УДК 621.396

ДИСПЕРСІЙНИЙ АНАЛІЗ МЕРЕЖНОГО ТРАФІКУ ДЛЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ

***О.А. Смірнов**, к.т.н., доцент, **Д.О. Даниленко**, асп.*
Кіровоградський національний технічний університет
assa_s@mail.ru

Сучасний розвиток телекомунікаційних систем та мереж і застосовуваних комп'ютерних технологій привів до появи якісно нових послуг і сервісів в інформаційній сфері, впровадження передових технологій обробки й передачі даних й їхньої доступності широкій користувальницькій аудиторії [1]. У той же час інтенсивний розвиток сучасних комп'ютерних технологій привів до появи нових погроз безпеки інформації, виникнення нових форм і способів несанкціонованого доступу до обчислювальних ресурсів телекомунікаційних систем та мереж [1-4]. Зокрема, найбільшу уразливість представляють застосовувані методи мережного управління, технології доступу до надаваних сервісів і послуг, процеси моніторингу стану телекомунікаційних систем та мереж. Під впливом шкідливого програмного забезпечення окремі комунікаційні й обчислювальні компоненти можуть бути переведені в несанкціоновані режими функціонування, що приводить до збоїв, різних порушень установленого порядку їхнього використання, знищення, перекручування, блокування, несанкціонованого витоку оброблюваної й переданої інформації, а також до порушення роботи методів і алгоритмів маршрутизації між вузлами телекомунікаційної системи [2-4]. Отже, розробка й дослідження методів моніторингу мережної активності, технологій виявлення шкідливого програмного забезпечення й запобігання його впливу на інфокомунікаційні ресурси, які захищаються, є актуальною науково-прикладною проблемою, її рішення безпосередньо пов'язане із забезпеченням безпеки сучасних телекомунікаційних систем та мереж й застосовуваних комп'ютерних технологій.

Мета даної роботи складається в проведенні експериментальних досліджень властивостей мережного трафіку при використанні різних телекомунікаційних служб і інформаційних сервісів, аналіз і обробка отриманих статистичних даних для обґрунтування практичних рекомендацій з побудови програмних і апаратних засобів моніторингу мережної активності, виявлення шкідливого програмного забезпечення й запобігання його впливу на інфокомунікаційні ресурси, які захищаються, для забезпечення безпеки сучасних телекомунікаційних систем та мереж.

Для забезпечення безпеки в сучасних телекомунікаційних системах та мережах застосовуються різні організаційно-технічні заходи, найбільш ефективні з яких складаються в побудові т.зв. систем виявлення (Intrusion Detection System – IDS) і запобігання (Intrusion Prevention System – IPS) вторгнень [2-4]. В основі функціонування IDS і IPS лежить збір, аналіз і обробка інформації про події, пов'язані з безпекою телекомунікаційної системи, яка захищається, накоплення отриманих даних і, на основі результатів проведеного аналізу (моніторингу) мережної активності окремих служб і сервісів, прийняття рішення щодо стану системи, яка захищається, з виявленням і можливою протидією несанкціонованому використанню інфокомунікаційних ресурсів [2-4].

Під системою виявлення вторгнень (СВВ) розуміють програмний або апаратний засіб, призначений для виявлення фактів неавторизованого доступу в комп'ютерну систему або мережу або несанкціоноване управління [2-4].

Під системою запобігання вторгнень (СЗВ) розуміють програмну або апаратну систему мережної й комп'ютерної безпеки, яка виявляє вторгнення або порушення безпеки, а також, яка реалізує автоматичний захист від виявлених порушень [2-4]. Системи IPS варто розглядати як розширення систем IDS. У той же час СЗВ відрізняються необхідністю відстеження мережної активності в реальному часі зі швидким реагуванням за допомогою реалізації відповідних дій по запобіганню виявлених атак. Можливі міри запобігання атак складаються в блокуванні потоків трафіку в телекомунікаційній мережі, скиданні з'єднань, видачі сигналів операторові й т.д. [2].

Перспективним напрямком у забезпеченні безпеки сучасних телекомунікаційних систем та мереж є застосування методів моніторингу мережної активності, технологій виявлення шкідливого програмного забезпечення й запобігання його впливу на інфокомунікаційні ресурси, що захищаються. Найпотужнішим механізмом вирішення вказаних задач є застосування методів виявлення і запобігання вторгнень у складі IDS та IPS систем, в основі роботи яких лежить використання статистичних даних про мережний трафік.

Для обробки експериментальних даних про мережний трафік телекомунікаційних систем і дослідження їх статистичних властивостей запропоновано використання математичного апарату дисперсійного аналізу. Він заснований на оцінці відносин вибіркових дисперсій та дозволяє підтвердити або спростувати статистичну гіпотезу про однорідність результатів моделювання по показнику розсіювання, обґрунтувати практичні рекомендації з побудови програмних і апаратних засобів моніторингу мережної активності для виявлення і запобігання вторгнень та підвищити таким чином рівень інформаційної безпеки в сучасних телекомунікаційних системах і мережах.

Література

1. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2010. – 944 с.
2. NIST Special Publication 800-94. Guide to Intrusion Detection and Prevention Systems (IDPS). – Computer Security Division Information Technology Laboratory National Institute of Standards and Technology, Gaithersburg. – 127 pages (February 2007)
3. Brian Caswell, Jay Beale, Andrew Baker. Snort Intrusion Detection and Prevention Toolkit. – Syngress Media, U.S. 2006.
4. Запечников С.В., Милославская Н.Г., Толстой А.И., Ушаков Д.В. Информационная безопасность открытых систем. Учебник для вузов. В 2-х томах. – М., 2008. – Т. II: Средства защиты в сетях. – 558 с.