УДК 004.75

Ю.Р. Гарасим, В.Б. Дудикевич
Національний університет “Львівська політехніка”,
кафедра захисту інформації

МЕТОД СТВОРЕННЯ ПРОФІЛЕЙ ЗАХИСТУ ДЛЯ МЕРЕЖ ЗВ’ЯЗКУ ТА СИСТЕМ КОМУТАЦІЇ

Розглянуто підхід до створення профілей захисту для мереж зв’язку та систем комутації, основу якого становить метод, що визначає критичність сегментів.

Ключові слова – захист, мережа, зв’язок, система комутації, метод

This paper is observed an approach of generation security profile for communication networks and switching systems basis on the method of definition segment`s criticality.

Keywords – security, network, communication, switching system, method

Вступ

Інтеграція інформаційних технологій у мережі зв’язку та системи комутації спричинила актуальність питання захисту інформації в них.

Загрози різного походження в комп’ютерних мережах та мережах передавання даних усім добре відомі. Більшість організацій витрачають великі кошти та багато часу, захищаючи конфіденційність, цілісність та доступність своїх комп’ютерних інформаційних ресурсів. Проте, аналогічні загрози властиві телекомунікаційним мережам.

Нехтування тим фактом, що можливий несанкціонований доступ (НСД) у відомчі мережі зв’язку є основою успішних дій хакерів, фрікерів та інших зловмисників (викрадення конфіденційної інформації, збитки через оплату чужих міжнародних переговорів, зниження професійної репутації компанії, фінансові втрати, які пов’язані із дефектами в роботі системи зв’язку тощо). Загроза НСД здійснюється у серце телекомунікаційної мережі – відомчої аналогової/цифрової системи комутації (відомчої АТС). До сьогодні ймовірність виявлення та покарання таких злочинів дуже мала, саме відсутність серйозної статистики свідчить лише про складність виявлення та розслідування злочинів у цій сфері. [1].

Схожість та відмінності телекомунікаційних та комп’ютерних інформаційних систем

Робота знаходиться на перетині двох галузей – телефонії та інформаційної безпеки. Перша з них успішно розвивається з 1876 р., коли Олександр Белл винайшов перший телефонний апарат. Друга – молодша та менше вивчена, вона потребує розроблення нових методів та моделей – виникла на базі інформаційних технологій, що активно інтегруються в галузь телефонії. Своєю чергою, розвиток та інтеграція IT-рішень призводить до появи нових видів загроз та вразливостей, що потребують застосування нових рішень щодо захисту чи комплексного застосування вже відомих та перевірених.

Під час розвитку відомчі АТС (ВАТС) пройшли шлях від примітивних контактно-механічних пристроїв із забезпеченням обмеженої кількості послуг до програмно-керованих цифрових систем на мікропроцесорній платформі, що забезпечують сотні додаткових видів послуг та дозволяють комутувати різні види трафіку (мова, факс, дані).

Швидкий розвиток ВАТС із відсутністю продуманого державного контролю може призвести до серйозних проблем в галузі інформаційної безпеки. Це пов'язане з тим, що створення кожної нової відомчої системи зв'язку означає формування на основі державної системи нумерації (у разі невиділеної мережі) окремої інформаційної системи з передаванням на рівень цієї мережі усіх функцій експлуатації, технічного обслуговування, адміністрування та забезпечення безпеки мережі.

Схожість телекомунікаційних та комп'ютерних систем:

- ВАТС також будуються на мікропроцесорній платформі (ЦП, ОЗП, ПЗП, пристрої вводу/виводу, ОС, прикладні програми);
- індивідуальна адресація абонентів (в ком'ютерних системах – мережева адреса, а в телефонії – телефонний номер мережі);
- великі обсяги передачі інформації;
- наявність каналів з'єднання з телефонною мережею загального користування та глобальною мережею Internet;
- цифрові методи оброблення інформації;
- використання відкритих стандартизованих протоколів взаємодії;
- децентралізоване управління;
- стратегічна важливість безперебійної, високонадійної роботи мережі, – дозволяє все вищесказане відносно проблем інформаційної безпеки комп'ютерних систем спроектувати й на сучасні системи телекомунікацій, що побудовані на комп'ютерних платформах.

Але відмінності телекомунікаційних та комп'ютерних систем вимагають індивідуального підходу до захисту ВАТС.

Серед відмінностей телекомунікаційних та комп'ютерних систем виділяють:

- ❖ кількість телефонних апаратів набагато більша від кількості комп'ютерів;
- ❖ для передачі інформації в мережі зв'язку на час сеансу встановлюється наскрізний постійний канал між абонентами, телекомунікаційні системи працюють як системи реального часу;
- ❖ технологічна неоднорідність в телекомунікаційних мережах – існує комутаційна техніка 30–40-річної давності, що використовує застарілі технології та протоколи, а також сучасні цифрові ВАТС;
- ❖ велика кількість з'єднувальних ліній для під'єднання ВАТС до телефонної мережі загального користування;
- ❖ різноманітність протоколів та фізичної області передачі інформації;
- ❖ менша доступність інформації про телекомунікаційне обладнання, повна закритість програмного забезпечення;
- ❖ складність організації покрокового тестування;
- ❖ широкий набір засобів адміністрування ВАТС дає настільки ж широкі потенційні можливості їх зловмисного використання [2].

Стан нормативно-правового забезпечення в Україні

В той час, коли весь світ поступово переходить на міжнародний стандарт ISO 15408 «The Common Criteria for Information Technology Security Evaluation» (Загальні критерії оцінки безпеки інформаційних технологій), що дозволяє проводити атестацію та сертифікацію об'єктів інформатизації за вимогами безпеки, в Україні залишаються нормативні документи системи ТЗІ: НД ТЗІ 1.1-001-99 «Технічний захист інформації на програмно-керованих АТС загального користування.

Основні положення», НД ТЗІ 3.7-002-99 «Технічний захист інформації на програмно-керованих АТС загального користування. Методика оцінки захищеності інформації (базова)», НД ТЗІ 2.5-001-99 «Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації функціональних послуг захисту», НД ТЗІ 2.5-002-99 «Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації гарантій захисту», НД ТЗІ 2.5-003-99 «Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації довірчих оцінок коректності реалізації захисту», НД ТЗІ 2.7-001-99 «Технічний захист інформації на програмно-керованих АТС загального користування. Порядок виконання робіт», якими визначається методологія створення системи ТЗІ АТС і оцінки захищеності її інформаційних ресурсів, були впроваджені ще в 90-х роках минулого століття. Сьогодні жоден з описаних в нормативних документах профіль захисту автоматизованих систем не описує підходу для визначення вимог безпеки до мереж зв'язку та вузлів комутації, що підтверджує актуальність цієї тематики. Стрімкий розвиток ВАТС не знайшов свого відображення в НД СТЗІ в Україні, що ускладнює завдання створення комплексної системи захисту в цій галузі [3, 4].

Класифікація та сегментація мереж зв'язку

Мережі зв'язку та системи комутації з точки зору інформаційних технологій можна розділити на два сегменти – системи управління та систему комутації.

З точки зору загроз інформаційній безпеці варто виділити 5 сегментів: система управління (СУ), система комутації (СК), система білінгу (СБ), абонентські пристрої (АП), сервіси.

Сучасні мережі зв'язку також поділяються на дві категорії: телефонні мережі загального користування, що відрізняються наземними каналами зв'язку, та мережі стільникових операторів, які відрізняються мобільністю абонентів та великою кількістю сервісів.

Телефонні мережі загального користування з точки зору загроз для сегментів коректно було б розділити на відомчі, місцеві та міжміські. В стільникових мережах такого поділу не відбувається.

Отже, пропонується така класифікація мереж зв'язку з точки зору інформаційної безпеки:

- відомчі;
- місцеві;
- міжміські;
- мережі стільникових операторів.

Кожен вид мережі складається з п'яти сегментів, що були описані вище, крім міжміської мережі, в якій відсутній сегмент абонентських пристроїв.

Оцінка рівня критичності сегментів мережі зв'язку та систем комутації дозволить виявити найвразливіші ділянки телефонних мереж та при проведенні робіт із захисту телефонних вузлів та мереж створити ефективнішу систему захисту інформації. Отже, на предмет критичності повинні бути проаналізовані кожен з 5 сегментів чотирьох видів мереж зв'язку.

Метод побудови профілю захисту для систем зв'язку та систем комутації

Основні компоненти методу наведені на рис. 1:

1. Метод, що визначає критичність сегментів, включає сегментацію та класифікацію мереж зв'язку та систем комутації, а також показники критичності для кожного з сегментів з точки зору інформаційної безпеки;
2. Стандарт ISO 15408.

Рис. 1. Метод побудови профілю захисту для систем зв'язку та систем комутації

Алгоритм роботи методу оцінки рівня критичності сегменту

Для оцінки рівня критичності сегменту проводиться:

- визначення приналежності сегменту до виду мережі та типу сегменту;
- складання моделі загроз для кожного сегменту кожного виду мережі;

- зіставлення моделі загроз до сегментів;
- підрахунок коефіцієнтів по кожному розділу загроз;
- порівняння отриманих результатів;
- визначення рівня критичності сегменту;
- визначення рівнів критичності;
- присвоєння рівнів критичності [5].

Створюється профіль захисту для системи управління ВАТС залежно від виду мережі зв'язку: відомчої, місцевої, міжміської або сотової (рис. 2) [6], [7], [8].

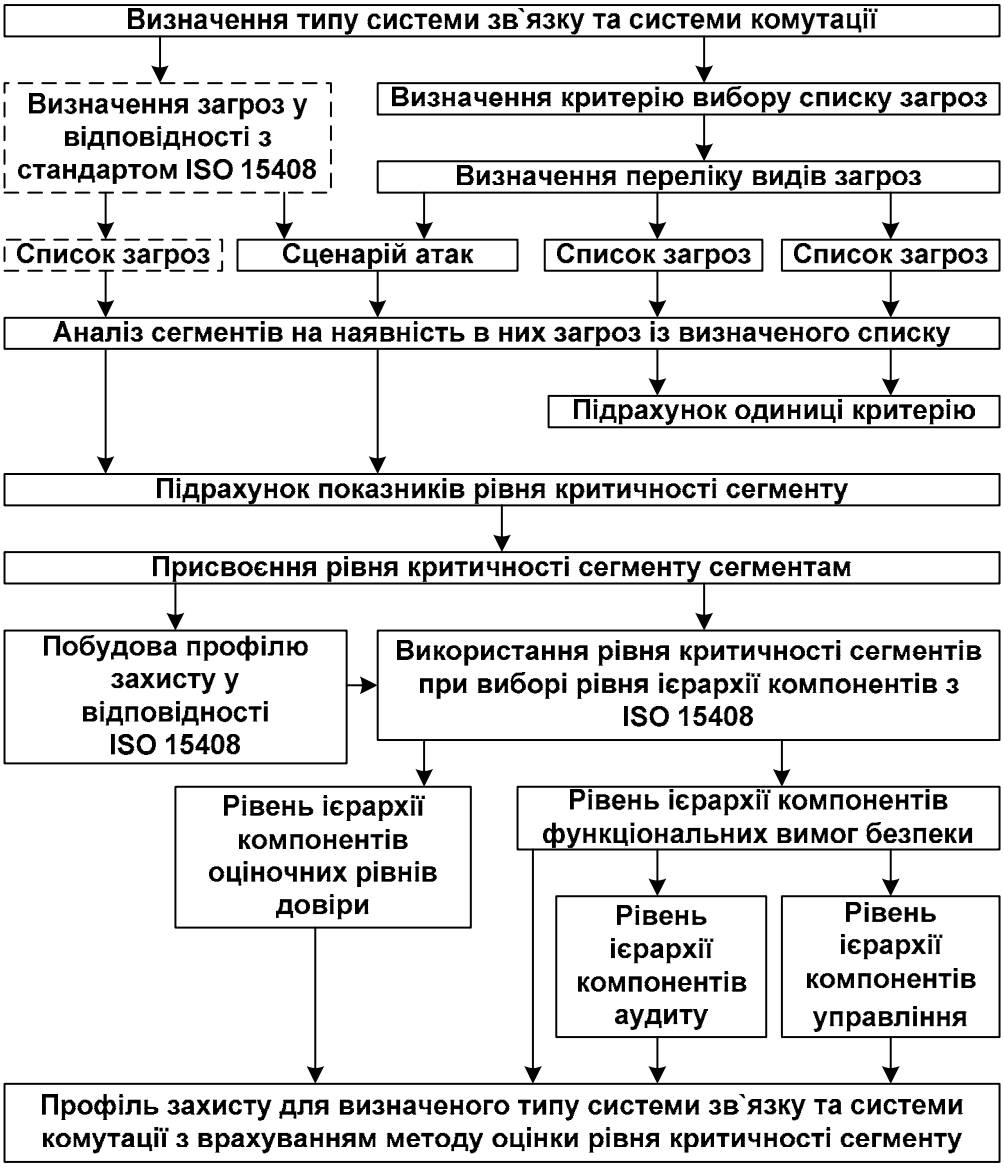

Рис. 2. Алгоритм роботи методу побудови профілю захисту для систем зв'язку та систем комутації

Висновки

Метод дає змогу оцінювати мережі зв'язку та системи комутації з точки зору інформаційної безпеки, враховуючи законодавчий аспект, специфіку об'єкта, досвід оцінювання стандартних об'єктів інформатизації.

Метод створення профілей захисту для мереж зв'язку дозволить висунути вимоги до захисту мереж зв'язку та систем комутації та сформувати їх в профіль чи завдання з безпеки.

Розроблення профілів захисту для мереж зв'язку та систем комутації дозволить атестувати мережі зв'язку та сертифікувати системи комутації відповідно до міжнародного стандарту ISO 15408.

1. Шпунт Я. Угрозы в области информационной безопасности. Новые тенденции. // Информационная безопасность и непрерывность бизнеса. Спецвыпуск №7. – М.: Intelligent Enterprise / Корпоративные системы. 2007. – С.12–17. 2. Таразевич С.А. Безопасность телефонних сетей // ЗАО «ТЕЛРОС». 3. Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення: НД ТЗІ 1.1-001-99 – Офіц. вид. – К. : ДСТСЗІ СБ України, 1999. – 15 с. – (Нормативний документ системи технічного захисту інформації). 4. Технічний захист інформації на програмно-керованих АТС загального користування. Методика оцінки захищеності інформації (базова): НД ТЗІ 3.7-002-99. – Офіц. вид. – К. : ДСТСЗІ СБ України, 1999. – 34 с. – (Нормативний документ системи технічного захисту інформації). 5. Минакова Н.А. Метод определения уровня критичности сегментов (МОУКС) сетей связи и систем коммутации. // Тр. 10-й междунар. Конф. «Теория и технология программирования и защиты информации», «Университетские телекоммуникации». – С.39–42, (2006г., г. Санкт-Петербург). 6. Васильева Н.А. Метод определения рекомендуемого уровня защищенности для сетей связи и систем коммутации // Журн. Научн. Публ. Аспир. и доктор. – С.22–29, (апрель 2008г., Курск). 7. Michael J. Wenstrom. Managing Cisco Network Security. – Indianapolis, USA: Cisco Press, 2001. – 768 p. 8. Menezes R. Self-Organization and Computer Security // Proceeding of the 2005 ACM Symposium on Applied Computing (SAC'05). – ACM, 2005.