УДК 621.391.2 **Л.О.Комарова**

ПРИНЦИПИ ОРГАНІЗАЦІЇ МЕТОДІВ ЗАХИСТУ ТРАНСПОРТНОГО ТРАФІКА ЄДИНОЇ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ З ТЕРИТОРІАЛЬНО РОЗПОДІЛЕНИМИ РЕСУРСАМИ У КРИЗОВИХ СИТУАЦІЯХ

Запропоновані принципи побудови захищеної ІКМ з територіально розподіленими телекомунікаційними й інформаційними ресурсами у кризових ситуаціях. Показано, що це дозволяє уникнути зайвих витрат на забезпечення захисту між довіреними користувачами однієї контрольованої зони і в той же час забезпечити конфіденційність, цілісність і доступність інформації, знизити ступінь уразливості ІКМ, що використовуються для цілей державного управління, безпеки і оборони України, забезпечити захищеність державних інформаційних ресурсів та інформації.

Ключові слова: інформаційно-телекомунікаційні мережі, засоби захисту, кризова ситуація.

Вступ

Сучасний етап розвитку суспільства характеризується зростаючою роллю інформаційної сфери, що відображає сукупність електронних комунікацій, інформаційно-комунікаційних технологій (ІКТ), мультисервісних систем і мереж зв’язку та передачі даних є індикатором успішної економіки, високих стандартів соціального і гуманітарного розвитку країн, ефективних і прозорих урядів та демократичних суспільств. ІКТ забезпечують зручність та ефективність роботи енергетичної, транспортної, логістичної інфраструктури та служб забезпечення життєдіяльності країни, підвищують спроможності оперативного реагування на надзвичайні події природного й техногенного характеру. У зв'язку з цим значною мірою зростають загрози безпеки інформаційних ресурсів і телекомунікаційних засобів і систем, як вже розгорнутих, так і тих що створюються на території України. Реалізація завдань забезпечення безпеки є складною і тому вимагає значних ресурсів, у тому числі і фінансових. Для оптимізації часових, людських і фінансових витрат стає необхідним розробити принципи побудови захищеної інформаційно-телекомунікаційної мережі (ІКМ) у кризових ситуаціях (КС). Під кризовою ситуацією розумітимемо сукупність динамічно змінюваних оцінок (результатів аналізу, узагальнення) множини фактів і зв’язків між ними, що складаються з причин і наслідків, залежних від подій, що відбуваються, і процесів, які приводять до складних чи фатальних наслідків.

Постановка задачі

Створювана ІКМ для виконання функцій, зі статусом спеціального призначення у КС, повинна будуватися з використанням сучасних ІКТ – цифрових систем передачі і комутації, відповідати пропонованим з боку замовника та відповідних служб вимогам безпеки передачі інформації та повинна забезпечувати:

- надання інформаційно-комунікаційних послуг користувачам незалежно від їх місцезнаходження;
- необхідну захищеність інформації;
- необхідну ефективність функціонування (стійкість і достовірність) системи при дії загроз у КС.

У роботі запропоновані принципи організації методів захисту, які дозволяють захистити транспортний трафік єдиним для всіх видів інформації (дані, мова, відео) і будь-якої кількості віддалених приймаючих і транспортуючих сторін.

Основна частина та результати

Передана інформація може бути як загальнодоступною інформацією, так і інформацією, доступ до якої обмежено (конфіденційна, державна таємниця). При побудові ІКМ у КС покладемо, що з метою економії значних фінансових коштів в якості первинної мережі будуть використовуватися орендовані у провайдера канали зв'язку або інформаційно-телекомунікаційні ресурси вже існуючих мереж зв'язку. Використання орендованих каналів зв'язку автоматично означає наявність у системи точок сполучення з мережами загального

доступу, у зв'язку з чим з'являються нові загрози і посилюються вимоги до системи забезпечення інформаційної безпеки.

У відповідності з визначеними до ІКМ у КС вимогами, щодо якості наданих послуг, захищеності та ефективності функціонування що реалізуються у напрямках атак запропоновано наступні принципи побудови захищеної ІКМ. Загальний вигляд захищеної ІКМ у КС та напрямки атак зображені на рис. 1.

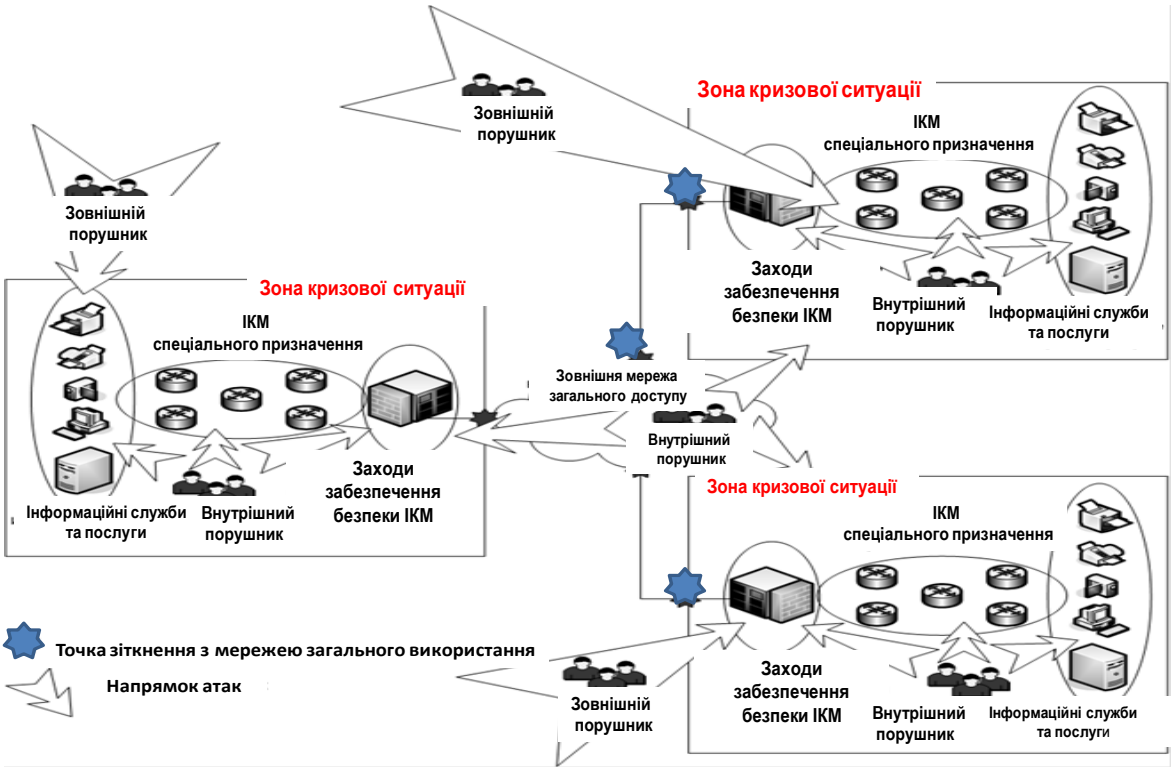

Рис.1. Захищена ІКМ у КС і вплив на неї за напрямками атак

ІКМ для виконання оперативних завдань у КС становлять інтерес для різного роду порушників, які можуть мати самі різні цілі: перевірити свої сили (без корисливих цілей і злих умислів), порушити роботу телекомунікаційної та/або інформаційної складових. Усіх порушників ІКМ можна розділити на дві категорії: внутрішні і зовнішні. Внутрішніми порушниками вважаються особи, які перебувають у контрольованій зоні, включаючи легітимних користувачів мережі, обслуговуючий персонал, який має доступ до інформаційно-телекомунікаційного обладнання та ресурсів тощо.

У зв'язку з тим, що ІКМ є мережею для виконання оперативних завдань у КС, всі працівники та обслуговуючий персонал, що має доступ до обладнання та інформації, вважається допущеним. Доступ сторонніх осіб (ремонтні бригади, перевірочні комісії і тощо) в контрольовану зону здійснюється тільки в супроводі довірених співробітників. Порушення користувачів даної категорії носять ненавмисний характер: спроба з'єднання з абонентом іншої робочої групи, вихід за межі тимчасового регламенту роботи спроба доступу до нерозв'язаним службам і послуг мережі.

Від внутрішніх порушників, які стають такими ненавмисно, використовуються засоби захисту, вбудовані в телекомунікаційне обладнання мережі. До таких засобів захисту належать:

- ідентифікація та аутентифікація;
- фільтрація за адресами;
- фільтрація по часу;
- фільтрація по використовуваних протоколах і портів.

Усі факти несанкціонованих дій повинні бути зафіксовані і передані відповідним підрозділам для з'ясування всіх подробиць інциденту.

Захист від внутрішніх загроз як:

- розголошення інформації, що захищається;
- обробка інформації на незахищених технічних засобах;
- несанкціонований доступ, у т. ч. зміна та копіювання;
- помилки персоналу при експлуатації технічних засобів і систем захисту;
- передбачає ненавмисне нанесення збитку організації і тому повинна більшою мірою здійснюватися організаційними, а не технічними заходами.

Зовнішніми порушниками вважаються особи, які знаходяться за межами контрольованої зони і не є користувачами або обслуговуючим персоналом ІКМ у КС. До даної категорії порушників відносяться хакери, конкуренти, розвідпідрозділи іноземних спецслужб та ін. Ця категорія порушників є найбільш небезпечною. У них можуть бути відомості про топологію мережі, що використовується телекомунікаційному обладнанні, засобах забезпечення безпеки, адресному просторі, наявних інформаційних ресурсах і т.п. Усі ці відомості спрощують завдання порушення конфіденційності, цілісності та доступності інформації, а також нормального функціонування телекомунікаційної складової.

Зовнішні порушники можуть використовувати різні методи досягнення своїх цілей:

- підслуховування і візуальне спостереження;
- побічні електромагнітні випромінювання та наведення;
- атаки з орендованих каналів зв'язку;
- перехоплення і зміна циркулює в мережі трафіку та інш.

Від різного роду спостережень, випромінювань і наведень захист здійснюється за допомогою відповідних заходів протидії: фізична охорона, атестація приміщень, перевірка обладнання на наявність програмно-апаратних закладок і тощо. Від усіх зовнішніх порушників, які намагаються встановити з'єднання з легітимним користувачем або отримати доступ до інформаційних ресурсів мережі у КС, захист проводиться розташованим на кордоні з мережею загального доступу пристроєм захисту. Воно виконує функції міжмережевого екрану, криптозахисту і тунелювання. Всі частини розподіленої ІКМ між собою об'єднані криптотунелями.

Даний комплекс заходів захисту запобігає можливість:

- аналізу внутрішньої адресної структури мережі;
- порушення конфіденційності переданої інформації;
- порушення цілісності інформації, що передається;
- аналізу частоти взаємодії різних користувачів і використання ними служб і послуг ІКМ;
- проникнення «вірусів» із зовнішньої мережі загального доступу і та ін..

Від повторного введення з відкритих каналів зв'язку вже переданих повідомлень використовується механізм імітуючої вставки. Імітовставка формується на передавальній стороні згаданим пристроєм захисту. На приймальній стороні вона перевіряється і у разі повторної доставки цього повідомлення воно просто видаляється, а факт самої події заноситься в журнал.

Загальна схема проходження інформації, що містить конфіденційні дані, через канали зв'язку загального доступу показана на рис. 2. У зв'язку тим, що дорогі пристрої захисту розташовуються тільки на кордоні з зовнішньою мережею, вдається уникнути надмірного захисту межах контрольованої зони та заощадити значні фінансові кошти. Криптографічно захищається тільки та інформація, яка виходить за межі контрольованої зони.

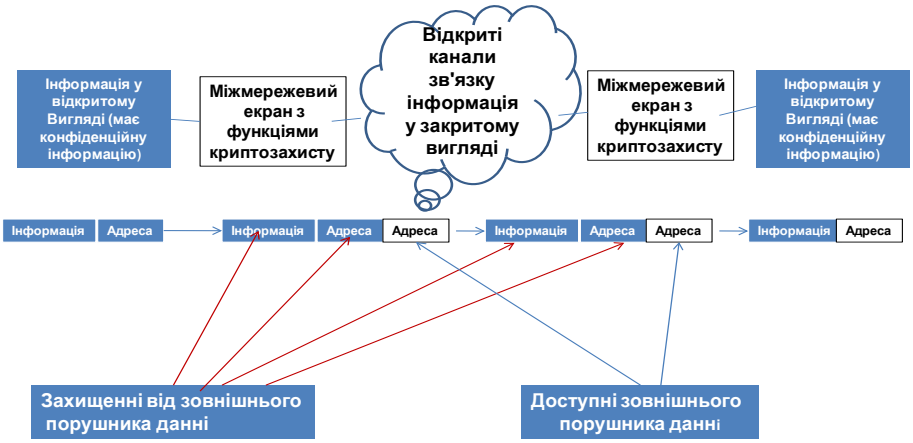

Рис. 2. Загальна схема проходження інформації, що містить конфіденційні дані, через канали зв'язку загального доступу

Висновок

Запропоновані вище принципи дозволяють уникнути зайвих витрат на забезпечення захисту між довіреними користувачами однієї контрольованої зони і в той же час забезпечити конфіденційність, цілісність і доступність інформації при передачі між територіально розподіленими частинами єдиної інформаційно-комунікаційної мережі у кризових ситуаціях, знизить ступінь уразливості ІКМ, що використовуються для цілей державного управління, безпеки і оборони України, забезпечить захищеність державних інформаційних ресурсів та інформації.

Література

1. Комарова Л.О. Моніторинг об’єктів в умовах апріорної невизначеності джерел інформації: монографія [Текст] / Бобало Ю.Я., Даник Ю. Г., Комарова Л.О., Лук’янов О.О., Максимович В.М., Писарчук О.О., Ріппенбейн В.В., Смук Р.Т., Стогній В.С., Сторонський Ю.Б., Стрихалюк Б.М.// – Львів: 2015. Видавництво Української академії друкарства – 360 с.

2. Комарова Л.О. Математична модель каналу зв’язку [Текст] / Комарова Л.О.// Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. –К., 2008. –№15. – С. 160-168 .

3. Комарова Л.О. Інформаційне забезпечення комплексного керування захистом складних систем [Текст] / Лантвойт О.Б., Гришин С.П., Винярський Я.Я., Л.О.Комарова // Журнал «Сучасна спеціальна техніка». – К., 2011. – №2(25). – С.112 -117.

Надійшла 19.11.2015 р. Рецензент: д.т.н., проф. Железняк В.К.