УДК 004.681

А. А. Завада, О. В. Самчишин, В. В. Охрімчук

АНАЛІЗ СУЧАСНИХ СИСТЕМ ВИЯВЛЕННЯ АТАК І ЗАПОБІГАННЯ ВТОРГНЕННЯМ

У статті проаналізовано основні механізми реалізації кібератак на ресурси інформаційно-телекомунікаційних систем та способи їх виявлення. Розглянуто переваги та недоліки основних типів систем виявлення атак і запобігання вторгненням. Запропоновано перелік показників для порівняльного аналізу зазначених систем та визначено властивості, які повинна мати сучасна система виявлення атак і запобігання вторгненням.

Постановка проблеми. 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. Тому системи захисту інформації (СЗІ), зокрема антивірусне програмне забезпечення й системи виявлення атак (СВА) тощо, стали невід'ємною частиною ІТС [1]. СЗІ є складними програмно-апаратними комплексами, що функціонують на основі спеціальних математичних методів і моделей. Висока надійність цих систем забезпечується перевірками програмних кодів та верифікацією реалізованих у них методів і моделей. Підтвердження відповідності (верифікація) здійснюється математичними методами згідно з критеріями ефективності функціонування СЗІ, визначеними на етапі специфікації. Аналіз цих критеріїв за рядом метрик дозволяє оцінити якість реалізації окремих елементів та системи в цілому.

Слід зазначити, що атаки на ІТС з кожним роком стають усе досконалішими, масштабнішими та інтенсивнішими. Враховуючи зазначене вище, актуальною є проблема розробки та удосконалення систем виявлення вторгнень в ІТС, головним завданням яких є саме виявлення мережних атак, спроб несанкціонованого доступу та використання ресурсів мережі. Постійний стрімкий розвиток методів та способів деструктивного програмного впливу на ІТС зумовлює необхідність проведення порівняльного аналізу існуючих систем виявлення атак і запобігання вторгненням з метою визначення найбільш ефективних механізмів захисту інформаційних ресурсів.

Огляд останніх досліджень і публікацій. Уперше ідея створення системи виявлення вторгнень з'явилась у 1980-х роках [2]. Наприкінці 1990-х років почалися активні розробки в цій галузі. У 1998 р. стартували такі відомі нині проекти, як Snort та Prelude [2]. Пізніше через ряд причин розробники почали реалізовувати багаторівневі системи захисту [6]. З аналізу доступних джерел [1–6] з'ясовано, що одним з перспективних шляхів підвищення рівня захищеності ІТС є вдосконалення активних засобів захисту інформації на базі систем виявлення атак (вторгнень) – IDS (Intrusion Detection Systems) та систем запобігання вторгненням – IPS (Intrusion Prevention Systems) [6, 10]. На сьогоднішній день таких систем відомо близько сотні, при цьому вони досить різноманітні

як за принципами роботи, так і за технологіями, що в них використовуються [6, 7]. Найбільш поширені комерційні СВА на базі хосту *Intruder Alert* (компанія *Symantec*) і мережі *Cisco Secure Scanner* (компанія *Cisco Systems*), гібридної СВА *RealSecure* (компанія *Internet Security Systems*), а також некомерційні СВА *ASAX* (*University of Namur, Belgium*), *SHADOW* (*Naval Surface Warfare Center, Dahlgren Division*) та *NetSTAT* (*University of California at Santa Barbara*) [2–9]. Враховуючи переваги та недоліки обох типів систем, вибір між IDS та IPS не є однозначним. У переважній більшості публікацій наведена інформація про ті чи інші СВА, яка носить, так би мовити, "рекламний характер" і не відображає повною мірою особливостей їх функціонування. Таким чином, залишається актуальним питання проведення саме порівняльного аналізу сучасних СВА.

Формулювання завдання дослідження. Насиченість ринку інформаційних технологій зазначеними системами ставить перед користувачем нагальну потребу вибору оптимальної системи виявлення атак і запобігання вторгненням, але здійснити його можливо лише на основі аналізу сучасного стану та перспектив їх найближчого розвитку. Ніні існує величезна кількість систем, що позиціонуються як IDS або IPS. Тому метою статті є проведення детального аналізу основних механізмів реалізації кібератак, а також переваг і недоліків сучасних систем виявлення атак та запобігання вторгненням.

Виклад основного матеріалу. На практиці використовуються різні комбінації атак. Наприклад, зловмисник використовує мережні сканери для виявлення топології мережі, потім – сканери вразливостей для визначення вразливих хостів. Знайдені на хості вразливості використовуються зловмисником для віддаленого виконання коду. Таким чином, у СВА повинні бути реалізовані механізми виявлення різних типів 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 вразливостей обчислювальної системи [2, 3].

Існують різні методи класифікації атак, наприклад, їх поділяють на пасивні та активні, зовнішні й внутрішні, навмисні й ненавмисні. 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 вразливостей (vulnerability scanners); зломщики паролів (password crackers); аналізатори протоколів (sniffers); збір інформації про характеристики ІТС (information gathering); несанкціонований доступ до інформаційних ресурсів системи (unauthorized access attempts); підозріла активність (suspicious activity); системні атаки (system attack).

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

Аналіз концептуальних основ побудови сучасних СВА дозволяє зробити висновок, що робота кожної із систем ґрунтується на методах визначення аномалій та зловживань. Базисом зазначених методів є моделі шаблонів (профілів) поведінки. Методи визначення аномалій призначені для виявлення невідомих атак і вторгнень на ІТС на основі моделей

шаблонів нормальної поведінки (ШНП). Для побудови моделей ШНП використовують методи статистичного виявлення, нейронних мереж, теорії масового обслуговування тощо. Характерним недоліком моделей ШНП на базі методів статистичного виявлення є велика кількість помилкових спрацювань системи, що зумовлено помилками першого (пропуск атаки – *false negative*) та другого (хибного спрацювання – *false positive*) роду [10].

У табл. 1 наведено основні механізми реалізації для різних типів атак [5].

Таблиця 1

Основні механізми реалізації атак

№ з/п	Тип атаки	Механізм реалізації атаки
1.	Віддалене проникнення	Віддалений виклик командного рядка 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	Багаторазові спроби аутентифікації в системі
6.	Аналіз мережного трафіка	Перемикання мережного інтерфейсу в “режим прослуховування” і перехоплення мережного трафіка
7.	Несанкціонована аутентифікація	Порушення прав доступу і незаконне використання ресурсів
8.	Шкідливі програми	Приховане встановлення програмних модулів, прихований запуск процесів

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 вразливостей; невідповідні параметри мережного трафіка; непередбачені атрибути; додаткові знання про порушення, – то можна виявити або знизити ризики від реалізації атак.

Основні механізми виявлення атак, визначені для різних класів атак, наведено в табл. 2 [5].

Таблиця 2

Основні механізми виявлення атак

№ з/п	Механізми виявлення атаки	Клас атак, що виявляються
1.	Відстеження спроб аутентифікації в системі	Зовнішні (внутрішні) мережні (локальні) активні
2.	Відстеження перехоплення мережного трафіка	Зовнішні мережні активні
3.	Відстеження мережного трафіка	Зовнішні мережні пасивні
4.	Відстеження запуску процесів та звернень до файлової системи й реєстру	Внутрішні локальні активні

Розглянемо переваги і недоліки сучасних систем виявлення атак і запобігання вторгненням. IDS можуть сповістити про початок атаки на мережу, причому деякі з них здатні виявляти раніше не відомі атаки. IPS не обмежуються лише оповіщенням, але й здійснюють різні заходи, спрямовані на блокування атаки (наприклад, розрив з'єднання або виконання скрипта (спеціальної команди), заданого адміністратором). На практиці досить часто програмно-апаратні рішення поєднують у собі функціональність двох типів систем, їх об'єднання іноді називають IDPS (IDS і IPS).

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

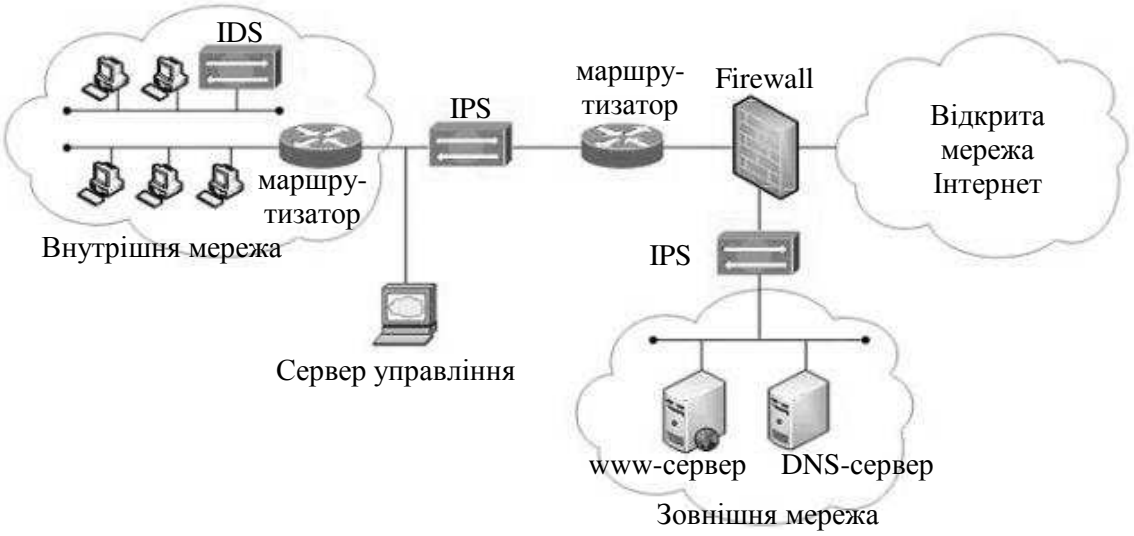

Рис. 1. Схема розміщення IDPS у комп'ютерній мережі

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 знаходиться за MME (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 електронної пошти, SMS); зміна налаштувань брандмауера (блокування IP-адреси порушника); розрив встановленого порушником TCP-з'єднання; запуск визначеної адміністратором програми (скрипта); занесення до протоколу інформації про атаку тощо.

IDPS класифікують у різний спосіб. Так, за способом реагування розрізняють пасивні та активні IDPS. Пасивні просто фіксують факт атаки, записують дані у файл журналу та видають попередження. Активні намагаються протидіяти атаці, наприклад, переконфігуровують MME або генерують списки доступу маршрутизатора [6].

За способом виявлення атаки розрізняють системи, що ґрунтуються на сигнатурному аналізі (signature-based) та на пошуку аномалій (anomaly-based). Перші порівнюють

інформацію трафіка з базою сигнатур атак, недоліком подібних систем є неможливість реагування на нові, невідомі види атак. Другі контролюють частоту подій або виявляють статистичні аномалії. Такі системи орієнтовані на виявлення нових типів атак, однак їх недоліком є необхідність постійного навчання [6].

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 трафіка в сегменті, вони 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 таких сенсорів є практично однаковою.

Системи виявлення атак мережного рівня використовують як джерело даних для аналізу необроблені мережні пакети. Як правило, у NIDPS застосовують мережний адаптер, який функціонує в режимі "прослуховування" (promiscuous) та аналізує трафік у реальному масштабі часу в темпі його проходження через сегмент мережі. Модуль розпізнавання атак використовує чотири широковідомі методи для розпізнавання сигнатури атаки: відповідність трафіка шаблону (сигнатурі), виразу чи байткоду, який характеризує атаку або підозрілу дію; контроль частоти подій або перевищення величини порога; кореляція декількох подій з низьким пріоритетом; виявлення статистичних аномалій. У разі виявлення атаки модуль реагування видає відповідне повідомлення та сигнал тривоги і пропонує широкий набір шляхів реалізації контрзаходів у відповідь на атаку, а також здійснює запис сесії для подальшого аналізу й збору доказів атаки.

Окремим сегментом систем виявлення атак мережного рівня є системи виявлення безпровідних атак – WIDS (Wireless Intrusion Detection System), основу яких складають сенсори, що виконують функцію збору безпровідного трафіка в режимі моніторингу та його обробку. Як правило, сенсори є достатньо інтелектуальними пристроями, які підтримують протоколи TCP/IP та мають розвинений інтерфейс управління.

Сучасні IDPS системного рівня для виявлення атак використовують журнали реєстрації подій. Цей процес автоматизований, він об'єднує складні методи виявлення, що ґрунтуються на новітніх дослідженнях у 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 вона 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 них 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.

На підставі проведеного вище аналізу IDPS мережного та системного рівнів визначимо їх основні переваги.

Переваги систем виявлення атак мережного рівня

1. Відносно низька вартість експлуатації. Це 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, у 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 не тільки інформацію про метод атаки, але й ту, що може допомогти для 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 надсилає встановлений прапорець Reset у заголовок TCP-пакета 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.

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 операційної системи (ОС). IDPS мережного рівня не залежать від ОС, встановлених у мережі, що підлягає захисту. IDPS системного рівня потребують встановлення конкретних ОС для правильного функціонування та генерування необхідних результатів.

Незважаючи на те, що IDPS системного рівня не настільки швидкі, як їх аналоги мережного рівня, їм характерний ряд переваг, яких не мають останні, до них відносять такі:

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) отримання доступу до привілейованих сервісів. Наприклад, IDPS системного рівня може контролювати всю logon- і logoff-діяльність користувача, а також дії, що він виконує 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, який 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, що виникають при експлуатації систем мережного рівня в мережах з комутацією та шифруванням. Комутація дозволяє керувати великомасштабними мережами як декількома 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, оскільки дозволяє розмістити IDPS лише на тих хостах, де 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. Відсутність потреби в додаткових апаратних засобах. IDPS системного рівня встановлюються на існуючу мережну інфраструктуру, враховуючи файлові сервери, веб-сервери та інші ресурси, що використовуються.

Аналіз зазначених вище 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. У [6] опубліковано низку звітів, що містять порівняльну оцінку IDPS, ця інформація може бути корисна для вибору системи, що задовольнила б необхідний рівень захисту інформаційного ресурсу. У [8] для порівняльного аналізу IDPS запропоновано такі показники:

1) *клас атак, що виявляються.* Даний показник визначає, які класи атак здатна виявляти IDPS (див. табл. 2). Клас атаки – це четвірка параметрів <L, R, A, D>, де L –

розташування об'єкта, що здійснює атаку (може бути внутрішнім відносно системи, яку захищають, чи зовнішнім); R – ресурс, який атакують (ресурси розподіляються за розміщенням (хостові, мережні) та типом (ресурси користувачів, систем управління базами даних, системні й обчислювальні ресурси тощо); A – цільовий вплив на ресурс (збір інформації, отримання прав користувача або адміністратора, порушення цілісності або працездатності ресурсу); D – ознака розподіленого характеру атаки;

2) *рівень спостереження за системою* визначає, на якому рівні системи збирають дані для виявлення атаки. Виділяють хостові та системні джерела. У межах хостових виділяють рівні ядра та додатка (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 хосту мережі; Hybrid – комбінація спостерігачів різних рівнів). Від рівня спостереження за системою залежить швидкість збору інформації, вплив системи на інформацію, що збирається, імовірність отримання спотвореної інформації;

3) *використаний метод виявлення атак,* що є ключовим показником порівняння IDPS. Виділяють два класи методів: виявлення аномалій (статистичний і кластерний аналізи, нейронні й імунні мережі, експертні системи, біометрія, аналіз систем станів) та виявлення зловживань (аналіз систем станів, графи атак, нейронні й імунні мережі, експертні системи, методи, що ґрунтуються на специфікаціях, сигнатурні методи). Для порівняльного аналізу методів виявлення атак у [9] запропоновано такі показники:

а) рівень спостереження за системою визначає рівень абстракції подій, які аналізуються в системі, що захищається, а також межі застосування методу для виявлення атак в мережах;

б) можливість верифікації методу 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 в будь-який момент часу, у тому числі в процесі експлуатації IDPS на його базі;

в) адаптивність методу – оцінка стійкості методу до малих змін реалізації атаки, які не змінюють результат атаки. Адаптивність – єдина суттєва перевага "альтернативних" методів виявлення атак перед "сигнатурними". Адаптивність до невідомих атак визначає здатність методу виявляти раніше не відомі атаки;

г) стійкість характеризує незалежність результату роботи методу 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, що можуть суттєво відрізнятись на різних хостах і в різних мережах);

д) обчислювальна складність – теоретична оцінка складності методу в режимі виявлення без урахування можливих попередніх етапів налаштування та навчання;

4) *масштабованість* визначає можливість додавання до аналізу нових ресурсів мережі, нових хостів і каналів передачі даних, у тому числі можливість управління єдиною розподіленою системою виявлення атак. Додатково можливим є віддалене управління IDPS. При повністю розподіленому управлінні необхідно керувати всіма

компонентами IDPS окремо, а при повністю централізованому усіма компонентами IDPS можна керувати з одного хосту. Оптимальною є організація управління за централізованою схемою, у якій може бути декілька центрів, що 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*. Цей показник визначає наявність у системі вбудованих механізмів відповідної реакції на атаку, окрім самого факту її реєстрації. Прикладом реакції можуть бути: розрив з'єднання з атакуючим об'єктом, блокування його на ММЕ, відстеження шляху проникнення атакуючого об'єкта 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, наявність вразливостей у компонентах IDPS, захищеність каналів передачі даних між ними, авторизацію компонентів усередині IDPS.

Таким чином, певна "ідеальна" сучасна система виявлення та запобігання вторгненням повинна мати такі найбільш важливі властивості: виявляти 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 їх виявлення); змінювати масштаб для ІТС різних класів: від локальних мереж класу "домашній офіс" до великих, багатосегментних корпоративних мереж, забезпечуючи можливість централізованого управління всіма компонентами IDPS; бути відкритою; мати вбудовані механізми реагування на вторгнення; бути захищеною від кібератак на компоненти IDPS, у тому числі від перехвату управління чи атаки типу DoS.

Висновки. Вибір IDPS повинен ґрунтуватись на вимогах, що висуваються до системи захисту інформації в кожному конкретному випадку. Проведене дослідження основних механізмів реалізації кібератак та порівняльний аналіз сучасних систем виявлення атак і запобігання вторгненням показав, що при вдосконаленні існуючих і проектуванні нових систем необхідно враховувати визначені властивості, зважаючи на особливості реалізації та функціонування ІТС, які підлягають захисту.

У подальшому потребує дослідження питання правильного розміщення IDPS у мережі, що має суттєве значення для оптимального моніторингу та досягнення максимального ефекту від її використання для захисту ІТС.

СПИСОК ЛІТЕРАТУРИ

1. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства / В. Ф. Шаньгин. – М. : ДМК Пресс, 2010. – 544 с.
2. Лукацкий А. В. Обнаружение атак / А. В. Лукацкий. – СПб. : БХВ-Петербург, 2003. – 256 с.
3. Ленков С. В. Методы и средства защиты информации : в 2 т. / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко ; под ред. В. А. Хорошко. – К. : Арий, 2008. – Т. 2 : Информационная безопасность. – 2008. – 344 с.

4. Лукацкий А. В. Предотвращение сетевых атак: технологии и решения / А. В. Лукацкий. – СПб. : Экспресс Электроника, 2006. – 268 с.
5. Обзор механизмов реализации и обнаружения атак [Электронный ресурс]. – Режим доступа : http://comp-bez.ru/?p=778.
6. Обзор систем обнаружения вторжений [Электронный ресурс]. – Режим доступа : http://www.connect.ru.
7. Информационная безопасность [Электронный ресурс]. – Режим доступа : 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.
10. Грищук Р. В. Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень : монографія / Р. В. Грищук. – Житомир : Рута, 2010. – 280 с.

Подано 23.11.12

А. А. Завада, А. В. Самчишин, В. В. Охримчук

АНАЛИЗ СОВРЕМЕННЫХ СИСТЕМ ВЫЯВЛЕНИЯ АТАК И ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ

В статье проведен анализ основных механизмов реализации кибератак на ресурсы информационно-телекоммуникационных систем и способов их выявления. Рассмотрены преимущества и недостатки основных типов систем выявления и предотвращения вторжений. Предложен перечень показателей для сравнительного анализа указанных систем. Определены основные, наиболее важные свойства, которые должна иметь современная система выявления и предотвращения вторжений.

A. A. Zavada , A. V. Samchyshyn, V. V. Okhrimchuk

ANALYSIS OF MODERN DETECTION OF ATTACKS AND PREVENTION OF INVASIONS OF SYSTEMS

In article the analysis of the main mechanisms of realization of cyberattacks to resources of the information-telecommunication systems and ways of detecting them. Discusses the advantages and disadvantages of the main types of detection and prevention intrusions of systems. Proposed list of indicators for the comparative analysis of these systems. Identified the main most important properties which the modern of detection and prevention intrusions system should have are defined.