законодавство з питань боротьби з організованою злочинністю та корупцією;
міжнародний досвід боротьби з організованою злочинністю;
газета Координаційного комітету по боротьбі з корупцією і організованою злочинністю при Президентові України “Крок”;
науково-практичний журнал "Боротьба з організованою злочинністю і корупцією (теорія і практика)";
огляд регіональної та центральної преси;
форум (обговорення актуальних питань законодавства).

Висновки

Вище розглянуто далеко не всі питання, пов’язані з безпечним функціонуванням інформаційних систем в Internet. Кожне з них, наприклад, розповсюдження вірусів чи використання не ліцензійного програмного забезпечення, потребує окремого дослідження. Вітчизняне інформаційне право знаходиться ще на стадії формування. В цілому це завдання вимагає системного підходу та координації діяльності не тільки державних структур та правоохоронних органів, а й усіх, зацікавлених в подальшому розвитку як Internet-культури взагалі, так і Internet-комерції зокрема.

Тому тільки скоординованими зусиллями організацій та відомств незалежно від форм власності, шляхом налагодження міжнародного співробітництва, використовуючи сучасні технології захисту інформації можна отримати переваги не тільки електронного бізнесу, а й інформаційної революції в цілому, не забуваючи при цьому про інформаційну безпеку як нашої держави, так і її окремих громадян.

Література: 1. Послання Президента України до Верховної Ради “Україна: поступ у XXI сторіччя. Стратегія економічного та соціального розвитку на 2000-2004 роки” // Урядовий кур’єр . – 2000. - № 16. – С. 7. 2. Указ Президента України Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні № 582 від 31 липня 2000 року. 3. Компьютерные преступления / Айков А., Сейгер К., Фонсторх У. - М., "Мир". - 1999. - С. 27. 4. Виявлення та розслідування злочинів, що вчиняються за допомогою комп’ютерних технологій Б. В. Романюк, М. І. Камлик, В. Д. Гавловський, В. Г. Хахановський, В. С. Цимбалюк за заг. ред. Я. Ю. Кондратьєва. -К., - 2000. 5. Криміналістика П. Д. Біленчук, В. В. Головач, М. В. Салтевський. К. – 1997. 6. Jane's Defence Weekly.— 1997 .— 16 July.— P. 10.

УДК 681.322:621.395

АСПЕКТИ ПОЛІТИКИ БЕЗПЕКИ СИСТЕМИ УПРАВЛІННЯ ТЕЛЕКОМУНІКАЦІЙНИМИ МЕРЕЖАМИ

Микола Тардаскін, Володимир Кононович
Одеський регіональний центр технічного захисту інформації ВАТ “УКРТЕЛЕКОМ”

Анотація: **Розглядається демонстраційний приклад політики безпеки інформації у системах управління телекомунікаційними мережами (СУТ). Охоплені питання, що мають бути застосовані при реалізації політики безпеки об’єктів СУТ.**

Summary: **Demonstrative examples of security policy in the Telecommunication Management Network (TMN) are considered. The aspects, which must application in security policy realization of the object of TMN examine.**

Ключові слова: **Політика безпеки, система технологічного управління, інформація, адміністратори, програмне забезпечення.**

Інформація, що використовується у системах управління телекомунікаційними мережами (СУТ), є критично важливою для галузі телекомунікацій [1]. Розміри та складність побудови СУТ великі і вона забезпечує обмін інформації між значною кількістю операторів [2]. Це призводить до збільшення ризиків і вимагає застосування більш сильних механізмів захисту, порівняно з тими, що потрібні при роботі з окремими персональними комп’ютерами (ПК). Посилені вимоги до захисту в обчислювальному середовищі СУТ зумовлюють необхідність даної політики.

І Мета і загальні положення політики безпеки

Метою роботи є розвиток нормативно-правової бази для реалізації комплексної системи захисту інформації СУТ [3, 4]. Політика безпеки є ключовим компонентом плану захисту СУТ. У той же час,

ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.

політика безпеки СУТ (далі – просто політика) є частиною загальної політики безпеки галузі і успадковує її принципи.

Політика визначає важливість (цінність) інформації, встановлює для усіх працівників важливість безпеки в середовищі СУТ, розподіляє їх ролі, встановлює обов'язки та відповідальність щодо забезпечення безпеки як даних і інформації, так і самої СУТ. Політика охоплює всі інформаційні цінності, ресурси і служби, що використовуються СУТ. Вона застосовується до серверів СУТ, периферійного устаткування, автоматизованих робочих місць і ПК у межах середовища СУТ. Ресурси СУТ включають дані, інформацію, програмне забезпечення, апаратні засоби, засоби обслуговування і телекомунікації. Політика застосовна до всіх осіб, що мають відношення до СУТ. Політика розробляється на рівні адміністрації служби, яких стосується ця політика, і формується групою осіб, включаючи керівників, співробітників служби безпеки та адміністраторів СУТ.

Політика повинна встановлювати: відповідальність за захист інформації в СУТ та обов'язки підрозділів.

Мета плану захисту інформації СУТ полягає в тому, щоб гарантувати цілісність, доступність та конфіденційність даних, що мають бути достатньо повними, точними, і своєчасними, щоб задовольняти потреби СУТ. Необхідно гарантувати:

- забезпечення відповідного рівня безпеки в середовищі СУТ згідно з критичністю інформації;
- рентабельність безпеки і базування її на співвідношенні вартості і ризику відповідно до керівних вимог;
- забезпечення відповідної підтримки захисту даних у кожній області функціонального управління;
- індивідуальну підзвітність щодо даних, інформації та інших комп'ютерних ресурсів, до яких є доступ;
- можливість перевірки середовища функціонування СУТ;
- забезпечення користувачів достатньо повними інструкціями з розподілу обов'язків щодо підтримки безпеки при роботі в СУТ;
- відповідність планів забезпечення безупинної роботи критично важливих функцій СУТ, планів відновлення роботи при стихійних лихах;
- виконання усіх відповідних законів, указів тощо.

II Відповідальність за впровадження політики

Політика безпеки СУТ визначає і встановлює відповідальність за захист інформації, що обробляється, зберігається і передається в СУТ, та належить самій СУТ. Основна відповідальність покладена на керівника підрозділу підприємства, що створює дані, обробляє їх і т. п. Додаткова відповідальність покладена на операторів, яким надано доступ до інформації. Адміністратори СУТ визначають роль окремих працівників, відповідальних за підтримку працездатності СУТ.

За впровадження і досягнення цілей політики безпеки відповідають такі групи співробітників:

1. Функціональне керівництво відповідає за інформування співробітників щодо політики, взаємодіє з усіма службовцями в питаннях з проблем безпеки.
2. Адміністратори СУТ здійснюють щоденне керування і підтримку працездатності СУТ, відповідають за забезпечення безупинного функціонування СУТ та за здійсненням заходів захисту в СУТ відповідно до варіантів політики безпеки СУТ.
3. Місцеві адміністратори відповідають за надання кінцевим користувачам доступу до необхідних ресурсів СУТ, що розміщені на серверах і автоматизованих робочих місцях, та входять у їхню зону відповідальності, і відповідають за забезпечення захисту своїх серверів.
4. Користувачі-оператори – це працівники, що мають доступ до СУТ. Всі користувачі-оператори даних відповідають за дотримання специфічних варіантів політики і відповідальні перед керівництвом при будь-якій підозрі щодо порушення захисту.

Порушення політики може піддати інформацію неприпустимому ризику втрати конфіденційності, цілісності або доступності при її зберіганні, обробці або передачі в межах СУТ. Порушники стандартів, процедур або інструкцій, що спрямовані на підтримку політики, мають бути притягнуті до дисциплінарної відповідальності.

III Розмежування доступу до СУТ

Передбачається система правил розмежування доступу.

1). Кожний ПК (автоматизоване робоче місце – АРМ) повинен мати свого відповідального за працездатність, безпеку комп'ютера та за дотриманням політик і процедур при використанні АРМ. Цю роль може виконувати основний користувач комп'ютера. Користувачі повинні бути навчені і забезпечені відповідними інструкціями, щоб вони могли коректно додержуватися усіх політик і процедур.

2). Щоб запобігти не авторизованому доступу до даних СУТ, програмному забезпеченню, іншим

ресурсам, що знаходяться на серверах СУТ, усі механізми захисту серверів СУТ повинні знаходитися під монопольним керуванням місцевого адміністратора і місцевого персоналу адміністраторів СУТ.

3). Щоб запобігти поширенню нелегального програмного забезпечення і сприяти виконанню ліцензійних угод про програми, користувачі повинні гарантувати, що їхнє програмне забезпечення має належні ліцензії і є безпечним.

4). За всі зміни (заміни) програмного забезпечення і створення резервних копій даних на серверах відповідають адміністратори СУТ.

5). Кожному користувачу після закінчення оформлення належної документації призначається унікальний ідентифікатор користувача і початковий пароль. Користувачі не повинні спільно використовувати призначені кожному з них ідентифікатори користувача.

6). Користувачі проходять процедуру автентифікації в СУТ перед зверненням до ресурсів СУТ.

7). Ідентифікатор користувача має періодично змінюватись.

8). Використання апаратних засобів СУТ типу моніторів чи реєстраторів (аналізаторів) трафіку і маршрутизаторів має бути авторизованим і проводитись під контролем адміністраторів СУТ.

9). Працівники, відповідальні за керування процесом роботи, функціонування і використання СУТ, повинні пройти курс навчання в області комп'ютерної безпеки і правил роботи у комп'ютерних мережах.

10). Звіти про безпеку повинні готуватися і розглядатися щодня.

IV Особливості забезпечення безпеки СУТ користувачами

Користувачами СУТ є працівники високої кваліфікації. Передбачається, що користувачі добре поінформовані щодо політики безпеки та інших застосовних законів, указів, варіантів політики безпеки, процедур і твердо їх дотримуються. Користувачі цілком відповідають за власну поведінку. Зокрема, користувачі відповідають за:

1. Дотримання відповідних законів, варіантів політики безпеки, процедур і пов'язаних з ними наслідків для СУТ.

2. Використання доступних механізмів безпеки для захисту конфіденційності і цілісності власної інформації, коли це потрібно. Повинні виконуватись місцеві процедури захисту критичних даних, процедури безпеки самої СУТ, використання механізмів захисту файлів для підтримки достатнього рівня керування доступом до файлів.

3. Вибір і використання відповідних паролів. Користувачі не повинні записувати паролі, розкривати їх іншим або спільно використовувати ідентифікатори користувачів.

4. Допомогу іншим користувачам, котрі не можуть належним чином використовувати доступні механізми захисту, сповіщення їх щодо незахищеності їхніх ресурсів.

5. Сповіщення місцевого адміністратора або керівника щодо порушень захисту або виявлених відмов.

6. Невикористання слабких місць СУТ. Не повинні проводитись навмисні зміни, знищення, читання, або передача інформації не авторизованим засобом. Не повинні створюватись спеціальні завади в одержанні іншими користувачами авторизованого доступу до ресурсів СУТ або до інформації.

7. Надання правильної інформації для ідентифікації й аутентифікації, коли це потрібно, і недопущення спроб вгадування подібної інформації для потреб інших користувачів.

8. Гарантування виконання резервного копіювання даних і програмного забезпечення, що знаходиться на жорсткому диску їх власного АРМ.

9. Розуміння принципів роботи зловмисного програмного забезпечення, методів, за допомогою яких воно вноситься і поширюється, і вразливих місць, що звичайно використовуються зловмисним програмним забезпеченням і не авторизованими користувачами.

10. Знання і використання відповідних політик і процедур для запобігання, виявлення і видалення зловмисного програмного забезпечення.

11. Знання про те, на що потрібно звертати увагу при роботі у визначених системах і конкретних програмах, щоб виявити ознаки їхньої незвичайної роботи, і що потрібно зробити, або з ким зв'язатися для одержання додаткової інформації.

12. Використання програмно-апаратних засобів захисту, що доступні для захисту системи від зловмисного програмного забезпечення.

13. Використання процедур з забезпечення безупинної роботи для стримування і відновлення при потенційних інцидентах.

V Особливості забезпечення безпеки СУТ функціональними керівниками

Функціональні керівники відповідають за розробку і виконання ефективних варіантів політики безпеки,

ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.

що відображають специфічні цілі СУТ. Задача захисту інформації і ліній зв'язку є важливою і критичною метою у повсякденній діяльності. Зокрема функціональні керівники відповідають за:

1. Проведення ефективного керування ризиком, щоб забезпечити основу для формулювання розумної політики безпеки. Керування ризиком потребує ідентифікації цінностей, котрі мають бути захищені, визначення уразливих місць, аналізу ризику їх використання та реалізації рентабельних засобів захисту.
2. Гарантування того, щоб кожний користувач одержав копію документу, що стосується варіантів політики безпеки та інструкції, до внесення його в списки користувачів СУТ.
3. Реалізацію програми навчання користувачів основам безпеки, щоб можна було гарантувати знання ними місцевих варіантів політики безпеки і правил роботи на комп'ютері.
4. Гарантування того, що весь персонал у межах операційної одиниці організації знає цю політику і відповідає за включення її в інструктажі з комп'ютерної безпеки і програми навчання.
5. Інформування місцевого адміністратора й адміністраторів СУТ про зміни в статусі будь-якого службовця, що використовує ресурси СУТ (перехід в іншу організацію, перехід із відділу у відділ або звільнення).
6. Гарантування того, що користувачі розуміють природу потенційного зловмисного програмного забезпечення, розуміють, як воно розповсюджується та які програмно-апаратні засоби захисту мають бути використані проти нього.

VI Особливості забезпечення безпеки адміністраторами СУТ

Передбачається, що адміністратори СУТ (або підготований для цього персонал) реалізують місцеві варіанти політики безпеки. Цей процес пов'язаний із застосуванням програмно-апаратних засобів захисту, архівацією критичних програм і даних, керуванням доступом і захистом устаткування СУТ. Зокрема, адміністратори СУТ несуть відповідальність за:

1. Коректне застосування доступних механізмів захисту для здійснення місцевих варіантів політики безпеки.
2. Повідомлення керівництва про працездатність існуючих варіантів політики безпеки і будь-які технічні рішення, що могли б сприяти поліпшенню їхньої ефективності.
3. Захищеність середовища СУТ та інтерфейсів із глобальними мережами.
4. Оперативне й ефективне улагоджування подій із комп'ютерною безпекою. Місцеві адміністратори мають повідомлятись щодо проникнень зловмисника в СУТ, допомагати іншим місцевим адміністраторам улагоджувати події з безпекою. Має бути налагоджене співробітництво з усіма адміністраторами при виявленні порушника.
5. Використання надійних і доступних засобів аудиту для полегшення виявлення порушень безпеки.
6. Проведення своєчасних перевірок системних журналів серверів СУТ.
7. Відстеження інформації щодо варіантів політики безпеки і заходів, спрямованих на забезпечення безпеки, інформування місцевих користувачів і повідомлення керівництва щодо змін або нових розробок у цьому питанні.
8. Надзвичайну обережність і коректність при застосуванні своїх повноважень і привілеїв. Безпека користувачів завжди повинна мати пріоритет.
9. Розробку відповідних процедур і видання інструкцій щодо запобігання, виявлення, і видалення зловмисного програмного забезпечення.
10. Своєчасне створення резервних копій усіх даних і програмного забезпечення на серверах СУТ.
11. Виявлення і рекомендацію пакетів програм для виявлення і видалення зловмисного програмного забезпечення.
12. Розробку процедур, що дозволяють користувачам повідомляти про комп'ютерні віруси й інші інциденти, і повідомлення осіб про потенційно можливу погрозу, що стосується їх.
13. Швидке повідомлення відповідної групи, що займається улагоджуванням подій щодо комп'ютерної безпеки, про всі інциденти, включаючи виявлення зловмисного програмного забезпечення.
14. Надання допомоги при визначенні джерела зловмисного програмного забезпечення і зони його поширення.
15. Забезпечення допомоги з видалення зловмисного програмного забезпечення.
16. Проведення періодичного аналізу для гарантування дотримання належних процедур безпеки, включаючи ті, що призначені для захисту від зловмисного програмного забезпечення.

VII Особливості забезпечення безпеки місцевими адміністраторами

Місцеві адміністратори використовують доступні служби і механізми захисту СУТ на сервері, що

знаходиться в їхній зоні відповідальності, щоб підтримувати і впроваджувати варіанти і процедури політики безпеки. Зокрема, місцеві адміністратори відповідають за:

1. Керування привілеями доступу всіх користувачів до даних, програм і функцій.

2. Контроль всіх пов'язаних з захистом подій і за розслідуванням будь-яких реальних або підозрюваних порушень там, де це доречно. Вони відповідають за повідомлення і координацію дій з адміністраторами СУТ з контролю або розслідування подій, пов'язаних із порушенням безпеки.

3. Підтримку і захист програмного забезпечення і відповідних файлів на сервері СУТ, використовуючи доступні механізми і процедури захисту.

4. Сканування серверу СУТ антивірусним програмним забезпеченням через регулярні інтервали часу для гарантування того, що ніякий вірус не розмістився на сервері СУТ.

5. Призначення унікального ідентифікатора користувача і початкового паролю (або іншої ідентифікаційної і аутентифікаційної інформації) кожному користувачу тільки після того, як буде оформлена належна документація.

6. За швидке повідомлення персоналу групи улагоджування подій із комп'ютерною безпекою про всі інциденти, включаючи зловмисне програмне забезпечення. У тому числі повідомляє адміністраторів про проникнення в СУТ, допомагає іншим місцевим адміністраторам улагоджувати порушення безпеки, співробітничає з іншими місцевими адміністраторами й адміністраторами СУТ у пошуку порушника.

7. Забезпечення допомоги при виявленні джерела зловмисного програмного забезпечення і зони його поширення.

ПК дуже уразливі до атак вірусів, нелегальних користувачів і пов'язаних з цим погроз. Програмне забезпечення виявлення вірусів має знаходитися на АРМ, серверах, тощо. Адміністратори СУТ особисто визначають конкретні програмні продукти та забезпечують їх оновлення. Запобігання вірусам у середовищі ПК має бути під постійною увагою користувача, щоб можна було виявляти потенційні загрози, боротися з ними і відновлювати середовище після ушкоджень. Користувач повинен завжди стежити за роботою АРМ, щоб знати, що є нормальною, а що ненормальною роботою. Користувачі повинні розпізнавати проблеми з безпекою і відновлювати середовище до нормального стану. Має велике значення навчання користувачів і створення переліку ефективних дій з адміністрування АРМ, специфічних для обчислювального середовища СУТ.

VIII Відновлення і забезпечення безупинної роботи СУТ

Інцидент із комп'ютерною безпекою – це будь-який несприятливий випадок, у ході якого може опинитися під загрозою деякий аспект безпеки: втрата конфіденційності даних, цілісності даних або цілісності системи, руйнація або відмова в обслуговуванні. В середовищі СУТ поняття інциденту з безпеки може бути поширене на усю область СУТ (апаратні засоби ЕОМ, програмне забезпечення, дані, передачу даних, і т. д.) включаючи саму СУТ. Плани відновлення в середовищі СУТ мають бути розроблені таким чином, щоб будь-який інцидент із захистом СУТ міг бути своєчасно улагоджений, із найменшим, наскільки це можливо, впливом на функціональні можливості управління телекомунікаційними мережами. План відновлення має описувати дії з улагоджування інциденту, дії з резервування і дії з відновлення.

Мета дій з улагоджуванню інциденту полягає в тому, щоб зменшити потенційно небезпечні наслідки проблеми, пов'язаної з безпекою СУТ. Це потребує не тільки улагодження інцидентів, але і ресурсів для попередження користувачів, співробітництва з усіма користувачами для гарантування того, що про інциденти буде вчасно повідомлено і вони будуть улагоджені, а майбутні інциденти – відвернені.

Плани дій з резервування підготовляються, щоб гарантувати, що функціональні процеси можуть бути коректно завершені при руйнації СУТ і продовжені згодом, коли СУТ буде відновлена.

Плани відновлення створюються, щоб забезпечити плавне, швидке відновлення середовища СУТ після перерви в її роботі. Мають бути розроблені та підтримуватися ряд інструкцій для зменшення тривалості відновлення. Пріоритет має бути надано тим додаткам, службам, що вважаються критичними для функціонування СУТ. Процедури дій з резервування мають гарантувати, що ці критичні служби і додатки доступні користувачам.

Для підтримання безпеки в середовищі СУТ, користувачі СУТ повинні пройти навчання у визначених сферах роботи і використання СУТ. Механізми захисту, процедури, і т. д. не можуть бути діючими, якщо вони використовуються неправильно. Метою навчання функціонального керівництва є розуміння важливості політики безпеки і розуміння того, як ця політика повинна ефективно здійснюватися в СУТ. Метою навчання адміністраторів СУТ є розуміння, як забезпечується захист СУТ при її повсякденній роботі, та як ефективно улагоджуються інциденти. Метою навчання користувачів є усвідомлення ролі користувача в політиці безпеки й обов'язків, покладених на нього в цій області, навчання використанню служб і механізмів захисту для ефективної підтримки безпеки, і розуміння того, як використовувати процедури дій з улагоджування

інциденту. Повинні реалізуватись такі вимоги до курсів навчання.

Функціональні керівники повинні:

1. Розуміти важливість політики безпеки СУТ і те, як ця політика впливає на рішення, прийняті щодо захисту СУТ. Розуміти важливість визначення адекватного ступеня безпеки для різноманітних типів інформації, якою володіє функціональне керівництво.

2. Розуміти, що СУТ має цінні ресурси. Розуміти важливість забезпечення адекватного захисту (через фінансування, укомплектовування персоналом тощо).

Адміністратори СУТ повинні:

1. Розуміти усі аспекти роботи СУТ. Мати здатність відрізняти нормальну роботу системи від ненормальної.

2. Розуміти роль адміністратора СУТ в реалізації політики безпеки СУТ.

3. Розуміти, як працюють служба і механізми безпеки. Бути спроможними розпізнати неправильне використання механізмів захисту користувачами.

4. Розуміти, як треба ефективно використовувати можливості з улагоджування інцидентів.

Користувачі СУТ повинні:

1. Розуміти політику безпеки й обов'язки користувача. Розуміти, чому важлива підтримка безпеки СУТ.

2. Розуміти, як використовувати служби і механізми захисту, забезпечувані СУТ, щоб підтримувати безпеку СУТ і захищати критичну інформацію.

3. Розуміти, як використовувати можливості з улагоджування інцидентів, знати, як повідомляти про інцидент тощо.

4. Відрізняти нормальну роботу автоматизованого робочого місця або ПК від неправильної роботи.

Розглянуті аспекти політики безпеки корисно враховувати при її розробці для всіх об’єктів на кожному рівні СУТ.

Література: 1. Кононович В. Г. Класифікація інформації у мережах загального користування відносно технічного захисту інформації // Зв’язок. – 2000. - № 4. 2. В. Б. Булгак, Э. В. Евреинов, И .А. Мамзелев Теория и проектирование управляющих систем электросвязи. – М.: Радио и связь, 1995. – 384 с. 3. Кононович В. Г., Голобородько Д. В. Методи та засоби захисту від несанкціонованого доступу в системі управління мережами електрозв’язку України // - К.: Зв’язок, № 2, 1999, с. 13 - 16. 4. ETSI publications ETR 340. Telecommunications security. Guidelines for security management techniques.

УДК 621.396.2

ИНФОРМАЦИОННАЯ И ТЕХНИЧЕСКАЯ БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТРАНКИНГОВЫХ СИСТЕМ

Виктор Иванов

Украинский научно-исследовательский институт радио и телевидения (УНИИРТ)

Анотація: **Дано порівняльний аналіз можливостей гарантування інформаційної та технічної безпеки в цифрових транкінгових системах стандартів TETRA та TETRAPOL.**

Abstract: **The article deals with comparative analysis of informational and technical security guaranteeing possibility in digital trunking systems of TETRA and TETRAPOL systems.**

Ключевые слова: **Транкинговые системы, TETRA, TETRAPOL, угрозы системам подвижной связи, угрозы системным связям, угрозы связям пользователя, угрозы сообщениям связи.**

Введение

Необходимость в техническом перевооружении корпоративно-ведомственных систем связи и внедрении новейших радио технологий подтверждается реалиями функционирования систем связи государственных структур Украины. Наиболее полно специфическим требованиям к услугам подвижной связи в интересах государственных структур, министерств и ведомств отвечают современные цифровые транкинговые системы, имеющие возможности организации оперативных групповых и экстренных вызовов, гибкого перераспределения канальной емкости в соответствии с информационной нагрузкой, организации прямой радиосвязи в отдаленных и труднодоступных районах и т.д.

Учитывая необходимость обеспечения всех условий межведомственного взаимодействия в рамках единых корпоративно-ведомственных сетей подвижной связи целесообразным видится разворачивание не наложенных сетей отдельных министерств, ведомств и организаций, а Единой Национальной Сети