УДК 004.681

Завада А.А., Охрімчук В.В.

СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ: СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ

В статті проведений аналіз основних механізмів реалізації атак на ресурси інформаційно-телекомунікаційних систем та механізмів їх виявлення. Визначені переваги та недоліки основних типів систем виявлення та запобігання вторгненням. Для порівняльного аналізу зазначених систем запропоновано перелік показників. Визначені властивості, котрі повинна мати сучасна система виявлення та запобігання вторгненням.

Ключові слова: система виявлення та запобігання вторгненням, атака, інформаційно-телекомунікаційна система, захист інформаційних ресурсів.

Вступ. Події, які відбуваються у світовому суспільстві наочно демонструють, що останнім часом критично важливим державним ресурсом, який забезпечує безпеку країни, стає інформація, яка циркулює в інформаційно-телекомунікаційних системах (ІТС) різного, у тому числі військового призначення. Зазначені системи є невід'ємною компонентою структури управління державою, економікою, фінансами та обороною. Можливість несанкціонованого впливу на них розглядається як пряма загроза національним інтересам країни.

Останнім часом у світі, зокрема і в Україні, спостерігаються процеси збільшення активності невладних Інтернет спілок, які певним чином намагаються впливати на політичні, законодавчі та економічні рішення керівництва країни. При цьому кіберпростір виступає в якості ефективного інструменту досягнення мети зловмисниками. Яскравим прикладом цього є січневі події 2012 року, які пов'язані із блокуванням доступу до інформаційних ресурсів офіційних сайтів державних органів влади незалежною інтернаціональною групою хакерів «Anonymous», що стало відповіддю на припинення роботи файлообмінника EX.ua силовими підрозділами держави. Слід зазначити, що атаки на ІТС з кожним роком стають все більш витонченими, масштабнішими та інтенсивнішими. Враховуючи вищезазначене, актуальною є проблема розробки та удосконалення систем виявлення вторгнень в ІТС, головною задачею яких є саме виявлення мережних атак чи спроб несанкціонованого використання ресурсів мережі.

Постановка проблеми. Одним з широко застосовуваних способів захисту локальних мереж від зовнішніх атак є використання міжмережних екранів (ММЕ). Однак в сучасних умовах застосування ММЕ дозволяє забезпечити лише необхідний, але явно недостатній рівень захищеності інформаційних ресурсів.

Одним з варіантів ефективного захисту ІТС є використання систем виявлення і запобігання вторгненням [1, 2]. Системи виявлення вторгнення (intrusion-detection system, IDS) можуть сповістити про початок атаки на мережу, причому деякі з них здатні виявляти раніше невідомі атаки. Системи запобігання вторгненням (intrusion-prevention systems, IPS) не обмежуються лише оповіщенням, але і здійснюють різні заходи, спрямовані на блокування атаки (наприклад, розрив з'єднання або виконання скрипта, заданого адміністратором). Враховуючи переваги та недоліки обох типів систем [3, 4], вибір між IDS та IPS не є однозначним. На практиці досить часто програмно-апаратні рішення поєднують в собі функціональність двох типів систем, їх об'єднання іноді називають IDPS (IDS і IPS). Враховуючи вищезазначене та обмеженість обсягу статті, далі мова буде вестись переважно саме про системи IDPS. Насиченість ринку інформаційних технологій зазначеними системами ставить перед користувачем нагальну потребу вибору оптимальної системи виявлення вторгнень, але такий вибір може бути здійснений лише на основі аналізу сучасного стану та перспектив їх найближчого розвитку.

Виклад основного матеріалу. З метою визначення сучасного стану та перспектив розвитку IDPS спочатку визначимось з такими категоріями як атака, класифікація та механізми реалізації і виявлення атак.

Виявлення атаки – це процес ідентифікації та реагування на підозрілу діяльність, яка направлена на обчислювальні чи мережні ресурси [1], при цьому під атакою розуміють будь-яку дію зловмисника, що призводить до реалізації загрози шляхом використання уразливостей обчислювальної системи [2, 3].

Існують різні методи класифікації атак. Наприклад, їх поділяють на пасивні та активні, зовнішні й внутрішні, навмисні й ненавмисні атаки. Характерний перелік типів атак на ІТС можна подати як [3, 4]: віддалене проникнення (remote penetration); локальне проникнення (local penetration); віддалена відмова в обслуговуванні (remote denial of service); локальна відмова в обслуговуванні (local denial of service); мережні сканери (network scanners); сканери уразливостей (vulnerability scanners); зломщики паролів (password crackers); аналізатори протоколів (sniffers).

Компанія Internet Security Systems, Inc., наприклад, пропонує такий перелік категорій можливих атак на ІТС [4]: збір інформації про характеристики ІТС (information gathering); спроби несанкціонованого доступу до інформаційних ресурсів системи (unauthorized access attempts); відмова в обслуговуванні (denial of service {DoS}); підозріла активність (suspicious activity); системні атаки (system attack).

Якщо знати характерні ознаки несанкціонованих дій (механізми реалізації атак), а саме: присутність повтору певних подій у системі; неправильні або невідповідні встановленим процесам поточні ситуації та команди; використання уразливостей; невідповідні параметри мережного трафіку; непередбачені атрибути; непояснені проблеми; додаткові знання про порушення, то можна виявити або знизити ризики від реалізації атак. У табл. 1 наведені основні механізми реалізації для різних типів атак [5].

Основні механізми реалізації атак Таблиця 1

№ з/п	Тип атаки	Механізм реалізації атаки
1	Віддалене виконання коду	Віддалений виклик командної строки шляхом переповнення буфера
2	Аналіз топології мережі	Передача мережних пакетів, що містять запити ECHO_REQUEST
3	Пошук уразливості	Сканування хосту
4	Відмова в обслуговуванні	Передача великої кількості мережних пакетів
5	Злам паролів	Багатократні спроби аутентифікації в системі
6	Аналіз мережного трафіку	Перемикання мережного інтерфейсу в «режим прослуховування» і перехоплення мережного трафіку
7	Шкідливі програми	Приховане встановлення програмних модулів, прихований запуск процесів

На практиці використовуються різні комбінації атак. Наприклад, зловмисник використовує мережні сканери для виявлення топології мережі, потім сканери уразливостей для визначення уразливих хостів. Знайдені на хості уразливості можуть використовуватись зловмисником для віддаленого виконання коду. Таким чином, в IDS повинні бути реалізовані механізми виявлення різних типів атак. Основні механізми виявлення атак, визначені для різних механізмів атак, наведені в табл. 2 [5].

Стандартні засоби захисту інформаційних ресурсів системи (ММЕ, сервери аутентифікації, системи розмежування доступу тощо) використовують у своїй роботі одну або дві ознаки, у той час як спеціалізовані системи виявлення атак, впроваджують для ідентифікації несанкціонованих дій практично весь зазначений перелік (див. табл. 1).

Вперше ідея створення системи виявлення вторгнень з'явилася в 1980-х роках. У кінці 1990-х років почалися активні розробки в цій галузі. Наприклад, у 1998 р. стартували такі відомі нині проекти, як Snort і Prelude [2]. Пізніше, з ряду причин розробники почали реалізовувати багаторівневі системи захисту [2, 6]. Ніні існує величезна кількість систем, які позиціонуються, як IDS, IPS або IDPS, при цьому вони досить різноманітні як за принципами роботи, так і за використовуваними технологіями [6, 7].

Основні механізми виявлення атак Таблиця 2

№ з/п	Механізми виявлення атаки	Механізм реалізації атаки
1	Відстеження спроб аутентифікації в системі	Багатократні спроби аутентифікації в системі
2	Відстеження перехоплення мережного трафіку	Перемикання мережного інтерфейсу в «режим прослуховування» і перехоплення мережного трафіку
3	Відстеження мережного трафіку	Передача мережних пакетів, що містять запити ECHO_REQUEST Сканування хосту Передача великої кількості мережних пакетів
4	Відстеження запуску процесів та звернень до файлової системи й реєстру	Прихований запуск процесів Віддалений виклик командного рядку шляхом переповнення буфера Приховане встановлення програмних модулів

Система IDPS дозволяє виявляти (блокувати) спроби зламу зловмисником ІТС (ресурсу) та сповіщає про це користувача. IDPS являє собою гібрид сніффера (модуля перехоплення трафіка, що працює в мережі, й використовується для збору інформації, яка в подальшому може бути використана як для діагностики, так і для взлому мережі), аналізатора та системи сповіщення (блокування). На рис. 1 показана загальна схема розміщення системи IDPS у комп'ютерній мережі.

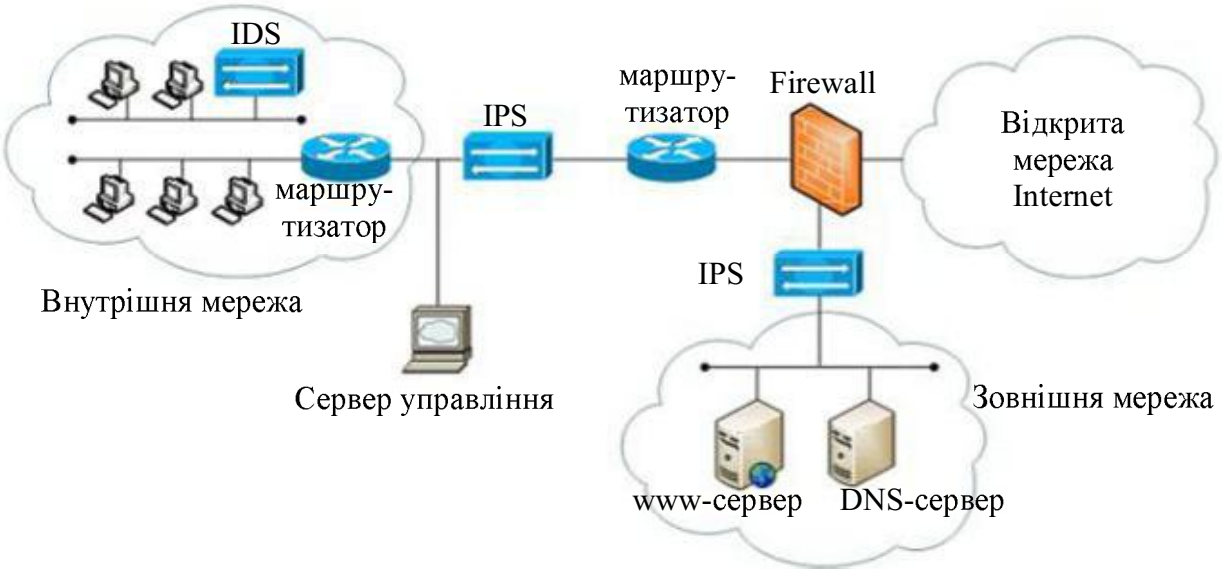

Рис. 1. Схема розміщення IDPS у комп'ютерній мережі

На рис. 1 детектори (сенсори) IDPS розміщені в точках входу в сегменти мережі. Мережні сегменти мають як внутрішні так і зовнішні ресурси. Сенсори відправляють свої звіти відносно подій на сервер управління, який розміщено за Firewall.

Сучасні IDPS здатні контролювати роботу мережних пристроїв та операційних систем (ОС), виявляти несанкціоновані дії та в автоматичному режимі виконувати визначені адміністратором функції, наприклад: сповіщення адміністратора (звукове попередження, повідомлення пошти/net send/SMS); зміна налаштувань брандмауера (блокування IP-адреси порушника); розрив встановленого порушником TCP-з'єднання; запуск визначеної адміністратором програми (скрипту); занесення до протоколу інформації про атаку тощо.

IDPS класифікують у різний спосіб. Так, за способом реагування розрізняють пасивні та активні IDS. Пасивні просто фіксують факт атаки, записують дані в файл журналу та видають попередження. Активні – намагаються протидіяти атаці, наприклад, переконфігуровують MME, або генерують списки доступу маршрутизатора.

За способом виявлення атаки розрізняють системи, засновані на сигнатурному аналізі (signature-based) та на пошуку аномалій (anomaly-based). Перший тип заснований на порівнянні інформації з базою сигнатур атак, недоліком систем даного типу є неможливість реагування на нові, невідомі види атак. Другий тип заснований на контролі частоти подій або виявлення статистичних аномалій. Така система орієнтована на виявлення нових типів атак, однак її недоліком є необхідність постійного навчання.

Найбільш популярною є класифікація IDPS за рівнем виявлення атак. Розрізняють мережний та системний рівні виявлення атак.

Мережні IDPS (Network based IDPS, NIDPS) аналізують мережний трафік з метою виявлення атак та іншої підозрілої активності. Такі системи повинні мати доступ до всього трафіку в сегменті і традиційно відрізняються розподіленою архітектурою, мають сенсори, які збирають інформацію про трафік і відправляють її на консоль управління. Сенсори можуть бути програмними та апаратними. Апаратні рішення значно виграють за швидкістю але програють за ціною. Функціональність систем є практично однаковою. Апаратні рішення пропонуються двома типами виробників. Перші - виробники мережного устаткування, які вбудовують в свої рішення модулі, що відповідають за виявлення і запобігання вторгненням (наприклад, Cisco або Juniper Networks). До другого типу відносяться компанії, орієнтовані на розробку програмних рішень в галузі інформаційної безпеки, в лінійці продуктів яких присутні апаратні рішення (наприклад, Check Point, IBM).

Системи виявлення атак мережного рівня використовують як джерело даних для аналізу необроблених мережних пакетів. Як правило, NIDPS використовують мережний адаптер, котрий функціонує в режимі “прослуховування” (promiscuous), та аналізують трафік в реальному масштабі часу у темпі його проходження через сегмент мережі. Модуль розпізнавання атак використовує чотири широко відомі методи для розпізнавання сигнатури атаки, це такі як: відповідність трафіка шаблону (сигнатурі), виразу чи байткоду, котрий характеризує атаку або підозрілу дію; контроль частоти подій або перевищення величини порогу; кореляція декількох подій з низьким пріоритетом; виявлення статистичних аномалій.

Як тільки атака виявлена, модуль реагування представляє широкий набір варіантів повідомлень, видачі сигналу тривоги та реалізації контрзаходів у відповідь на атаку. Ці варіанти змінюються від системи до системи, але, як правило, об’єднують в собі: повідомлення адміністратора через консоль або електронною поштою, завершення з’єднання з атакуючим хостом та запис сесії для подальшого аналізу та збору доказів атаки.

Сучасні IDPS системного рівня для виявлення атак використовують журнали реєстрації подій. Процес виявлення здійснюється автоматизовано та об’єднує складні методи виявлення, що ґрунтуються на новітніх дослідженнях в галузі математики. Як правило, IDPS системного рівня контролюють систему, події та журнали реєстрації подій безпеки (security log чи syslog). Коли якийсь з цих файлів змінюється, то IDPS порівнює нові записи з сигнатурами атак, щоб перевірити, чи є збіжність. Якщо така збіжність знайдена, то система надсилає адміністратору сигнал тривоги або приводить в дію інші задані механізми реагування.

IDPS системного рівня постійно розвиваються, поступово об’єднуючи все нові й нові методи виявлення. Одним з таких популярних методів є метод, що полягає у перевірці контрольних сум ключових системних та виконуючих файлів через регулярні інтервали часу на предмет несанкціонованих змін. При цьому, своєчасність реагування на атаки безпосередньо пов’язана з частотою опитування. З проведеного вище аналізу IDPS мережного та системного рівнів визначимо їх основні переваги.

Переваги систем виявлення атак мережного рівня.

1. Відносно низька вартість експлуатації IDPS мережного рівня. Що обумовлено, по-перше, необхідністю встановлення сенсорів лише в найбільш важливих місцях мережі для

контролю трафіка, що циркулює між чисельними сегментами мережі. По-друге, системи мережного рівня не потребують, встановлення програмного забезпечення системи виявлення атак на кожному окремому хості.

2. Можливість виявлення атак, які пропускаються на системному рівні. IDPS мережного рівня аналізують заголовки мережних пакетів на наявність підозрілої або деструктивної дії, в той час як IDPS системного рівня не працюють із заголовками пакетів і, відповідно, не можуть визначити певні типи атак. Наприклад, багато мережних атак типу DoS та "фрагментований пакет" (TearDrop) можуть бути ідентифіковані тільки шляхом аналізу заголовків пакетів. Крім того, IDPS мережного рівня дозволяють аналізувати зміст тіла даних пакета, шукаючи команди або певний синтаксис, який використовується в конкретних атаках.

3. Більша складність для зловмисника видалити сліди своєї присутності. IDPS мережного рівня використовує "живий" трафік при виявленні атаки в реальному масштабі часу. Дані, що аналізуються включають в себе не тільки інформацію про метод атаки, але і інформацію, яка може допомогти при ідентифікації зловмисника.

4. Можливість виявлення та реагування в реальному масштабі часу. IDPS мережного рівня виявляють підозрілі та зловмисні атаки в міру того, як вони відбуваються, і тому забезпечують більш швидке повідомлення та реагування, ніж IDPS системного рівня. Наприклад, зловмисник, який ініціює атаку мережного рівня типу DoS на основі протоколу TCP, може бути зупинений IDPS мережного рівня, що посилає встановлений прапорець Reset у заголовок TCP-пакету для завершення з'єднання з атакуючим хостом, до того, як атака призведе до руйнування або пошкодження хосту що атакується. IDPS системного рівня, як правило, не розпізнають атаки до моменту відповідного запису в журнал та застосовують дії у відповідь вже після того, як був зроблений запис. Повідомлення в реальному масштабі часу дозволяє швидко зреагувати у відповідності із заздалегідь визначеними параметрами.

5. Можливість виявлення невдалих спроб атак, або підозрілих намірів. IDPS мережного рівня, що встановлена із зовнішньої сторони MME, дозволяє виявляти атаки, спрямовані на інформаційні ресурси за MME. IDPS системного рівня не ідентифікує відбитих атак, які не досягають хосту за MME. При цьому втрачається важлива інформація, яка може бути використана для вдосконалення політики безпеки.

6. Незалежність від ОС. IDPS мережного рівня не залежать від ОС, встановлених в мережі, що підлягає захисту. IDPS системного рівня потребують встановлення конкретних ОС для правильного функціонування та генерування необхідних результатів.

Переваги систем виявлення атак системного рівня.

Незважаючи на те, що IDPS системного рівня не настільки швидкі, як їх аналоги мережного рівня, їм характерний ряд переваг, які не мають останні. До цих переваг слід віднести наступні:

1. Можливість підтвердження успіху або зриву атаки. Оскільки IDPS системного рівня використовують журнали реєстрації, що містять дані про події, які дійсно мали місце, то системи цього класу дозволяють з високою точністю визначати - чи дійсно була атака вдалою чи ні.

2. Можливість контролю конкретного хосту. IDPS системного рівня дозволяють контролювати дії користувача, доступ до файлів, зміни прав доступу до файлів, спроби встановлення нових програм та (або) спроби отримання доступ до привілейованих сервісів. Наприклад, IDPS системного рівня може контролювати всю logon- и logoff-діяльність користувача, а також дії, що виконує кожен користувач при підключенні до мережі. Технологія виявлення атак на системному рівні може також контролювати діяльність, яка зазвичай ведеться лише адміністратором.

IDPS системного рівня можуть контролювати зміни в ключових системних файлах або файлах, що виконуються. Спроби перезапису таких файлів або інсталяцій "троянських коней" можуть бути виявлені та припинені. Системи мережного рівня іноді пропускають такий тип атак.

3. Можливість виявлення атак, які пропускають системи мережного рівня. IDPS системного рівня можуть виявляти атаки, які не можуть бути виявлені засобами мережного рівня. Наприклад, атаки, що здійснюються з сервера, що атакується, не можуть бути виявлені системами виявлення атак мережного рівня.

4. Можливість використання для мереж з шифруванням та комутацією. Оскільки IDPS системного рівня встановлюється на різних хостах мережі, яку необхідно захистити, то вона може вирішити деякі з проблем, які виникають при експлуатації систем мережного рівня в мережах з комутацією та шифруванням. Комутація дозволяє керувати великомасштабними мережами, як декількаами мережними сегментами. У результаті буває складно визначити найкраще місце для встановлення IDPS мережного рівня. Виявлення атак на системному рівні забезпечує більш ефективну роботу в комутуючих мережах, так як дозволяє розмістити IDPS лише на тих хостах, на яких це необхідно.

Певні типи шифрування також є проблемними для систем виявлення атак мережного рівня. Залежно від того, де здійснюється шифрування (канальне або абонентське), IDPS мережного рівня може залишитися нечутливою до певних атак.

5. Можливість виявлення та реагування в масштабі часу близькому до реального. На відміну від застарілих систем, які перевіряють статус та зміст журналів реєстрації через заздалегідь визначені інтервали часу, сучасні IDPS системного рівня отримують переривання від ОС, як тільки з'явиться новий запис в журналі реєстрації. Цей новий запис може бути оброблений відразу, що значно зменшує час між розпізнаванням атаки та реагуванням на неї. Таким чином, залишається затримка між моментом запису ОС події в журнал реєстрації та моментом розпізнавання її системою виявлення атак, але в багатьох випадках зловмисник може бути виявлений та зупинений перш ніж зможе нанести шкоду.

6. Відсутність потреби в додаткових апаратних засобах. IDPS системного рівня встановлюються на існуючу мережну інфраструктуру, враховуючи файлові сервера, Web-сервера та інші ресурси, що використовуються.

Аналіз вищезазначених переваг IDPS мережного та системного рівнів показав, що ці системи ефективно доповнюють одна одну. Таким чином, наступні покоління IDPS у перспективі повинні поєднувати в собі інтегровані системні та мережні компоненти. Синтез цих двох технологій сприятиме підвищенню ефективності захисту мереж від атак та зловживань, дозволить реалізувати більш жорстку політику безпеки та внести більшу гнучкість у процес експлуатації мережних ресурсів.

На сьогоднішній день на ринку IT-технологій IDPS представлені значною кількістю програмних та програмно-апаратних комплексів. Прикладом таких систем є програмні продукти Kerio WinRoute Firewall, SNORT, McAfee Entercept, ETrust Intrusion Detection, Symantec ManHunt та інші [5, 6]. Слід зазначити, що розробники IDPS практично не дають доступного об'єктивного опису їх переваг та недоліків, що значно ускладнює вибір потрібного продукту користувачеві. Для вирішення цієї проблеми на даний час ведеться розробка єдиного стандарту для тестування IDPS. В [6] опублікований ряд звітів, що містять порівняльну оцінку IDPS, ця інформація може бути корисна користувачеві для вибору системи, що задовольнила б необхідний рівень захисту інформаційного ресурсу. В [8] для порівняльного аналізу IDPS запропоновані такі показники:

1) *Клас атак, що виявляються.* Даний показник визначає, які класи атак здатна виявляти IDPS. Це один з ключових показників. Клас атаки - це четвірка параметрів <L, R, A, D>, де L - розташування об'єкта, що здійснює атаку (може бути внутрішнім по відношенню до системи, яку захищають {li}, чи зовнішнім {le}); R - ресурс, який атакують (ресурси розподіляються за розміщенням (хостові {rl}, мережні {rn}) та типом (ресурси користувачів {ru}, системні ресурси {rs}, ресурси СУБД {rd}, обчислювальні ресурси {rc} та ресурси захисту {rp}); A - цільовий вплив на ресурс (збір інформації {as}, отримання прав користувача ресурсу {au}, отримання прав адміністратора ресурсу {ar}, порушення цілісності ресурсу {ai}, порушення працездатності ресурсу {ad}); D - ознака розподіленого характеру атаки.

2) *Рівень спостереження за системою*. Визначає, на якому рівні системи збирають данні для виявлення атаки. Виділяють хостові та системні джерела. В межах хостових джерел виділяють рівні ядра та додатку. Від рівня спостереження за системою залежить швидкість збору інформації, вплив системи на інформацію, що збирається, ймовірність отримання спотвореної інформації. Слід зазначити, що використання методу виявлення, який дозволяє аналізувати поведінку на всіх рівнях абстракції, не означає, що ця можливість реалізована в конкретній системі. Найчастіше реалізація має менші можливості, ніж теоретичні можливості використаного методу. (HIDS – спостереження на рівні ОС окремого хосту мережі; NIDS – спостереження на рівні мережної взаємодії об'єктів на хостах мережі; AIDS – спостереження на рівні окремих додатків хоста мережі; Hybrid – комбінація спостерігачів різних рівнів).

3) *Використаний метод виявлення атак.* Метод виявлення атак є ключовим показником порівняння IDPS. Виділяють два класи методів: методи виявлення аномалій (статистичний аналіз, кластерний аналіз, нейронні мережі, імунні мережі, експертні системи, біометрія, SVM, аналіз систем станів) та методи виявлення зловживань (аналіз систем станів, графи атак, нейронні мережі, імунні мережі, SVM, експертні системи, методи, засновані на специфікаціях, MARS – Multivariate Adaptive Regression Splines, сигнатурні методи). Адаптивність до невідомих атак визначає здатність методу виявляти раніше невідомі атаки.

Для порівняльного аналізу методів виявлення атак в [9] запропоновано такі показники:

а) *рівень спостереження за системою* (даний показник визначає рівень абстракції подій, аналізуємих у захищаємій системі та визначає межі застосування методу для виявлення атак в мережах);

б) *можливість верифікації методу* (даний показник дозволяє оцінити, чи може кваліфікований оператор IDPS або експерт відтворити послідовність кроків з прийняття рішення щодо наявності атаки {наприклад, вважається, що сигнатурні методи можливо верифікувати, а кластерні – ні}, можливість верифікації дозволяє провести експертну оцінку коректності методу та його реалізації у будь-який момент часу, в тому числі в процесі експлуатації IDPS на його базі);

в) *адаптивність метода* (оцінка стійкості метода до малих змін реалізації атаки, котрі не змінюють результат атаки, адаптивність – єдина суттєва перевага «альтернативних» методів виявлення атак перед «сигнатурними»);

г) *стійкість* (даний показник характеризує незалежність результату роботи метода від системи, що захищається – для одного й того ж входу метод повинен давати один вихід, проблема стійкості особливо гостро стоїть для статистичних методів, які аналізують абсолютні значення параметрів продуктивності та завантаженості ресурсів мережі та хостів, котрі можуть суттєво відрізнятись на різних хостах і у різних мережах);

д) *обчислювальна складність* (теоретична оцінка складності методу в режимі виявлення, без урахування можливих попередніх етапів налаштування та навчання).

4) *Масштабуємість*. Визначає можливість додавання до аналізу нових ресурсів мережі, нових хостів і каналів передачі даних, в тому числі можливість управління єдиною розподіленою системою виявлення атак. Додатково може бути присутня можливість віддаленого управління IDPS. При повністю розподіленому управління необхідно управляти всіма компонентами IDPS окремо. При повністю централізованому управлінні всі компоненти IDPS можуть управлятись з одного хосту. Оптимальною є організація управління за централізованою схемою, в котрій може бути декілька центрів, і вони можуть динамічно мінятись.

5) *Відкритість.* Визначає наскільки система є відкритою для інтеграції до неї інших методів виявлення атак, компонентів сторонніх розробників та поєднання її з іншими системами захисту інформації. Це можуть бути програмні інтерфейси для підключення додаткових модулів і (чи) реалізація стандартів взаємодії мережних компонентів.

6) *Формування відповідної реакції на атаку*. Визначає наявність в системі вбудованих механізмів відповідної реакції на атаку, окрім самого факту її реєстрації. Прикладом реакції

можуть буди розрив з'єднання з атакуючим об'єктом, блокування його на MME, відстеження шляху проникнення атакуючого об'єкту в систему, яка захищається.

7) *Захищеність*. Визначає ступінь захищеності IDPS від атак на її компоненти, включаючи захист інформації, що циркулює, стійкість до часткового виходу компонентів з ладу чи їх компрометації. Розглядаються питання наявності уразливостей в компонентах IDPS, захищеність каналів передачі даних між ними, авторизація компонентів всередині IDPS.

Висновки. Вибір IDPS повинен ґрунтуватись на вимогах, що висуваються до системи захисту інформації в кожному конкретному випадку. Певна "ідеальна" система виявлення та запобігання вторгненням повинна мати властивості: покривати всі класи атак (повна система); дозволяти аналізувати поведінку ІТС, яку захищають, на всіх рівнях: мережному, хостовому, на рівні ОС та окремих додатків; бути адаптивною до невідомих атак (використовувати адаптивний метод виявлення атак); змінювати масштаб для ІТС різних класів: від невеликих локальних мереж класу «домашній офіс» до крупних багатосегментних корпоративних мереж, забезпечуючи можливість централізованого управління всіма компонентами IDPS; бути відкритою; мати вбудовані механізми реагування на атаки; бути захищеною від атак на компоненти IDPS, в тому числі від перехвату управління чи атаки типу DoS. Правильне розміщення системи IDPS в мережі не впливає на її топологію, проте має суттєве значення для оптимального моніторингу та досягнення максимального ефекту від її захисту.

ЛІТЕРАТУРА

1. Шаньгин В.Ф. Защита компютерной информации. Эффективные методы и средства / В.Ф. Шаньгин – М.: ДМК Пресс, 2010. – 544 с.
2. Лукацкий А.В. Обнаружение атак / А.В. Лукацкий – С-Петербург: БХВ-Петербург, 2003. – 256 с.
3. Методы и средства защиты информации. В 2-х томах / Ленков С.В., Перегудов Д.А., Хорошко В.О. Под ред. В.А. Хорошко. – К.: Арий, 2008. – Том II. Информационная безопасность. – 344 с.
4. Лукацкий А.В. Предотвращение сетевых атак: технологии и решения / А. В. Лукацкий – С-Петербург: Экспресс Электроника, 2006. – 268 с.
5. Обзор механизмов реализации и обнаружения атак [Электронный ресурс] Режим доступа к статье: http://comp-bez.ru/?p=778
6. Обзор систем обнаружения вторжений [Электронный ресурс] Режим доступа к статье: http://www.connect.ru
7. Информационная безопасность [Электронный ресурс] Режим доступа к статье: http://www.data.com/lab_tests/intrusion.html
8. Критерии сравнения систем обнаружения атак [Электронный ресурс] Режим доступа к статье: http://inf-bez.ru/?p=480
9. Критерии сравнения методов обнаружения атак [Электронный ресурс] Режим доступа к статье: http://inf-bez.ru/?p=478

Надійшла: 27.01.2012

Рецензент: д.т.н., проф. Лєнков С.В.