2. Додонов А.Г., Кузнецова М.Г., Горбачик Е.С. Введение в теорию живучести вычислительных систем. – К.: Наук. Думка, 1990. – 184 с.

3. Романов О.І., Лівенцев С.П., Павлов І.М. Методика оцінювання надійності комплексних систем захисту інформації у спеціальних телекомунікаційних системах // Зв'язок, 2005. – № 2. – С. 36-38.

4. Рижаков В.А., Сакович Л.М. Кількісне оцінювання структурної надійності систем зв'язку // Зв'язок, 2004. – № 4. – С. 53-57.

5. Леваков А. Анатомия информационной безопасности США. Jet Info online №6(109). -- 2002. *http://daily.sec.ru/dailypblshow.cfm?rid=9&pid=5503&pos= =13&stp= 10.*

6. Леваков А. В интересах внутренней безопасности США. Jet Info Специальный выпуск. 2004. – С. 36. *http://www.jetinfo.ru.*

7. Богуш В.М., Юдін О.К. Інформаційна безпека держави. - К.: МК-Прес, 2005. – 432 с.

Надійшла 29.09.2006

УДК 681.3

Дуткевич Т.В., Піскозуб А.З.

ОСОБЛИВОСТІ ЗАСТОСУВАННЯ СИСТЕМ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ АТАК У ВИСОКОШВИДКІСНИХ КОРПОРАТИВНИХ МЕРЕЖАХ

1. Основні проблеми виявлення та запобігання атак в корпоративних мережах

Проблема безпеки корпоративних мереж набуває надзвичайної актуальності. Існуючі на сьогодні методи захисту: брандмауери, антивіруси, віртуальні мережі, системи виявлення та запобігання атак - не здатні у повній мірі задовольняти вимоги корпоративного інформаційного середовища. В умовах чіткої тенденції до масового використання сучасних засобів телекомунікації, зокрема мережі Internet, у бізнес-процесах та з іншого боку, зростання складності Internet загроз - вірусів і хробаків, DoS атак, атак на засоби електронної комерції, життєво важливим є забезпечення високого рівня захисту ресурсів корпоративних мереж. Тому виникає потреба у дослідженні проблем систем безпеки та розробки нових методів, здатних ефективно захищати ресурси корпоративних мереж [1].

Традиційні програмні та апаратні засоби не відповідають вимогам корпоративних мереж, оскільки вони не здатні ефективно аналізувати потік даних, не знижуючи при цьому загальної продуктивності мережі. Висока вартість комерційних кінцевих рішень не дозволяє широко впроваджувати їх у вітчизняні корпоративні мережі.

Дана проблема робить особливо актуальною розробку спеціалізованих засобів, зокрема систем виявлення та запобігання атак, в основі яких лежить рішення з відкритим кодом, для ефективного захисту високошвидкісного середовища корпоративної мережі.

Останні дослідження проведені групою дослідницьких лабораторій NSS відображають переваги тільки кінцевих продуктів окремих виробників. На скільки нам відомо, інших ґрунтовних досліджень особливостей підходів виробників до виявлення атак, результати яких доступні для публічного ознайомлення, немає. Наявні результати досліджень не можуть мати достатньої достовірності, оскільки, в більшості випадків, проводяться на замовлення виробників і як результат - недолікам приділяють недостатньо уваги. Перебільшення отриманих результатів призводить до хибного відчуття безпеки.

Невирішеними залишається ряд проблем. Серед них: відсутність стандартизованих методів оцінки продуктивності та ефективності систем виявлення та запобігання атак, відсутність єдиних підходів до виявлення атак, не зацікавленість більшості комерційних виробників у розвитку вільного програмного забезпечення, низька сумісність кінцевих

рішень з рішеннями сторонніх виробників, велика вартість кінцевих рішень. Виникає завдання виявити недоліки та переваги запропонованих виробниками підходів виявлення та запобігання атак.

Метою статті є виявити переваги та недоліки існуючих комерційних рішень та рішень з відкритим кодом на основі єдиного підходу до оцінки систем виявлення та запобігання атак, дати оцінку щодо придатності та доцільності їх використання, виявити перспективні підходи виявлення та запобігання атак, розглянути напрямки розвитку підходів до виявлення та запобігання атак в високошвидкісних корпоративних мережах. Визначити чи здатні існуючі системи виявлення та запобігання атак з відкритим кодом використовуватися, як альтернативна комерційним системам виявлення атак. Результати викладені в даний статті є основою для наших подальших досліджень в напрямку підвищення ефективності методів виявлення та запобігання атак.

Для ефективного проведення досліджень визначимо основні вимоги корпоративних мереж, дотримання яких дозволить досягнути високої надійності засобу виявлення та запобігання атак як елемента мережевої інфраструктури, і лінійної продуктивності, яка гарантує відсутність сповільнення роботи мережі. Такими вимогами є мала затримка, мультигігабітна швидкість, велика кількість з'єднань, висока доступність та відмінна точність: *Мала затримка* – не більше 3 мілісекунд, – незалежно від розміру кадру, типу трафіку, пропускної здатності чи кількості фільтрів для виявлення атак затримка не повинна перевищувати вказаного значення. В іншому разі можливе суттєве зниження продуктивності мережі, що в деяких випадках призводить до її непрацездатності. В таблиці 1 наведено залежність швидкості передачі даних в мережі від часу затримки пакетів пристроєм.

Таблиця 1

Ефективна швидкість передачі даних в мережі

Середня затримка	Ефективна швидкість
10 мікросекунд	1 Гбіт/с
100 мікросекунд	100 Мбіт/с
1 мілісекунд	1 Мбіт/с
10 мілісекунд	100 Кбіт/с
100 мілісекунд	10 Кбіт/с
1 секунда	1 Кбіт/с

Мультигігабітна швидкість – IDS та IPS повинні бути здатними аналізувати магістральний трафік для захисту від внутрішніх атак.

Велика кількість з'єднань – IDS та IPS повинні підтримувати до 1 мільйона одночасних з'єднань та десятків тисяч нових з'єднань за секунду.

Висока доступність – в разі виходу з ладу IDS або IPS повинні переключатися в режим "прозорого" комутатора.

Відмінна точність – при перевірці трафіку IDS чи IPS повинні мати достатню обчислювальну потужність для визначення легітимного трафіку і пропускати лише його [2].

2. Особливості архітектур та кінцевих рішень систем виявлення та запобігання атак

Кожен виробник має власне бачення корпоративної безпеки. Найбільшими виробниками програмно-апаратних продуктів захисту є компанії Internet Security Systems, Cisco Systems, TippingPoint та Sourcefire. Розглянемо особливості підходів, які використовує кожен виробник та спробуємо здійснити аналіз відповідності запропонованих рішень вимогам корпоративних мереж.

2.1. Комерційні рішення від компанії Cisco Systems

Cisco Systems - лідер у виробництві мережевого обладнання, власну філософію безпеки представляє в архітектурі SAFE (див. рис.1). Вона спроектована для запобігання та вдалого проведення більшості атак на вразливі ресурси корпоративної мережі. Архітектура SAFE не є революційним підходом у проектуванні мереж, а тільки рекомендаціями щодо мережевої безпеки. SAFE пропонує два дизайни: централізований чи односайтовий і розподілений чи багатосайтовий. В односайтовому дизайні рекомендують розміщувати мережеві IDS сенсори в корпоративних модулях, модулях керування, VPN модулях, модулях сервера, модулях зовнішніх ресурсів, модулях електронної комерції. При чому, в кожному модулі розміщений резервний сенсор. Така надлишковість дозволяє контролювати мережу в разі виходу з ладу обладнання чи зміни шляху маршрутизації пакетів [3].

Рис. 1. Структура архітектури SAFE

В багатосайтовому дизайні моніторинг трафіку в корпоративній мережі розподіляється на відокремлені частини і здійснюється на локальному, регіональному рівні та рівні корпоративної мережі за допомогою захищених, виділених на певний період часу з'єднань. Дві серії IDS і IPS призначені для використання в високошвидкісних корпоративних мережах - Cisco IPS 4200 та Cisco Catalyst 6500 IDS [3].

Cisco IPS 4200 – серія систем запобігання атак, спеціально спроектована для ефективної паралельної перевірки декількох мережевих сегментів через їх підключення до 8 мережевих інтерфейсів, причому підтримується робота одночасно в двох режимах – пасивному (passive) та вбудованому (inline). При поєднанні з модулем Cisco EtherChannel для вирівнювання навантаження в комутаторах серії Cisco Catalyst 6500, пристрої здійснюють аналіз трафіку зі швидкістю передавання даних в мережі до 8 Гбіт/с.

Сервісний IDS модуль IDSM-2 для серії Cisco Catalyst 6500 дозволяє інтегрувати усі можливості IPS в комутатори цієї серії, причому аналіз трафіку здійснюється зі швидкістю до 600 Мбіт/с [4].

Характеристики окремих IDS та IPS від компанії Cisco Systems представлені в табл. 2:

Таблиця 2. Характеристики IDS та IPS від компанії Cisco Systems

	Cisco IDS 4250-XL	Cisco IPS 4255	Cisco IDSM-2
Продуктивність, Мбіт/с	800	500	600
З'єднань за секунду	4000	5000	6000

2.2. Комерційні рішення від компанії Internet Security Systems

Internet Security Systems (ISS) пропонує архітектуру безпеки Proventia Enterprise Security Platform (ESP) (див. рис.2) і акцентує увагу не на реакції на атаку, а на випереджаючому блокуванні ймовірної атаки, зупиняючи атаку ще до її здійснення. Перевагою Proventia ESP є потужне, єдине ядро, яке використовується для всіх продуктів, що забезпечують безпеку мережі. Сімейство продуктів Proventia ESP включає системи попередження атак, міжмережеві екрани, віртуальні приватні мережі (VPN), системи оцінки вразливостей, антивіруси, засоби безпеки електронної почти, Web-фільтри, антишпигунські модулі і системи захисту програм. Додатково здійснюється контроль і захист серверів, мереж, робочих станцій, безпровідних точок доступу, віддалених точок доступу з врахуванням їх особливостей. Всі засоби безпеки можуть централізовано керуватися за допомогою системи керування SiteProtector [5]. Інтегрована, випереджаюча технологія захисту надає такі переваги: забезпечення мережевої та системної цілісності, захист від втрати конфіденційної інформації, зниження необхідності негайного поновлення виявлених вразливих систем, краща сумісність з іншими засобами захисту.

Розглянемо особливості запропонованих компанією ISS рішень. Серії Proventia Integrated Security Appliances (ISA) M50 і M30 поєднують систему запобігання атак з міжмережевим екраном, сигнатурним і аномальним типом антивірусу, VPN, Web-фільтрами і антишпигунськими технологіями. Proventia ISA M50 спроектована з врахуванням потреб великих корпоративних мереж, дозволяє підключати до 2500 вузлів, гарантує постійну доступність мережі і найважливіших систем. Proventia ISA M30 використовується для сегментів мережі і дозволяє контролювати до 500 вузлів.

Рис. 2. Архітектура безпеки Proventia ESP

Як Proventia ISA M50, так і M30 пропонують захист від загроз, який дозволяє, не знижуючи продуктивності мережі, блокувати небезпечний код та атаки типу MS Blaster, Sasser і SQL Slammer [6]. Серія IDS Proventia A здатна перевіряти до 4 сегментів мережі змішаного типу і виконувати аналіз трафіку з пропускною здатністю від 200 до 1200 Мбіт/с [7]. Технічні параметри серій Proventia ISA наведені в таблиці 3.

Таблиця 3.
Характеристики IDS та IPS компанії ISS

	Серія Proventia M30	**Серія Proventia M50**	**Серія Proventia A**
Кількість протоколів які перевіряються	Більше 137	Більше 137	Більше 137
Кількість відомих атак	Більше 2500	Більше 2500	Більше 2500
Кількість атак які виявляються без додаткового налаштування	Більше 600	Більше 600	1700
Максимальна кількість хостів	500	2500	4 мережеві сегменти
Продуктивність	200 Мбіт/с	800 Мбіт/с	1200 Мбіт/с
Максимальна кількість нових з'єднань	4,100	12,000	20,000
Максимальна кількість з'єднань	101,000	101,000	N/A

2.3. Комерційні рішення від компанії TippingPoint

Компанія TippingPoint пропонує архітектуру системи безпеки (див. рис. 3), спеціально спроектовану відповідно до потреб провайдерів, навчальних установ, закладів охорони здоров'я, фінансових інституцій, урядових установ, корпоративних мереж.

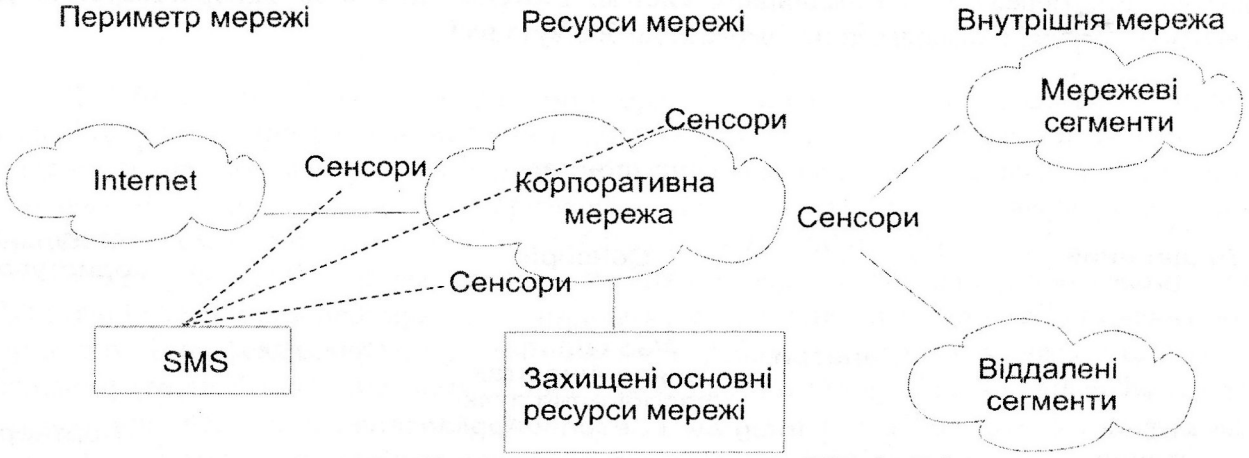

Рис. 3. Архітектура безпеки компанії TippingPoint

Сімейство продуктів TippingPoint містить системи запобігання атак, які призначені для захисту периметру мережі, внутрішніх мережевих сегментів, центральних ресурсів мережі та ресурсів віддалених підрозділів. Сенсори системи забігання атак централізовано керуються з допомогою системи керування безпекою TippingPoint Security Management System (SMS), внаслідок чого досягається підвищення безпеки і ефективності мережевої політики безпеки. Мережа може бути поділена на фізичні або логічні сегменти з додаванням політики безпеки для кожного сегменту[8].

Особливістю архітектури мережевої безпеки TippingPoint є захист протоколів і програм від затоплення трафіком, переповнення буферу, невідомих атак і вразливостей. Пристрої, які є складовими даної архітектури безпеки, виконують нормалізацію трафіку для виявлення небезпечних або недопустимих пакетів, здійснюють повторну побудову TCP пакету і IP-дефрагментацію, що дозволяє збільшити пропускну здатність мережі і захищати її від багатьох методів проникнення.

Пристрої TippingPoint забезпечують значну продуктивність, стабільність і точність. Ці переваги досягаються за рахунок використання механізму знешкодження небезпеки TippingPoint's Threat Suppression Engine (TSE). TSE являє собою лінійний апаратний процесор, який містить всі функції, необхідні для запобігання атак - IP-дефрагментацію, повторну побудову TCP-потоку, статистичний аналіз, формування трафіку, блокування потоку, визначення стану потоку і перевірку прикладного рівня в 170 протоколах [9]. Блок-схема архітектури TSE наведена на рис. 4. TSE перебудовує і перевіряє вміст потоку на прикладному рівні. Потік перевіряється на присутність небезпечного вмісту кожен раз, коли система отримує новий пакет, що розпочинає новий сеанс з'єднання. Як тільки потік вважається підозрілим, отриманий пакет і всі наступні пакети його послідовності блокуються. Це гарантує неможливість досягнення атаки до місця призначення.

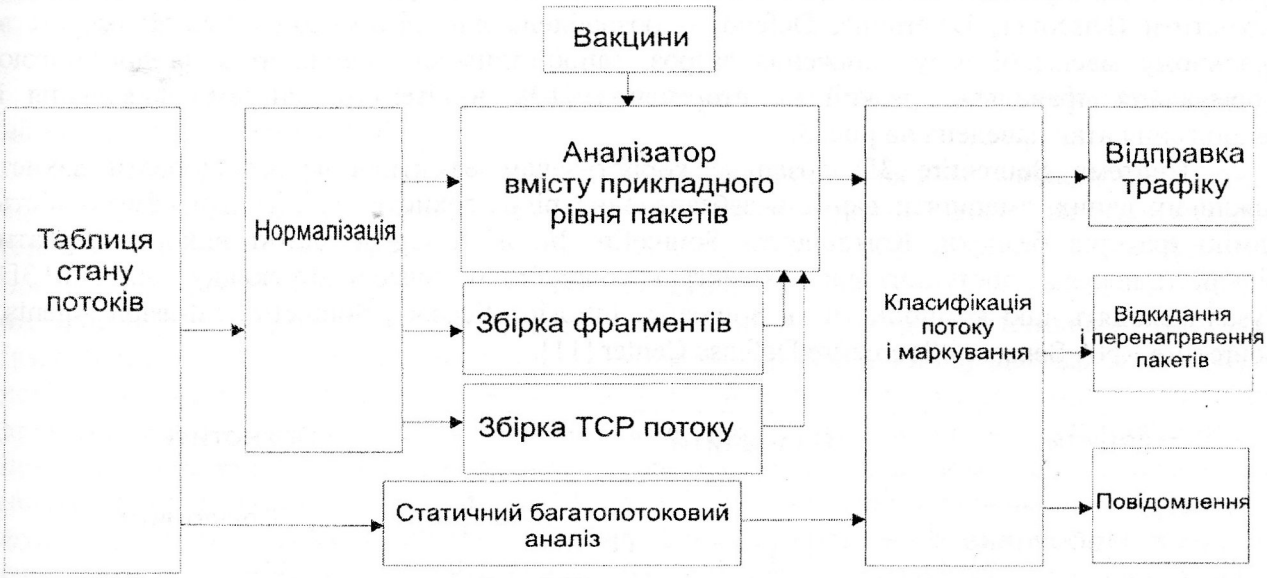

Рис. 4. Блок-схема архітектури TSE

Наведена технологія запобігання атак є поєднанням високошвидкісних мережевих процесорів і процесорів аналізу окремих програм (ASIC - application specific processors). Ці високоспеціалізовані процесори дозволяють IPS запобігати атакам з високою точністю, при швидкості трафіку у декілька Гбіт/с і мікросекундними затримками. Можливість масштабування системи дозволяє функціонувати одночасно тисячам фільтрів, не впливаючи на продуктивність чи точність. В архітектурі TSE використовуються спеціалізовані ASIC, магістральна шина з перепускною здатністю 20 Гбіт/с і високопродуктивний мережевий процесор для виконання повної перевірки потоку на 2-7 рівнях [9]. Особливості системи виявлення атак для корпоративних мереж від компанії TippingPoint наведені в табл. 4.

Таблиця 4

Характеристики IDS компанії TippingPoint

	TippingPoint 5000E
Кількість відомих протоколів	170
Продуктивність	5.0 Гбіт/с
Затримка	< 150 мс
Кількість одночасних з'єднань	2,000,000
Кількість нових з'єднань	1,000,000

2.4 Особливості рішень компанії Sourcefire для виявлення атак в корпоративних мережах

У підході компанії Sourcefire поєднуються гнучкість і точність у виявленні і запобіганні атак з революційним підходом дослідження особливостей мережі і виявленням вразливостей. Архітектура системи безпеки Sourcefire 3D System – Виявити, Визначити, Захистити (Discover, Determine, Defend) – розроблена для ефективного захисту мереж в реальному масштабі часу, зниження загроз, запобігання здійснення атак за допомогою формування правильної реакції на вторгнення [10]. Архітектура системи виявлення і запобігання атак наведена на рис. 5.

Система Sourcefire 3D дозволяє користувачам ефективніше здійснювати захист важливих даних, зменшити вартість забезпечення рівня захисту і збільшити ефективність адміністраторів безпеки. Компоненти Sourcefire Intrusion Agent здатні використовувати більшість переваг, доступних для архітектури Sourcefire 3D System. До складу Sourcefire 3D System входять такі компоненти як Sourcefire Intrusion Sensors, Sourcefire Intrusion Agents, Sourcefire RNA Sensors і Sourcefire Defense Center [11].

Рис. 5. Архітектура безпеки Sourcefire 3D System

Сенсор системи виявлення атак Sourcefire Intrusion Sensor здійснює виявлення і запобігання атак, аналізуючи трафік мережі з продуктивністю до 8 Гбіт/с – при виявленні загрози може блокувати, повідомляти про атаку чи навіть модифікувати підозрілі пакети. На відміну від IPS першого покоління Sourcefire Intrusion Sensors мають надзвичайну точність, зменшуючи ризики пов'язані з проблемами хибного спрацювання (false positives), методами проникнення і потенційними умовами для відмови в обслуговуванні.

Таблиця 5.
Характеристики IDS Sourcefire IS5800

	Sourcefire IS5800
Кількість відомих протоколів	135
Кількість відомих атак	3600*
Затримка	100 мілісекунд
Продуктивність	До 4 Гбіт/с
Кількість одночасних з'єднань	1,000,000
Кількість нових з'єднань	16,000

* - Використовує сигнатури для IDS Snort

Основним компонентом архітектури Sourcefire 3D System є система виявлення атак IS5800. Вона розроблена з врахуванням особливостей корпоративних мереж. Висока продуктивність IS5800 досягається за рахунок використання спеціалізованих процесорів для обробки мережевого трафіку. Максимальна кількість процесорів – 14. IS5800 дозволяє "гарячу" заміну і гарантує високу доступність для всіх компонентів системи: блоків живлення, інтерфейсних карт, дисків і процесорів [12]. Особливості рішень компанії Sourcefire подані в табл. 5.

2.5. Особливості систем виявлення атак та запобігання атак з відкритим кодом на прикладі системи SNORT

Snort - це безкоштовна система виявлення та запобігання атак з відкритим кодом, в якій поєднується два способи виявлення та запобігання мережних атак – за їх сигнатурою (система, базована на правилах (rule-based system)), чи на основі детектування аномалій (адаптивна (adaptive system) чи безсигнатурна система). Для першого методу використовується новий високопродуктивний аналізатор (High Performance Multi-Rule Inspection Engine), що здатний аналізувати мережевий трафік, який передається зі швидкістю декількох Гбіт/с, використовуючи велику кількість правил без втрати пакетів [13]. В основі другого, безсигнатурного методу виявлення атак лежить так званий "нормальний" профіль поведінки системи, коли Snort дозволяє виявляти нові атаки, зокрема: відхилення від нормального функціонування мережі. Інформація про виявленні порушення нормального функціонування мережі записуються в базу даних. Додатково записуються пакети, які спричинили спрацювання системи, що дозволяє проводити подальше дослідження виявлених атак. Безсигнатурна модель виявлення атак реалізована у вигляді препроцесорів. На сьогодні використовується десять препроцесорів, оптимізованих для виконання вузькоспеціалізованих завдань. Крім безсигнатурної моделі препроцесори реалізують функції контролю вмісту пакетів [14]. Snort може інтегруватися з іншими засобами безпеки корпоративної мережі, зокрема, міжмережевими екранами.

3. Висновки та перспективи

Підсумовуючи особливості підходів виробників систем безпеки до виявлення атак, зазначимо, що усі виробники IDS чи IPS застосовують подібні підходи – розподілені мережеві архітектури IDS чи IPS. При цьому основну увагу виробники приділяють сенсорам системи виявлення атак і системам їх керування. Найбільша продуктивність досягається за рахунок використання спеціалізованих процесорів і спеціалізованого програмного забезпечення, яке враховує особливості середовища, в якому воно функціонує (TippingPoing 5000E, Sourcefire IS 5800) або використання системи виявлення атак в запропонованій виробником архітектурі (Cisco Systems IDS 4200 Sensor Series, Cisco Systems IDSM-2, ISS Poventia M30 and M50 Series, ISS Proventia A series).

Розглянувши системи різних виробників, ми прийшли до висновку, що всі вони є дорогі, мають велику складність і не завжди можна адекватно вибрати то чи інше рішення для конкретної мережі за всіма параметрами – продуктивністю, кількістю сигнатур, кількістю з'єднань.

Кожен виробник використовує власний підхід, проте в основі кожного методу лежить сигнатурний підхід. Проте ситуація може змінитися, оскільки обчислювальна потужність процесорів зростає і це дозволить ефективно використовувати штучний інтелект для виявлення і запобігання атак.

Іншою проблемою є велика початкова вартість – 8000-80000/сенсор, що суттєво звужує коло українських установ та компаній, які можуть ефективно впровадити ці комерційні рішення. Одним з вирішень даної проблеми є використання програмного забезпечення з відкритим кодом, яке може вільно використовуватись, проте вимагає значних затрат фахівців на етапі експлуатації.

На основі проведеного дослідження наявних систем та виявлених проблем нами пропонується розробка системи виявлення атак, особливістю якої буде інтеграція з комунікаційним обладнанням на апаратному рівні. Підвищення швидкодії буде досягнуто за рахунок використання одного з двох підходів. Перший підхід полягає у поєднанні аналізу трафіку з засобами, інтегрованими у високошвидкісні комутатори, та одночасне використання сенсорів, орієнтованих на певні програмні продукти та особливості операційних систем [14].

Другим підходом для підвищення швидкодії систем виявлення атак є апаратна реалізація алгоритмів виявлення атак на основі сигнатур та їх інтеграція в комунікаційне обладнання. Основною особливістю є використання на кожному з портів комутатора сенсора системи виявлення атак на основі сигнатурного методу, в прозорому для користувача режимі. Для досягнення значного підвищення швидкодії сигнатури розміщуються в пам'яті системи виявлення атак комутатора і централізовано поновлюються. Сенсори об'єднані між собою додатковою високошвидкісною шиною передачі даних, при чому шина повністю ізольована від портів комутатора, тобто факт існування системи не можливо виявити, аналізуючи мережеві пакети. Для об'єднання сенсорів різних комутаторів використовується додатковий комунікаційний порт. Вартість обладнання не надто зросте, враховуючи невелику додаткову вартість при запровадженні даного рішення.

Паралельно з вдосконаленням існуючих методів, заслуговує уваги використання нейронних мереж для розробки систем виявлення атак та аналізу трафіку для автоматичного написання сигнатур атак [15].

Список літератури

1. *Cisco* Intrusion Detection System. http://www.cisco.com/en/US/products/hw/modules/ps2706/ps5058/index.html

2. *The Profound* Benefits of Network-Based Intrusion Prevention. http://www.preferredtechnology.com/support/whitepapers/download/The_Power_of_NBIPS.pdf

3. *Cisco* Intrusion Prevention System Solution. http://www.cisco.com/en/US/ /products/hw/vpndevc/ps4077/products_data_sheet0900aecd801eeea5.html

4. *Proventia* ESP Brochure. http://documents.iss.net/literature/proventia/Proventia_ESP_Brochure.pdf

5. *Proventia* Intergrated Security Appliance. http://documents.iss.net/literature/ proventia/ProventiaM50andM30_Datasheet.pdf

6. *Proventia* Intrusion Detection Appliances. http://www.iss.net/ products_services/enterprise_protection/proventia/a_series.pdf

7. *Intrusion* Prevention System, TrippingPoint Security Solutions. http://www.tippingpoint.com/solutions_enterprise.html

8. *TrippingPoint* Threat Suppression Engine. http://www.tippingpoint.com/technology_tse.html
9. *TippingPoint* Intrusion Prevention Systems http://www.tippingpoint.com/pdf/resources/datasheets/400917-002_TP-IPS.pdf
10. *Sourcefire* Intrusion Agent for Snort http://www.sourcefire.com/products/is_agent.html
11. *Sourcefire* IS5800 – A Revolutionary Approach to Enterprise Inrtusion Prevention http://www.sourcefire.com/products/is5800.html
12. *The Snort* Project, "Snort, Users Manual 2.4.0RC1" http://cvs.snort.org/viewcvs.cgi/snort/doc/ snort_manual.pdf/rev=1.31.2.3.2.4
13. *Snort* 2.0 Hi-performance Multi-rule Inspection Engine. Sourcefire, 2004.
14. *Raven Alder*, Jacob Babbin, Adam Doxtater. Snort 2.1. Second Edition Syngress Publishing, 2004.
15. *Лукацкий А.В.* Обнаружение атак. -БХВ-Петербург, 2001. -С.144-149.

Надійшла 19.09.2006

УДК 004.681 **Кулагин Е.А.**

ОЦЕНКА СТОЙКОСТИ СКРЫТЫХ КАНАЛОВ В ПРОВОДНЫХ ТЕЛЕФОННЫХ ЛИНИЯХ ПРОТИВ ПАССИВНЫХ АТАК

Введение

В условиях информационного противоборства большое значение приобретают проблемы сохранения секретности и имитостойкости информации. Одними из наиболее распространенных во многих странах сред передачи информации являются телефонные сети, абонентский участок которых представляет собой проводные линии, по которым передаются сигналы аналогового канала тональной частоты (ТЧ).

При обеспечении секретности связи по аналоговым каналам ТЧ чаще всего используются различные методы скремблирования речи. Несмотря на то, что современные методы скремблирования позволяют обеспечить высокую криптостойкость сообщений [1], у них есть один существенный недостаток. Факт передачи скремблированного сообщения может привлечь внимание противника и в случае невозможности раскрыть содержимое сообщений он может применить активные атаки по их уничтожению. Сокрытие факта передачи сообщения позволит существенно повысить секретность передаваемой информации за счет того, что противник не знает против какого, из большого множества каналов, он должен применять вычислительно емкие атаки.

Обеспечение имитостойкости речевых сигналов при современных методах синтеза речи так же является актуальной задачей. Обмен парольными фразами является малоэффективной защитой, так как параллельно требуется иметь секретную систему передачи паролей. Одним из наиболее эффективных решений этой проблемы является встраивание в сообщение цифровых водяных знаков.

Задачи обеспечения скрытности передаваемого сообщения и обеспечения имитостойкости телефонного канала можно решить методами стеганографии, путем встраивания в открытый телефонный канал скрытного канала передачи секретных сообщений либо передачи меток идентификации.

Теоретическая возможность создания таких скрытых каналов основывается на нечувствительности человеческого слуха к незначительным изменениям параметров