

# АНАЛІЗ СУЧАСНИХ СИСТЕМ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ ВТОРГНЕНЬ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

В. І. Мешков<sup>1</sup>, В. О. Віролайн<sup>1</sup>

<sup>1</sup> Державний ВНЗ «Національний гірничий університет», м. Дніпропетровськ

## Анотація

Системи, які направлені на захист інформації як відкритої, так і з обмеженим доступом, повинні складатися з програмних та апаратних засобів, які забезпечують аналіз, моніторинг, контроль інформаційно-телекомунікаційної системи (ІТС). До таких засобів відноситься: міжмережеві екрани, антивірусні системи, системи виявлення та запобігання вторгнень. Для існуючих ІТС є багато підходів до побудови комплексного захисту, його необхідно обирати в залежності від розміру ІТС. Для невеликих ІТС – достатньо буде обмежитись налаштуванням міжмережевого екрану та антивірусної системи, для середніх і великих, наприклад, хостинг провайдер – необхідно застосувати більш суттєві механізми захисту, такі як: системи виявлення та запобігання вторгнень.

**Ключові слова:** системи виявлення вторгнень, системи запобігання вторгнень, міжмережевий екран, антивірусний захист, віртуальна приватна мережа, класифікація.

## Вступ

Способи захисту інформації на підприємстві, також як і канали витоку, постійно змінюються. З'являються нові пропозиції від різноманітних компаній, що надають послуги із захисту інформації. Панацеї звичайно немає, але є кілька базових кроків побудови системи захисту інформаційно-телекомунікаційної системи (ІТС) підприємства, на які необхідно обов'язково звернути увагу.

Багатьом напевно знайома концепція глибокого захисту від злову інформаційно-телекомунікаційної системи. Основна її ідея полягає в тому, щоб використовувати кілька рівнів захисту. Це дозволить, мінімізувати збиток, пов'язаний з можливим порушенням периметра безпеки вашої ІТС.

## 1. Види захисту ІТС

До базового захисту ІТС підприємства можна віднести:

1. Firewall (укр. міжмережевий екран) – це програма або обладнання, яке перешкоджає зловмисникам і деяким типам шкідливих програм отримувати доступ до комп'ютера по мережі або через Інтернет. Для цього Firewall перевіряє дані, що надходять з Інтернету або по мережі, і блокує їх або дозволяє передачу на комп'ютер (рис. 1).

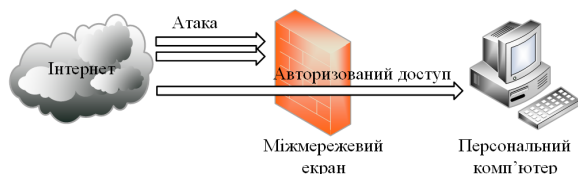


Рис. 1. Схема роботи міжмережевого екрану

2. VPN (англ. Virtual Private Network, укр. віртуальна приватна мережа).

Віртуальна приватна мережа представляє собою підключення типу «точка-точка» (логічне з'єднання), яка працює поверх приватної або публічної мережі.

VPN-підключення типу «мережа-мережа» (логічне з'єднання) дозволяють організаціям встановлювати маршрутизовані підключення між окремими офісами (або між іншими організаціями) по публічній мережі, при цьому забезпечуючи захищеність зв'язку (рис. 2).[2]

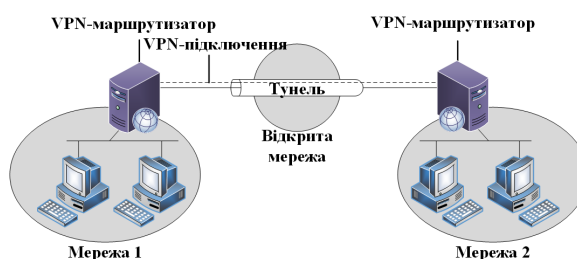


Рис. 2. Організація VPN-з'єднання двох віддалених вузлів

3. IDS/IPS (англ. Intrusion Detection System /Intrusion Prevention System, укр. Система виявлення вторгнення (СВВ)/Система запобігання вторгнення (СЗВ)).

СВВ – програмний або апаратний засіб, призначений для виявлення фактів несанкціонованого доступу в комп'ютерну систему (мережу), або несанкціонованого управління такою системою.

СЗВ – програмна або апаратна система забезпечення безпеки, яка активно блокує вторгнення у разі їх виявлення.

Архітектура СВВ (рис. 3) і СЗВ (рис. 4).[1]

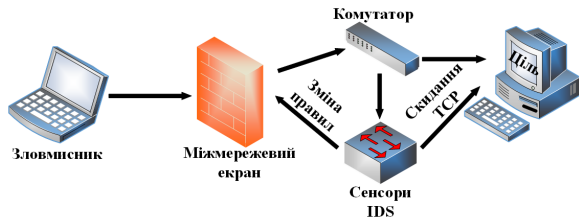


Рис. 3. Система виявлення вторгнень

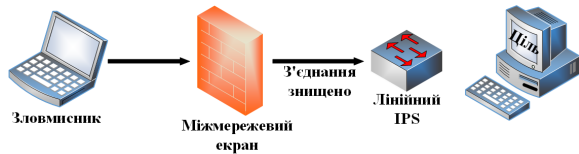


Рис. 4. Система запобігання вторгнень

4. Антивірусний захист – програмне забезпечення, яке здатне знаходити, «лікувати», блокувати, а також повністю видаляти віруси з системи. Антивірусний захист здатний моментально попереджати про те, що на тій чи іншій веб-сторінці є вірус і ваша система може бути пошкодженою. Це дуже зручно, так як сама програма в цей же час прийме всі необхідні заходи. На даний момент існують багато різних програм антивірусного захисту, які відрізняються за: ціною, швидкістю роботи, якістю антивірусних баз та іншими параметрами.

5. Білі списки – перелік певних програм та служб, які може використовувати користувач. Контролює білі списки – адміністратор. Білі списки можна створити, як за допомогою вбудованих засобів операційної системи, так і за допомогою стороннього програмного забезпечення.

6. Фільтрація спаму – процедура, яка перевіряє вхідну кореспонденцію (E-mail) за встановленими налаштуваннями фільтрів і забезпечую виявлення небажаної розсилки, яка може містити в собі: рекламні пропозиції, «листи щастя», комп'ютерні віруси або опинитися спробою фішингу. До основних способів фільтрації спаму відносяться:

- Спеціалізовані постачальники сервісів фільтрації спаму;
- Програмне забезпечення для фільтрації спаму на власних поштових серверах.

7. Підтримка програмного забезпечення (ПЗ) в актуальному стані. Своєчасне оновлення ПЗ це є усуненням вразливостей виявлених у програмному продукті. Підтримка системи, ПЗ в актуальному розробником стані – означає роботу в більш безпечному середовищі. В більшості систем передбачений механізм повного автоматичного оновлення.

8. Фізична та технічна безпека корпоративної мережі. Маючи фізичний доступ до мережевого пристрою зловмисник, в більшості випадків, легко отримає несанкціонований доступ до мережі підприємства. Забезпечення фізичної та технічної безпеки корпо-

ративної мережі унеможливилює фізичний доступ до її складових.[8]

Необхідно звернути увагу на те, що утримувати захист корпоративної мережі на високому рівні досить важко. Ви повинні бути впевнені, що компанія не залежить всього лише від одного-двох рубежів захисту. Завжди прагніть стежити за актуальною інформацією і свіжими рішеннями на ринку інформаційної безпеки.

## 2. Система виявлення вторгнень

Системи виявлення вторгнень все частіше стають необхідним доповненням інфраструктури мережевої безпеки. СВВ служать механізмами моніторингу та спостереження підозрілої активності. Вони можуть виявити атакуючих, які змогли обійти Firewall, і видати звіт про це адміністратору, який, у свою чергу, зробить подальші кроки щодо запобігання атаки. Технології виявлення вторгнень не роблять систему абсолютно безпечною. Як правило, СВВ мають наступну структуру (рис. 5).[1]

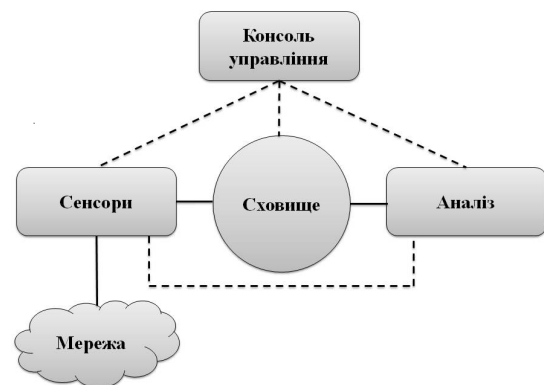


Рис. 5. Загальна структура СВВ

- Сенсорна підсистема – відповідає за збір інформації, пов'язану з безпекою мережі.
- У сховищі, зберігається інформація, що надходить від сенсорів й аналізатору.
- Аналізатор – виявляє підозрілий трафік і атаки, ґрунтуючись на даних від сенсорів.
- Консоль управління, дозволяє конфігурувати СВВ.[5]

## 3. Класифікація СВВ

Системи виявлення вторгнень можна класифікувати:

### 1. За характером відповідної реакції:

- пасивні – системи виявлення, в яких після виявлення та розпізнавання підозрілого трафіку, СВВ тільки повідомляє користувача або адміністратора про загрозу;
- активні – системи запобігання, що протистоять вторгненням, шляхом скидання з'єднання або зміна правил Firewall з метою блокування підозрілого трафіку;

- гібридні, що здійснюють виявлення та протистоять вторгненням в автоматичному режимі.

## 2. За методиками аналізу:

- статистичні СВВ – використовує статистичний підхід, після установки «навчаються» адміністратором, який задає політику СВВ, відповідну нормальної активності в мережі – типи трафіку, з'єднання між вузлами, використовувані протоколи і порти. При виявленні аномалій в роботі мережі або статистично значущих відмінностей трафіку від типового в даній мережі, СВВ оповіщає про це адміністратора. Основною проблемою такого підходу є складність в налаштуванні і велика кількість хибнопозитивних тривог у разі некоректно заданих правил.
- сигнатурні СВВ аналізують трафік у мережі або порівнюють пакети з базою даних сигнатур (відомих атрибутів атак). При такому підході основною проблемою є старіння баз сигнатур.
- гібридна СВВ поєднує два і більше підходів для розробки СВВ. Дані від агентів на хостах комбінуються з мережевою інформацією для створення найбільш повного уявлення про безпеку мережі.

## 3. За рівнем виявленням атак:

- NIDS (англ. Network Intrusion Detection Systems). Відстежує вторгнення, перевіряючи мережевий трафік і веде спостереження за декількома хостами. Мережева система виявлення вторгнень отримує доступ до мережевого трафіку, підключаючись до концентратора або комутатора, налаштованому на дублювання портів, або мережевий ТАР пристрій. Перевагами NIDS є велике покриття для моніторингу та у зв'язку з цим централізоване управління, також NIDS не впливають на продуктивність і топологію мережі. До недоліків цих систем можна віднести: високу завантаження системи, NIDS потребує додаткового налаштування і функціональності мережевих пристроїв. Системи NIDS не можуть аналізувати зашифровану інформацію і розпізнавати результати атак.
- GrIDS (англ. Graph-Based Intrusion Detection System). Ця система являється удосконаленою версією NIDS. У кожний сегмент LAN встановлюється свій сніфер. Інформація від них збирається разом, аналізується і представляється у виді схеми інформаційних потоків. Усі NIDS не залежать від типу використовуваної в мережі ОС. Для роботи їм необхідний виділений вузол у контрольованому сегменті і мережевий адаптер, який уміє приймати усі типи пакетів. Логічним вирішенням буде встановлення захищеного з'єднання між NIDS і консоллю управління.
- OIDS (англ. Operational Intrusion Detection Systems). Система спеціалізується на внутрішніх атаках. Ці системи розробили на випадок, якщо зломиснику вдалося увійти в систему від імені зареєстрованого користувача. Або, коли атака на мережу відбувається зсередини її самої. Система порівнює дії конкретного користувача у

даний момент часу з його звичайними діями, і у разі великих розбіжностей видає повідомлення. Простіше кажучи, оцінюється типовість дій (операцій) кожного з користувачів, в той час коли NIDS оцінює типовість трафіку.

- HIDS (англ. Host-based Intrusion Detection System). Ця система працює з інформацією, зібраною всередині одного комп'ютера. Таке розташування дозволяє HIDS аналізувати діяльність з великою вірогідністю і точністю, визначаючи тільки ті процеси і користувачів, які мають відношення до конкретної атаки в ОС. HIDS зазвичай використовують інформаційні джерела двох типів: результати аудиту ОС і системних журналів подій. HIDS мають можливість стежити за подіями локально, відносно хоста, можуть визначати атаки, які не можуть виявити NIDS. HIDS можуть функціонувати в системі, в якій мережевий трафік зашифрований, і система не вимагає додаткової функціональності мережевих пристроїв. До недоліків цієї системи відноситься: висока завантаження системи хоста, мале покриття для моніторингу, не мають централізованого управління і вони можуть бути заблоковані деякими DoS-атаками або навіть заборонені.
- ERIDS (англ. External Routing Intrusion Detection System). Приклад інноваційної та вузькоспеціалізованої системи. Необхідність її створення була продиктована тим фактом, що крім простого і розподіленого способу збору даних про мережі існують менш тривіальні. Наприклад, зломисник спочатку здійснює атаку на маршрутизатор, змінює його налаштування так, що він направляє трафік через сегмент, який не контролюється і доступний атакуючому.[3]

## 4. Інфраструктура хостинг провайдера з використанням IDS

Для забезпечення інформаційної безпеки ІТС хостинг провайдера необхідно реалізувати механізми захисту в системі.

Схема мережі хостинг провайдера зображена на рисунку 5.

У мережі хостинг провайдера використовують комбінацію з мережевої та хостової СВВ. Система HIDS розміщується на окремому вузлі і відстежує ознаки атак на даний вузол. Система NIDS знаходиться на окремій системі, яка відстежує мережевий трафік на наявність признаков атак, які проводяться у підконтрольному сегменті системи.[4]

Існує 5 основних типів сенсорів HIDS:

- аналізатори журналів;
- сенсори ознак;
- аналізатори системних викликів;
- аналізатори поведінки програм, служб;
- контролери цілісності файлів.

Слід зауважити, що деякі розробники ПЗ пропонують нові функціональні можливості сенсорів HIDS.

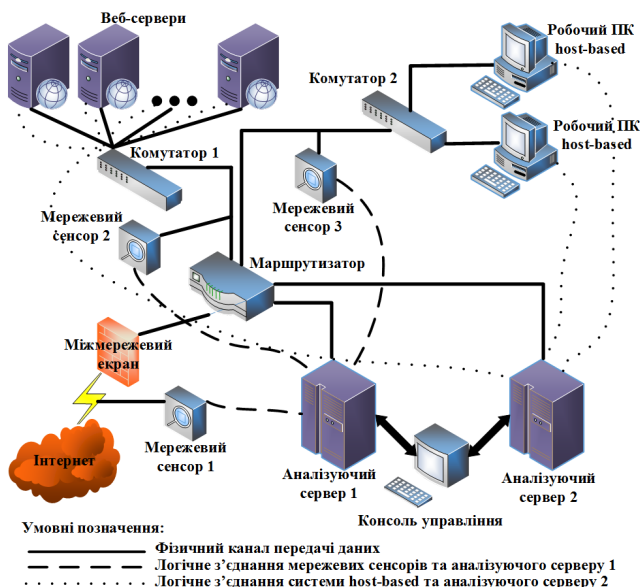


Рис. 6. Схема мережі хостинг провайдера

При розміщенні сенсорів NIDS необхідно керуватися ще одним ключовим правилом. Якщо в мережі використовуються комутатори замість концентраторів, сенсор виявлення вторгнень не буде правильно працювати, якщо він просто підключений до порту комутатора. Комутатор буде відправляти тільки трафік, спрямований на сенсор, до того порту, до якого підключений сенсор. У випадку з комутованою мережею існують два варіанти використання сенсорів виявлення вторгнень: застосування порту, що відстежує комутатор, або застосування мережевого розгалужувача.

Найбільш популярними системами з відкритим кодом є Snort, Suricata і OSSEC HIDS, з пропрієтарним кодом CATNET і McAfee IPS, Cisco Secure IDS, Dragon IDS.[6]

Для захисту веб-сторінок від НСД необхідно реалізувати функціональні послуги безпеки інформації згідно НД ТЗІ 2.5-010-03 «Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу».

Для технології T2 {КА-2, KB-1, ЦА-1, ЦО-1, ЦВ-1, ДВ-1, ДР-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-1, НВ-1} системи IDS дозволяють реалізувати частину критеріїв використовуючи свої механізми аналізу інформації, яка циркулює в ІТС провайдера.[7]

## Висновки

Сучасні системи забезпечення інформаційної безпеки корпоративної мережі підприємства дають можливість обрати найбільш вдалий та дієвий спосіб захисту інформації, яка циркулює в ІТС. Враховуючи це, власник ІТС має можливість обрати, відповідно до свого бюджету, необхідні механізми захисту починаючи від антивірусного ПЗ, закінчуючи системами виявлення та запобігання вторгненням. Кінцевою метою власника ІТС є розробка комплексної системи захисту інформації, яка забезпечить надійний захист інформації з обмеженим доступом.

## Перелік використаних джерел

1. Scarfone Karen. Guide to Intrusion Detection and Prevention Systems (IDPS) — 2007. — 127 p.
2. Mattord Verma. Principles of Information Security — 2008. — 300 p.
3. Sen Sevil. Power-Aware Intrusion Detection in Mobile Ad Hoc Networks — 2006. — 20 p.
4. Anderson Ross. Security Engineering: A Guide to Building Dependable Distributed Systems — 2007. — 388 p.
5. Jackson Kathleen. A Phased Approach to Network Intrusion Detection — 1991. — 30 p.
6. Syngress. Snort IDS and IPS Toolkit — 2007. — 197 p.
7. ДСТСЗІ СБ України. НД ТЗІ 2.5-010-03 «Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу» — 2003. — 16 с.
8. М. В. Грайворонський, О. М. Новіков. Безпека інформаційно-комунікаційних систем — 2009. — 608 с.