

**Романов В.В., Савчук О.В.**

ННК “Інститут прикладного системного аналізу” НТУУ “КПІ”, Київ, Україна

## Організація інформаційної безпеки в мережі IP-телефонії

Фактор широкого розповсюдження систем IP-телефонії обумовлює актуальність досліджень з організації інформаційної безпеки в мережі IP-телефонії.

Перед проектуванням власної системи захисту інформації у мережі IP-телефонії необхідно було провести огляд і аналіз існуючих рішень, а саме:

- виявити та систематизувати можливі загрози в системах IP-телефонії;
- проаналізувати та визначити засоби захисту сигнальних протоколів;
- визначити та систематизувати засоби захисту систем IP-телефонії;
- проаналізувати різні реалізації систем IP-телефонії;
- визначити практичні рекомендації для розробки та впровадження систем захисту.

В роботі представлені схеми захисту від двох провідних постачальників VoIP- обладнання – Cisco та Avaya. Проведений аналіз ефективності існуючих систем, а також підрахунок їх вартості, виявив їх переваги та недоліки.

Компанія Cisco в черговий раз довела, що вона здатна побудувати VoIP-мережу, яка може серйозно протистояти витонченим хакерських атакам. Обрана IP-телефонна мережа з використанням мережевої інфраструктури третього рівня та додаткових засобів безпеки – найбільш досконале рішення на сьогоднішній день, що використовує всі доступні засоби захисту. Необхідно підкреслити, що представлена топологія складається з набагато більшої кількості засобів безпеки, ніж використовується більшістю користувачів. Схема Cisco забезпечує ряд потужних додаткових можливостей: захист від переповнення буферів сервера; недопущення запуску незареєстрованих додатків; захист від атак типу syn flood на стек протоколу TCP-сервера; визначення сканування портів, яке зазвичай проводиться хакерами для виявлення запущених сервісів і їх можливих вразливостей перед початком атаки [1].

Розглянуті в роботі схеми захисту відомих компаній потребують багато фінансових ресурсів, тому однією із компаній України з інформаційних технологій було поставлено завдання спроектувати систему, яка була б оптимальним варіантом за показником ціна/якість, і відповідала б наступним вимогам:

- працювала на основі SIP-протоколу;
- забезпечувала захист від різноманітних атак, направлених на вузли системи;
- відповідала вимогам відмовостійкості;
- забезпечувала сервісом не менш ніж 4 тисячі абонентів;
- легко розширювалась у бік нарощування потужностей;
- не давала можливості маніпулювання сервісами;
- легко була інтегрована в існуючу мережу;

З точки зору вибору обладнання були обрані наступні критерії: -вартість (порта, обслуговування, установки); -функціональні можливості (сервісні, підтримуємі протоколи, можливість нарощування системи); -технічні характеристики (кількість портів, надійність). Попередній аналіз показав, що системі потрібен SoftSwitch для встановлення і проведення з'єднань, прикордонний мережевий екран для захисту, коммутатор для підключення обладнання та додаткових сервісів. Також потрібно реалізувати елемент відмовостійкості та контролю навантаження.

Виходячи з заявлених умов до обладнання та аналізу існуючих систем, було вирішено взяти: в якості SoftSwitch – Cisco BTS 10200; в якості прикордонного контролера доступу – Асме SBC серії Net-Net-4000; в якості Switch – Cisco 3560.

Все обладнання буде розташовано на двох технічних площадках. Устаткування серії Net-Net 4000 може бути налаштоване для підтримки як інтегрованої, так і розподіленої моделі прикордонного контролера сесій. В якості інтегрованого SBC платформа Net-Net 4000 виконує функції управління сесіями на кордоні мережі та управління середовищем передачі даних (шлюзу

packet-to-packet - пакетного шлюзу) з високим ступенем інтеграції. Розподілена конфігурація SBC дозволяє фізично розділити функції управління сесіями на кордоні мережі та функції управління середовищем передачі даних за допомогою стандартного інтерфейсу управління.

Програмний комутатор Cisco BTS 10200 також служить інтерфейсом до платформ додаткових послуг та передових програм. Використовуючи функціональні можливості пакетних мереж і одночасно підтримуючи традиційні інфраструктури комутації каналів, програмний комутатор Cisco BTS 10200 надає провайдерам послуг і операторам можливість поступового переходу до пакетних мереж.

Впровадження комутатора Cisco BTS 10200 забезпечить швидке розгортання послуг, надійність операторського класу, гнучкість надання послуг, масштабованість та економію коштів за рахунок оптимізації капіталовкладень та ефективності процесу експлуатації. Система управління програмним комутатором Cisco BTS 10200 надає оператору гнучкі можливості по маршрутизації голосового трафіку.

Комутатори сімейства Cisco Catalyst 3560 - це лінійка комутаторів корпоративного класу з фіксованою конфігурацією. Вони призначені для локальних мереж невеликих підприємств або віддалених офісів і відмінно підходять на роль комутатора мережі доступу. Ці комутатори ідеально підходять для локальних мереж доступу підприємств і філій. Завдяки підтримці портів 10/100/1000 Мбіт/с і технології PoE, пристрої дозволяють розгорнути нові програми, такі як IP-телефонія, бездротовий доступ, відеоспостереження [2].

Представлена схема захисту може підтримувати до 3 тисяч SIP сесій водночас, що в свою чергу може задовольнити до 5 тисяч абонентів. Оновлення існуючих та додавання нових сервісів реалізується налаштуванням відповідного ПЗ на Cisco BTS, або підключенням відповідних серверів до Cisco 3560, для цього передбачено 24 гігабітних порта та 4 SFP модуля. Отже розроблена схема легко розширюється в разі потреби і забезпечує сервісом заявлену кількість абонентів.

Безпеку інформації в даній схемі реалізовано на двох SBC. Абсолютно весь трафік, надходячий до мережі оператора, буде спершу надходити до SBC, а потім, після проходження фільтрів, поступати далі в мережу.

Отже система має наступні апаратні і програмні характеристики:

- Підтримка трьох тисяч SIP-сесій водночас.
- Максимальна кількість абонентів дорівнює п'яти тисячам абонентів.
- Мережеві екрани SBC гарантують захист від Dos-атак.
- Також Асте підтримує функцію авторизацію клієнтів, що виключає можливість маніпуляції з сервісами, контроль навантаження на прикордонних екранах.
- Система легко інтегрується в існуючу мережу провайдера.
- Система виконана з урахування вимогам відмовостійкості.
- Завдяки великій кількості портів на комутаторах, система легко розширюється і дає змогу легко підключати нові сервіси.
- Все обладнання підключене до елементів безперебійного живлення і бензинового генератора.

Розміщення системи легко забезпечується існуючими площами приміщень провайдера на двох технічних площадках. Особливість реалізації VoIP дає змогу підключити будь якого клієнта не тільки з мережі провайдера, але і з інших мереж [3].

**Література.** **1.** Ernest Brickell, Clinton Brooks, Vinton Cerf, Whitfield Die, Susan Landau, Jon Peterson, John Treichler. - Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP. - June 13, 2006., **2.** Gokul Bhupathiraju. Security aspects in Voice over IP systems. - November 16, 2006. **3.** David Endler, Mark Collier. Hacking Exposed VoIP: Voice Over IP Security Secrets & Solutions. - McGraw-Hill/Osborne. - 2007.