДАЧІ ІНФОРМАЦІЇ В МВС

Вступ

Розглянемо використання розроблених методів [1] до проектування загальної топологічної структури фрагмента базової мережі МВС.

Фрагмент базової мережі включає вузли зв'язку в східному і південному регіонах України, які розташовані в містах Київ, Дніпропетровськ, Харків, Донецьк, Запоріжжя, Сімферополь, Одеса, Севастополь.

Телекомунікаційна мережа призначена для забезпечення обміну даними між підрозділами МВС з рівнями «місцевий-регіональний-центральний» на принципах глобальної корпоративної мережі архітектури IP (Internet Protokol). Система також дозволяє побудувати мережу обміну даними других підрозділів, які мають у своєму складі ту ж саму архітектурну ідеологію.

Мета роботи

Метою створення корпоративної мережі (КМ) є впровадження нових інформаційних технологій для забезпечення необхідного рівня оперативності інформації.

Основна частина

Корпоративна мережа повинна забезпечувати:

- єдину телекомунікаційну мережу доступу локальних та віддалених користувачів;
- можливість нарощування локальних і віддалених сегментів мережі на основі високошвидкісних (до 2 Мб/ сек) і швидкісних (до 115 кб/ сек) каналів зв'язку, а також