УДК 004.056.53 **С.В. Лазаренко**

ОСОБЛИВОСТІ ФУНКЦІОНУВАННЯ СИСТЕМ ВИЯВЛЕННЯ АТАК НА АВТОМАТИЗОВАНІ СИСТЕМИ

Проаналізована актуальність використання систем виявлення атак на автоматизовані системи. Визначені методи виявлення атак, які використовуються в сучасних системах Intrusion Detection System(IDS). Надана класифікація та архітектура сучасних систем виявлення атак. Наведена схема функціонування distributed IDS(dIDS). Проведено аналіз можливостей, як переваг так і недоліків, сучасних засобів виявлення атак.

Ключові слова: системи виявлення атак, системи IDS, dIDS, архітектура систем виявлення атак.

1. Введення.

Виявлення атак - це процес ідентифікації і реагування на підозрілу діяльність, спрямовану на обчислювальні чи мережні ресурси.

У свою чергу атака - це будь-яка дія порушника, що приводить до реалізації погрози шляхом використання вразливостей автоматизованої системи.

Повідомлення про проникнення в корпоративні мережі і атаки на Web-сервера останнім часом з'являються усе частіше. Зі збільшенням кваліфікації зловмисники стають більш винахідливими в розробці і застосуванні методів проникнення за захисну перешкоду. Знайти таких зловмисників дуже важко. Вони маскуються під авторизованих користувачів, використовують проміжні вузли для приховування своєї істинної адреси, здійснюють атаки розподілені в часі (протягом декількох годин) і просторі (одночасно з декількох вузлів) і т.ін. Багато атак здійснюються за дуже короткий час (хвилини і навіть секунди), що також не дозволяє знайти і запобігти їм стандартними захисними засобами.

Пов’язано це з тим, що більшість комп'ютерних захисних систем побудовано на класичних моделях розмежування доступу, розроблених у 70-х, 80-х роках. Згідно з цими моделями, суб'єкту (користувачу або програмі) на основі заданих правил дозволяється чи забороняється доступ до якого-небудь об'єкта (наприклад, файлу). Однак дії, суб'єкта над об'єктом, ніяк не регламентується, і в такому разі неможливо, наприклад, запобігти копіювання файлу користувачем, якому доступ до даного файлу дозволений. Розвиток цих моделей дозволив усунути ці недоліки шляхом контролю конфіденційності (модель Белла-Лападула) чи цілісності (модель Біба) інформаційних потоків. Однак виникає закономірне протиріччя між зручністю використання системи і рівнем забезпечуваної нею безпеки. Приходиться чимось жертвувати. Або зручністю використання системи, що захищається, або рівнем її захищеності.

Крім того, моделі управління доступом не можуть допомогти у випадку реалізації атак від авторизованих користувачів чи процесів (програм), що пройшли процедуру автентифікації. Якщо зловмисник підібрав чи перехопив пароль, то ніяка система розмежування доступом не допоможе запобігти крадіжці чи підміну інформації, що доступна для скомпрометованого користувача.

Недостатня ефективність таких традиційних механізмів захисту, як розмежування доступу, автентификация, фільтрація й ін., обумовлена тим, що при їхньому створенні не враховані багато аспектів, пов'язаних із сучасними атаками.

Однією з технологій, що може бути застосована для виявлення порушень, що не можуть бути ідентифіковані за допомогою моделей контролю доступу і є *технологія виявлення атак*.

2. Класифікація систем виявлення атак.

Механізми виявлення атак, застосовувані в сучасних системах виявлення атак IDS (IntrusionDetectionSystem), засновані на декількох загальних методах. Слід зазначити, що ці методи не є взаємовиключними. У багатьох системах використається комбінація декількох методів.

Класифікація систем виявлення атак може бути виконана по декількох ознаках:

- по способу реагування;
- по способу виявлення атаки;
- по способу збору інформації про атаку.

По способу реагування розрізняють пасивні й активні IDS. Пасивні IDS просто фіксують факт атаки, записують дані у файл журналу та видають попередження. Активні IDS намагаються протидіяти атаці, наприклад, шляхом реконфігурації міжмережевого екрану або генерації списків доступу маршрутизатора.

По способу виявлення атаки системи IDS прийнято ділити на дві категорії:

- виявлення аномального поводження (anomaly-based);
- виявленнязловживань (misuse detection або signature-based).

Технологія виявлення атак шляхом ідентифікації аномального поводження заснована на наступній гіпотезі. Аномальне поводження користувача (тобто атака або яка-небудь ворожа дія) проявляється як відхилення від нормального поводження. Прикладом аномального поводження може служити велика кількість з'єднань за короткий проміжок часу, високе завантаження центрального процесора й т.п.

Якщо можливо було б однозначно описати профіль нормального поводження користувача, то будь-яке відхилення від нього можна ідентифікувати як аномальне поводження. Однак аномальне поводження не завжди є атакою. Наприклад, одночасну посилку великої кількості запитів від адміністратора мережі система виявлення атак може ідентифікувати як атаку типу «відмова в обслуговуванні» (denial of service).

При використанні системи з такою технологією можливі два випадки:

- виявлення аномального поводження, що не є атакою, і віднесення його до класу атак;
- пропуск атаки, що не підпадає під визначення аномального поводження. Цей випадок більше небезпечний, чим помилкове віднесення аномального поводження до класу атак.

При настройці та експлуатації систем цієї категорії адміністратори зіштовхуються з наступними проблемами:

- побудова профілю користувача є важко формализованим і трудомістким завданням, що вимагає від адміністратора великої попередньої роботи;
- визначення граничних значень характеристик поводження користувача для зниження ймовірності появи одного із двох вищезгаданих крайніх випадків.

Технологія виявлення аномалій орієнтована на виявлення нових типів атак. Однак недолік її - необхідність постійного навчання. На поточний момент технологія виявлення аномалій не одержала широкого поширення, і в жодній комерційно-розповсюджувальній системі вона не використається. Пов’язано це з тим, що дана технологія важко реалізується на практиці.

Суть іншого підходу до виявлення атак - виявлення зловживань - полягає в описі атаки у вигляді сигнатури (signature) і пошуку даної сигнатури в контрольованому просторі (мережному трафике або журналі реєстрації). Як сигнатура атаки може виступати шаблон дій або рядок символів, що характеризують аномальну діяльність. Ці сигнатури зберігаються в базі даних, аналогічної тієї, котра використається в антивірусних системах. Варто помітити, що антивірусні резидентні монітори є часткою случаємо системи виявлення атак, але оскільки ці напрямки споконвічно розвивалися паралельно, те прийнято розділяти їх. Тому дана технологія виявлення атак дуже схожа на технологію виявлення вірусів, при цьому система може виявити всі відомі атаки. Однак системи даного типу не можуть виявляти нові, ще невідомі види атак.

Підхід, реалізований у таких системах, досить простий, і саме на ньому засновані практично всі запропоновані сьогодні на ринку системи виявлення атак. Однак при експлуатації й цих систем адміністратори зіштовхуються із проблемами. Перша проблема

полягає у створенні механізму опису сигнатур, тобто мови опису атак. Друга проблема полягає в тому, як описати атаку, щоб зафіксувати всі можливі її модифікації.

Слід зазначити, що перша проблема вже частково вирішена в деяких продуктах. Наприклад, компанією Internet Security Systems, Inc. реалізовано систему опису мережних атак Advanced Packets Exchange, і з її допомогою розроблена система аналізу захищеності Internet Scanner.

На сьогодні найбільш популярною є класифікація по способу збору інформації про атаку, а саме:

- виявлення атак на рівні мережі (network-based);
- виявлення атак на рівні хоста (host-based);
- виявлення атак на рівні додатка (application-based).

Система першого типу (network-based) працює по типу сниффера, «прослуховуючи» трафік у мережі й визначаючи можливі дії зловмисників. Пошук атаки йде за принципом «від хоста до хоста». Системи, що входять у перший клас, аналізують мережний трафік, використовуючи, як правило, сигнатури атак й аналіз «на льоту». Метод аналізу «на льоту» полягає в моніторингу мережного трафіка в реальному або близькому до реального часу й використанні відповідних алгоритмів виявлення. Найчастіше використовується механізм пошуку в трафіку певних рядків, які можуть охарактеризувати несанкціоновану діяльність. До таких рядків можливо віднести '\\winnt\system32\config' (даний рядок описує шлях до файлів SAM, Security і т.д.) або 7 etc/pas swd' (даний рядок описує шлях до списку паролів ОС UNIX).

Системи другого типу (host-based) призначена для моніторингу, детектування та реагування на дії зловмисників на певному хості. Система перевіряє й виявляє спрямовані проти хоста дії. Ці системи аналізують реєстраційні журнали операційної системи або додатка. Аналіз журналів реєстрації є одним з найперших реалізованих методів виявлення атак. Він полягає в аналізі журналів реєстрації (log, audit trail), створюваних операційною системою, прикладним програмним забезпеченням, маршрутизаторами й т.д. Запис у журналі реєстрації аналізуються й інтерпретуються системою виявлення атак. До переваг цього методу можливо віднести простоту його реалізації.

Однак за цією простотою приховано ряд недоліків:

- для достовірного виявлення тієї або іншої підозрілої діяльності необхідна реєстрація в журналах великого обсягу даних, що негативно позначається на швидкості роботи контрольованої системи;
- при аналізі журналів реєстрації дуже важко обійтися без допомоги фахівців, що істотно знижує коло поширення цього методу;
- до дійсного моменту немає уніфікованого формату зберігання журналів;
- аналіз записів у журналах реєстрації здійснюється не в реальному режимі часу, тому цей метод не може бути застосований для раннього виявлення атак у процесі їхнього розвитку.

Очевидним недоліком є те, що системи рівня хоста не можуть виявити атаки, які спрямовані на вузли, що не використовують журнали реєстрації або для яких не існує відповідної реалізації агента.

Як правило, аналіз журналів реєстрації є доповненням до інших методів виявлення атак, зокрема до виявлення атак «на льоту». Використання цього методу дозволяє проводити «розбір польотів» вже після того, як була зафіксована атака, для того щоб виробити ефективні заходи запобігання аналогічних атак у майбутньому.

Третій тип IDS (application-based) заснований на пошуку проблем у певному додатку.

Кожний із цих трьох типів систем виявлення атак (на рівні мережі, на рівні хоста й на рівні додатка) має свої переваги та недоліки. Необхідно відмітити, що лише деякі системи виявлення атак можуть бути однозначно віднесені до одного з названих класів. Гібридні IDS, що представляють собою комбінацію різних типів систем, як правило, містять у собі

можливості декількох категорій.

3. Архітектура системи виявлення атак.

На основі аналізу існуючих рішень можливо привести перелік компонентів, з яких складається типова система виявлення атак.

Модуль спостереження. Цей модуль забезпечує збір даних з контрольованого простору (журналу реєстрації або мережного трафіку). Різні виробники дають цьому модулю наступні назви: сенсор (sensor), монітор (monitor), зонд (probe) і т.д.

Залежно від архітектури системи виявлення атак модуль спостереження може бути фізично роз'єднаний від інших компонентів, тобто перебувати на іншому комп'ютері.

Підсистема виявлення атак. Дана підсистема є основним модулем системи виявлення атак. Вона здійснює аналіз інформації, яка одержуэться від модуля спостереження. За результатами цього аналізу дана підсистема може ідентифікувати атаки, приймати рішення щодо варіантів реагування, зберігати відомості про атаку в сховище даних і т.д.

База знань. Залежно від методів, що використовуються в системі виявлення атак, база знань може містити профілі користувачів й обчислювальної системи, сигнатури атак або підозрілі рядки, що характеризують несанкціоновану діяльність. База знань може поповнюватися виробником системи виявлення атак, користувачем системи або третьою стороною, наприклад аутсорсинговою компанією, що здійснює підтримку цієї системи.

Сховище даних. Забезпечує зберігання даних, зібраних у процесі функціонування системи виявлення атак.

Графічний інтерфейс. Навіть дуже потужний й ефективний засіб не буде використовуватись, якщо в нього відсутній «дружній» інтерфейс. Залежно від операційної системи, під управлінням якої функціонує система виявлення атак, графічний інтерфейс повинен відповідати стандартам де-факто для Windows й UNIX.

Підсистема реагування. Ця підсистема здійснює реагування на виявлені атаки й інші контрольовані події.

Підсистема управління компонентами. Дана підсистема призначена для управління різними компонентами системи виявлення атак. Під терміном «управління» розуміється можливість зміни політики безпеки для різних компонентів системи виявлення атак (наприклад, модулів спостереження), а також одержання інформації від цих компонентів (наприклад, відомостей про зареєстровану атаку). Управління може здійснюватися за допомогою як внутрішніх протоколів та інтерфейсів, так і вже розроблених стандартів, наприклад SNMP.

Системи виявлення атак будуються на основі двох архітектур: «автономний агент» та «агент-менеджер». У першому випадку на кожний вузел що захищається, або сегмент мережі встановлюються агенти системи, які не здатні обмінюватися інформацією між собою, а також не можуть керуватися централізовано з єдиної консолі. Цих недоліків позбавлена архітектура «агент-менеджер». У цьому випадку в розподіленій системі виявлення атак dIDS (distributed IDS), що складається з безлічі IDS, розташованих у різних ділянках великої мережі, сервери збору даних і центральний сервер, що аналізує, здійснюють централізований збір й аналіз зареестрованних даних, Управління модулями dIDS здійснюється із центральної консолі управління. Для великих організацій, у яких філії рознесені по різних територіях і навіть містах, використання такої архітектури має принципове значення.

Загальна схема функціонування dIDS наведена на Рис. 1.

Така система дозволяє підсилити захищеність корпоративної подсетизавдяки централізації інформації про атаку від різних IDS. Розподілена система виявлення атак dIDS складається з наступних підсистем: консоль управління, що аналізують сервери, агенти мережі, сервер збору інформації про атаку. Центральний сервер, що аналізує, звичайно складається з бази даних й Web-сервера, що дозволяє зберігати інформацію про атаки й

маніпулювати даними за допомогою зручного Web-інтерфейсу. Агент мережі - один з найбільш важливих компонентів dIDS. Він являє собою невелику програму, ціль якої - повідомляти про атаку на центральний сервер, що аналізує.

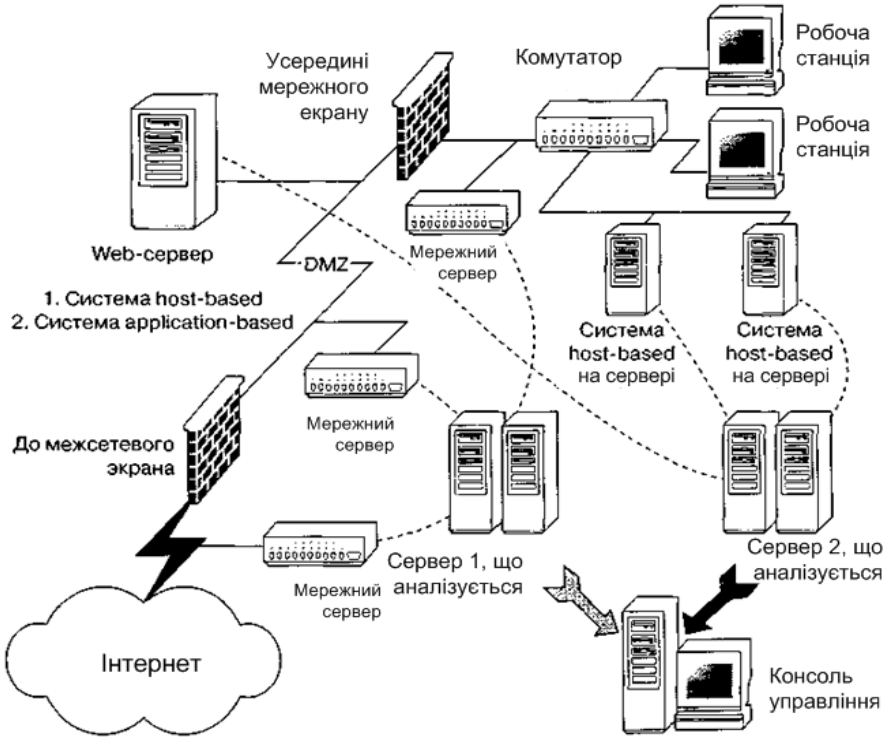

Рис. 1. Загальна схема функціонування розподіленої IDS

Сервер збору інформації про атаку - частина системи dIDS, що логічно базується на центральному сервері, що аналізує. Сервер визначає параметри, по яких групуються дані, отримані від агентів мережі. Угруповання даних може здійснюватися по наступних параметрах:

- IP-адреса атакуючі;
- порт одержувача;
- номер агента;
- дата, час;
- протокол;
- тип атаки й т.д.

Незважаючи на деякі сумніви в ефективності застосування IDS користувачі вже широко застосовують як вільно розповсюджувані, так і комерційні засоби IDS.

4. Застосування засобів виявлення атак.

У наш час на розвиток і захищеність мереж значною мірою впливає ряд факторів:

- об'єднання локальних мереж підрозділів у єдину корпоративну мережу організації;
- підключення корпоративної мережі організації до глобальної мережі Інтернет;
- підключення до корпоративної мережі організації зовнішніх користувачів (клієнтів, постачальників продукції й ін.);
- різке збільшення швидкостей передачі й обсягів переданої інформації;
- використання в корпоративній мережі різноманітного програмного та апаратного

забезпечення.

Дія цих факторів приводить до розширення границь мережі, росту кількості людей, що мають доступ до корпоративної мережі підприємства, підвищенню складності мереж та істотному ускладненню управління ними. Це, у свою чергу, приводить до збільшення потенційних можливостей для реалізації загроз безпеки інформації.

Для більшості організацій захист мережних ресурсів від несанкціонованого доступу стає однієї з найбільш гострих проблем, від рішення якої залежить як життєздатність підприємства, так і його подальший розвиток. Перед підрозділами, що забезпечують інформаційну безпеку організацій, ставиться завдання забезпечити ефективний захист мережних ресурсів у мережному середовищі.

Ефективний захист складається не тільки із застосування традиційних механізмів забезпечення безпеки (криптографії, автентифікації, контролю доступу й т.д.), а й додаткових заходів. Наприклад, модель адаптивного управління безпекою мережі ANS (Adaptive Network Security) дозволяє контролювати й постійно виявляти загрози, що змінюються, та ризики для безпеки інформації, реагувати на них у режимі реального часу, використовуючи правильно спроектовані й добре керовані процеси та засоби захисту. Адаптивне управління безпекою мережі являє собою процес, що використовує технологію аналізу захищеності, технологію виявлення атак, адаптивні і керуючі компоненти.

Очевидно, що одна система не в змозі ефективно реалізувати весь комплекс таких технологій. Тому для реалізації концепції адаптивної безпеки необхідно використовувати сукупність систем, об'єднаних загальним задумом. На ринку представлено кілька десятків комерційних систем IDS, що забезпечують вибір прийнятного рішення. На сьогодні закінчені рішення пропонують компанії Internet Security Systems, Cisco Systems і деякі інші.

Наведемо приклади реалізацій технологій управління безпекою мережі (продукти зазначених компаній).

Продукти компанії Internet Security Systems

Компанія ISS займає провідні позиції в частині реалізації систем виявлення атак. Вона пропонує ціле сімейство рішень для різних рівнів.

RealSecure Network Sensor - програмне рішення, призначене для встановлення на виділений комп'ютер у критичному сегменті мережі. Аналізуючи мережевий трафік і зіставляючи його з базою сигнатур атак, сенсор виявляє різні порушення політики безпеки.

Система *RealSecure Gigabit Sensor* обробляє більше 500 тис. пакетів у секунду, використовуючи запатентований алгоритм семирівневого аналізу, виявляє велику кількість атак, що можуть бути пропущені іншими системами. Застосовується головним чином у мережах, що працюють з великим навантаженням.

RealSecure Server Sensor дозволяє виявляти атаки, спрямовані на конкретний вузол мережі, на всіх рівнях. Крім виявлення атак RealSecure Server Sensor має можливість проведення аналізу захищеності й виявлення уразливостей на контрольованому вузлі.

Система виявлення атак *RealSecure Desktop Protector* (раніше називалася BlacklCE Agent) є програмним рішенням, призначеним для виявлення в реальному масштабі часу мережних атак, спрямованих на робочі станції корпоративної мережі.

RealSecure for Nokia - це програмно-апаратне рішення, розроблене компаніями Internet Security Systems та Nokia. Воно поєднує в собі всі функціональні можливості мережевого сенсора RealSecure Network Sensor і Nokia IP Network Security Solutions. Система RealSecure for Nokia функціонує під управлінням захищеної операційної системи IPSO, що базується на ОС FreeBSD.

Система *RealSecure Guard* є програмним рішенням, що сполучує в собі можливості міжмережевого екрану та системи виявлення атак у режимі реального часу. Система RealSecure Guard встановлюється між мережею, що захищається, і відкритими сегментами мережі (так названа inline-IDS) та аналізує весь трафік, що через неї минає, у пошуках

заборонених або небезпечних пакетів. Система RealSecure Guard може виявляти атаки як на сегмент мережі (Fast Ethernet), так і на окремі, найбільш важливі вузли.

Для управління перерахованими системами RealSecure використовується модуль RealSecure SiteProtector, який є основним компонентом централізованого управління як для систем Internet Scanner, так і для System Scanner. Дана система орієнтована на застосування у великих, територіально-розподілених мережах або в організаціях, що використовують одночасно кілька рішень компанії ISS.

БільшепростийдляуправліннямодульRealSecure WorkGroup Manager призначенийтільки RealSecure Network Sensor, Gigabit Sensor, RealSecure Server Sensor та RealSecure for Nokia. Даний модуль управління орієнтований на застосування в компаніях, де відсутні інші рішення компанії ISS та в мережі встановлено невелика кількість сенсорів (до п'яти).

RealSecure Command Line Interface призначений для управління з командного рядка тільки RealSecure Network Sensor й Gigabit Sensor. Цей модуль управління орієнтований на локальне використання. Модуль RealSecure Sensor Manager являє собою графічну надбудову над інтерфейсом командного рядка.

Продукти компанії Cisco Systems

Компанією Cisco Systems здійснюється випуск серії продуктів Cisco IDS, що містять рішення для різних рівнів. До неї входять три системи 42xx версії 2.2.1 (network-based), серед яких:

- Cisco IDS 4210 v.2.2.1 оптимізована для моніторингу атак у середовищі 10/100BASE-T, швидкість 45 Мб/з (network-based);
- Cisco IDS 4235 v.2.2.1 оптимізована для моніторингу атак у середовищі 10/100/1000BASE-TX, швидкість 200 Мб/з (network-based);
- Cisco IDS 4250 v.2.2.1 оптимізованадля моніторингу атак у середовищі 10/100/1000BASE-TX, швидкість 500 Мб/з, може бути використана для захисту гігабітної мережі (network-based).

Укомутаторі Catalyst єпідсистема IDS - Catalyst 6000 Intrusion Detection System Module (swithed-integrated network-based).

Cisco IDS Host Sensor 2.0 й Cisco IDS Host Sensor Web Server, розробленікомпанією Entercept, забезпечуютьзахистнарівніхоста (host-based).

IDS нарівнімаршрутизатора (Firewall Feature Set 12.1(4)T) здатнавідбивати 59 найнебезпечнішихвидіватак (система network-based).

Привикористанні IDS нарівнімежмережевогоекрану PIX 535, 525, 515E, 506E, 501 (v.6.2.2) відбиваєтьсябільше 55 найнебезпечнішихвидіватак (система network-based).

Управління системами захисту здійснюється за допомогою CiscoWorks VPN/ Security Management Solution (VMS) або Cisco IDS software version 3.1(2).

Кориснісистемийпродукти IDS випускаютьтакожіншікомпанії, зокрема Symantec, Enterasys Networks, Computer Associates, NFR Security, Intrusion Inc., OneSecure, Recourse Technologies йін.

Такимчиномтехнологіївиявленняатакдозволяютьвирішитицілийрядзадач, якіпідвищуютьзахищеністьвузлівкорпоративноїмережітазахистінформації.

Разом з тим, на сьогоднішньому етапі розвитку інформаційних технологій вони не дозволяють:

- компенсувати неефективність механізмів автентифікації та ідентифікації;
- проводити всебічний аналіз атак без людської участі (вони тільки допомагають в цьому);
- усунути слабості мережевих протоколів;
- усунути проблеми в надійності і цілісності інформаційних систем;
- ефективно аналізувати весь трафік у високошвидкісних мережах.

Не зважаючи на виявлені недоліки використання систем виявлення атак є ефективним засобом захисту автоматизованих систем та захисту інформації.

5. Висновки.

Технології виявлення атак дозволяють вирішити цілий ряд задач, які підвищують захищеність вузлів корпоративної мережі та захист інформації, а саме:

1. Моніторинг і аналіз користувацької, мережної та системної активності.
2. Аудит системної конфігурації та виявлення вразливостей.
3. Контроль цілісності файлів та інших ресурсів корпоративної мережі.
4. Розпізнавання шаблонів дій, що відображають відомі атаки.
5. Статистичний аналіз шаблонів аномальних дій.
6. Автоматичну інсталяцію відновлень ПЗ, що поставляється виробником.
7. Інсталяцію та підтримку роботи серверів-пасток для запису інформації про порушників.

Література

1. Лукацкий А.В. Обнаружение атак / Лукацкий А.В. – СПб.: БХВ-Петербург, 2003. – 624 с.

2. Лукацкий А.В. Предотвращение сетевых атак: технологии и решения / А.В.Лукацкий. – СПб.: Экспресс Электроника, 2006. – 268 с.

3. Юдін О.К. Захист інформації в мережах передачі даних / О.К.Юдін, Г.Ф. Конахович, О.Г. Корченко // Підручник МОН України. – К.: Видавництво *DIRECTLINE*, 2009.-714с.

4. Пауэр Р. Эксперты дискутируют о настоящем и будущем систем обнаружения атак/ [Р. Пауэр и др.] под ред. ПауэраР.; пер. сангл. - Computer Security Journal vol. XIV, №1, http://www.citforum.ru/security/internet/attack.shtml

5. Леннон Э. Компьютерные атаки: что это такое и как защититься от них / [Леннон Э. и др.] под ред. Э. Леннона; пер.с англ. - Бюллетень лаборатории информационных технологий NIST за май 1999 г., http://www.citforum.ru/security-/internet/secatt.shtml

6. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. пособие./ А.А. Малюк.– М.: Горячая линия – Телеком, 2004. – 280 с.

7. Городецький В.І. Багатоагентні технології комплексного захисту інформації в телекомунікаційних системах/ [В.І Городецький та інш.] під ред. В.І Городецького. ISINAS - 2000. Праці. - СПб. 2000.

Надійшла 15.02.2015 р. Рецензент: д.т.н., проф. Дудикевич В. Б.