УДК 004.056 **Лук'яненко Т.Ю., Поночовний П.М., Легомінова С.В.**
DOI: 10.31673/2409-7292.2022.021521

МЕТОДИКА ВИЯВЛЕННЯ МЕРЕЖЕВИХ ВТОРГНЕНЬ І ОЗНАК КОМП'ЮТЕРНИХ АТАК НА ОСНОВІ ЕМПІРИЧНОГО ПІДХОДУ

У статті проведено аналіз характеристик виявлення мережевих вторгнень в інформаційну систему і виявлення ознак комп'ютерних атак на підприємстві; аналіз можливих дій зі сторони зловмисників, досліджено методи та принципи встановлення оптимальної системи виявлення мережевих вторгнень; розглянуто можливості розробки та використання систем виявлення мережевих вторгнень і виявлення ознак комп'ютерних атак на підприємстві в сучасних умовах; досліджено і розроблено рекомендації щодо впровадження систем виявлення вторгнень і виявлення ознак комп'ютерних атак для можливого подальшого встановлення їх в систему захисту інформації будь-якої організації.

Ключові слова: безпека, системи виявлення мережевих вторгнень, загрози, зловмисник, інформація, захист, інформаційна система, атака.

Вступ

На сьогоднішній день існує велика кількість різноманітних методів та засобів захисту від кібератак на об'єктах інформаційної діяльності [1]. Нажаль на теперішній час не існує абсолютно універсального методу протидії кібератакам і тому виникає необхідність комплексного підходу до вирішення даної задачі. Масовані кібератаки ініціюють створення спеціальних технічних рішень, засобів та систем протидії кібератакам. Для виявлення мережевих вторгнень використовуються сучасні методи [2,3,4], моделі [5], засоби [6], програмне забезпечення і комплексні технічні рішення для систем виявлення та запобігання вторгнень, які можуть залишатись ефективними при появі нових або модифікованих видів кіберзагроз. Але на практиці при появі нових загроз та аномалій, породжених атакуючими діями з невстановленими або нечітко визначеними властивостями, зазначені засоби не завжди залишаються ефективними і вимагають тривалих часових ресурсів для їх відповідної адаптації. Тому, системи виявлення вторгнень (СВВ) повинні постійно досліджуватись і удосконалюватись для забезпечення безперервності в їх ефективному функціонуванні.

Мета статті полягає в підвищенні рівня захищеності систем виявлення мережевих вторгнень та ознак комп'ютерних атак за рахунок оптимального використання ресурсів системи.

Можливості систем виявлення мережевих вторгнень

Система виявлення мережевих вторгнень - це програмний процес, який працює на спеціально виділеній системі, і відповідає за перемикання мережевої карти в системі в нерозбірливий режим роботи, при якому мережевий адаптер пропускає весь мережевий трафік в програмне забезпечення. Аналізує трафік, використовуючи набір правил і ознак атак для визначення того, чи представляє цей трафік якийсь інтерес. Після чого генерується відповідна подія. В більшість систем вже вбудований набір ознак атак, з якими порівнюється трафік в каналі зв'язку. При відсутності якихось ознак атаки в системі виявлення вторгнень, система не помічає цю атаку. Дані системи дозволяють вказувати певний трафік за адресою джерела, кінцевій адресі, порту джерела або кінцевого порту. Це дає можливість відстеження трафіку, який відповідає ознакам атак.

Існує безліч можливих методів атак та способів їх виявлення. Для виявлення багатьох типів атак потрібно розуміти принцип дії хакерів та можливі способи протидії - для спеціалістів інформаційної безпеки. Для цього розглянемо особливості використання шлюзів додатків, систем виявлення вторгнень і визначення DDoS атак.

Шлюз додатків. Приклад роботи шлюзу представлений на рис. 2.

Для забезпечення більш адресної безпеки, брандмауери повинні комбінувати при роботі пакетні фільтри зі шлюзами додатків. Шлюз додатків переглядає не лише заголовки, але й приймає рішення щодо дотримання політики на основі даного прикладного рівня. Шлюз додатків - це сервер, що працює на прикладному рівні, і через цей шлюз мають протікати всі дані додатків (вхідні і вихідні). На одному хості може працювати одразу

декілька шлюзів додатків, проте кожний шлюз - це самостійний сервер з власним набором процесів.

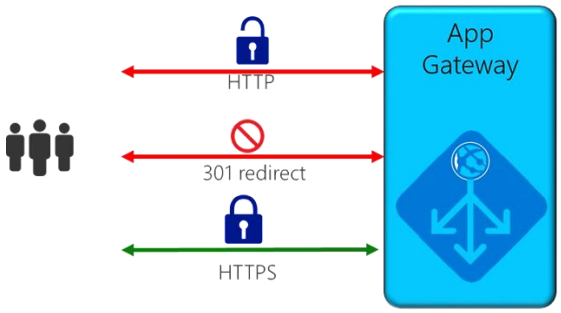

Рис. 2. Приклад роботи шлюзу додатків

Для виявлення багатьох типів атак потрібно виконувати поглиблену перевірку пакетів - аналізувати не лише поля заголовків, а й дані додатків, що містяться у пакеті. Шлюзи додатків можуть виконувати дану операцію, проте вони вирішують цю задачу лише для конкретного додатку. Системи виявлення сигнатур (рис. 3) можна розділити на дві категорії: ті, що працюють на основі перевірки сигнатур і ті, що працюють на основі виявлення аномалій.

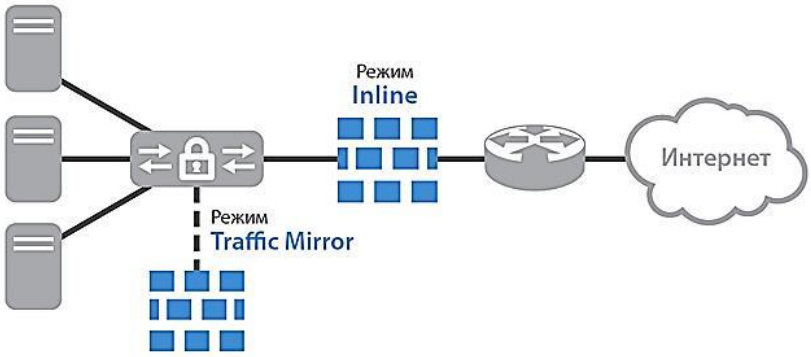

Рис. 3. Принцип роботи системи виявлення сигнатур

Система, що працює на основі перевірки сигнатур, веде загальну базу даних сигнатур атак. Кожна сигнатура - це набір правил, що описують способи боротьби з вторгненнями. Дана система аналізує кожний пакет, що проходить повз неї, порівнюючи його вміст з сигнатурами бази даних. Якщо пакет співпадає з сигнатурою, то генерується попередження. Проте мінусом даного підходу є те, що система безсильна проти незареєстрованих атак, збіг сигнатур може бути зовсім не атакою, а також при порівнянні пакету з величезною колекцією сигнатур система може просто не впоратись з такою роботою і проґавити шкідливі пакети.

Система, що працює на основі виявлення аномалій, створює профіль надійного трафіку, який спостерігається у штатному режимі. Потім вона відстежує такі потоки пакетів, які мають, статичні зміни. Наприклад непропорціональне збільшення пакетів, чи різкий скачок інтенсивності сканування портів. Гарною стороною є те, що вони можуть відстежувати нові, ще не описані атаки, проте з іншої сторони, виключно важко розрізняти нормальній і статично незвичайний трафік.

DDoS атака (рис. 4). Двома основними елементами нейтралізації великомасштабних DDoS-атак є пропускна здатність (або транзитний потенціал) та продуктивність сервера, достатня для поглинання та нейтралізації атак.

Транзитний потенціал. При проектуванні програм необхідно переконатися, що постачальник послуг хостингу надає надмірну пропускну здатність підключення до Інтернету, яка дозволяє обробляти великі обсяги трафіку. Оскільки кінцева мета DDoS-атак – вплинути на доступність ресурсів або додатків, необхідно розміщувати їх поруч не тільки з кінцевими користувачами, але й з великими вузлами міжмережевого обміну трафіком, які легко забезпечать вашим користувачам доступ до програми навіть за великого обсягу трафіку. Робота з інтернет-додатками забезпечує ще більші можливості. У цьому випадку можна скористатися мережами розповсюдження контенту (CDN) та сервісами інтелектуального перетворення адрес DNS, які створюють додатковий рівень мережної інфраструктури для обслуговування контенту та дозволу DNS-запитів з місць, які найчастіше розташовані ближче до кінцевих користувачів.

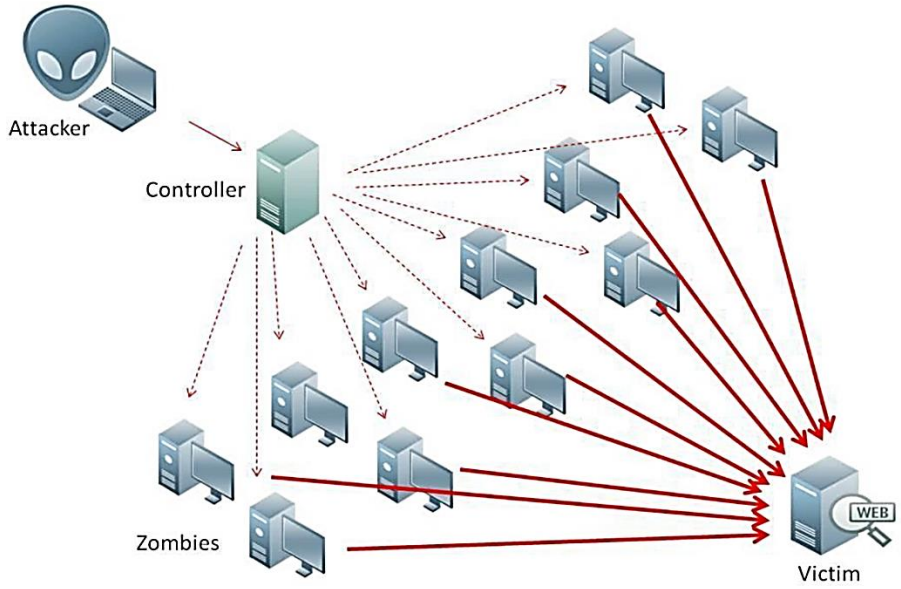

Рис. 4. Приклад DDoS атаки

Продуктивність сервера. Більшість DDoS-атак є об'ємними та споживають багато ресурсів, тому важливо мати можливість швидко збільшувати чи зменшувати обсяг своїх обчислювальних ресурсів. Це можна забезпечити, використовуючи надмірний обсяг обчислювальних ресурсів або ресурси зі спеціальними можливостями, такими як продуктивні мережеві інтерфейси або покращена мережна конфігурація, що дозволяє підтримувати обробку великих обсягів трафіку. Крім того, для постійного контролю та розподілу навантажень між ресурсами та запобігання перевантаженню будь-якого одного ресурсу часто використовуються відповідні балансувальники.

Для того щоб визначити DDoS атаку за допомогою програми можна також відфільтрувати окремі адреси джерел пакетів та проаналізувати окремі їх колонки. Коли виявляється підвищення обсягу трафіку, що потрапляє на хост, як орієнтир можна брати максимально можливий обсяг трафіку, який хост може обробити без погіршення його доступності. Така концепція називається обмеженням швидкості. Більш просунуті методи захисту відповідно мають додаткові можливості і можуть інтелектуально приймати тільки трафік, який дозволено, аналізуючи окремі пакети. Для використання подібних засобів необхідно визначити характеристики хорошого трафіку, який зазвичай отримує цільовий об'єкт, та мати можливість порівнювати кожен пакет із цим еталоном.

Таким чином досліджено - яким способом та чи інша атака може здійснювати вплив на ІС. Тож аналізуючи цей матеріал є можливість розробити методику побудови системи виявлення мережевих вторгнень та виявлення ознак комп’ютерних атак.

Розробка методики побудови систем виявлення мережевих вторгнень і виявлення ознак комп'ютерних атак

Для розробки методики побудови систем виявлення мережевих вторгнень і виявлення ознак комп'ютерних атак в цій статті визначено, що засобами технології виявлення мережевих атак є програмні та апаратні системи виявлення, які функціонують переважно в TCP / IP мережах і базуються на сигнатурних та статистичних методиках виявлення на основі хостових і мережевих моделей. Виявлення атак вимагає виконання однієї з двох умов: або розуміння очікуваної поведінки контрольованого об'єкта системи, або знання всіх можливих атак і їх модифікацій. У першому випадку використовується технологія виявлення аномальної поведінки, а в другому – технологія виявлення зловживань. Застосовувані при виявленні та запобіганні мережевих атак методи і моделі зводяться до мережевого і хостового аналізу сигнатурних і статистичних даних мережевого трафіку з подальшим виведенням засобів виявлення атак про здійснення атаки. До таких висновків відносяться повідомлення на консоль або в журнали засобів виявлення атак про час виявлення, проведення, назви та типу атаки. Результатами роботи засобів виявлення атак є дані про номери пакетів, що містяться в сеансі атаки.

Сигнатурний аналіз і контроль профілів при виявленні комп'ютерних атак включає в себе аналіз заданих заздалегідь послідовностей, як самих аналізованих даних, так і послідовностей дій. Сучасні методики виявлення мережевих атак досить різнорідні і не зведені до єдиного критерію, за яким можливо оцінювати ефективність їх застосування. Таким критерієм може служити повнота охоплення всіх аналізованих параметрів, необхідних для точного і найбільш ймовірного виявлення атаки з мінімально хибним спрацьовуванням.

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 [2].

Методики виявлення і запобігання зводяться до застосування технологій виявлення мережевих атак, які включають в себе програмні та апаратні системи виявлення атак, функціонуючі переважно в *TCP / IP* мережах і базуються на сигнатурних та статистичних методиках виявлення атак, на основі хостових і мережевих моделей, результатом яких є виявлення атак з метою автоматизації забезпечення захисту локальної обчислюваної мережі (ЛОМ). У таких методиках спільною рисою з формальної точки зору є те, що існує кілька підходів подання повідомлень про виявлені атаки. При виявленні мережевих атак в основному застосовуються методики, узагальнення приватних рішень, які будуються з використанням різноманітних методів і технологій.

Підсистема системи виявлення вторгнень передає в систему підтримки рішень вектор виду:

$$S = \left(A, C, G, T, M, P, P_н, P_в\right) \tag{1}$$

де A – системний ідентифікатор виявника атаки,

C – ідентифікатор виявленої атаки,

G – вид атаки,

T – системний час атаки,

M – ідентифікатор методу, яким виявлена атака,

P – вірогідність проведення атаки,

$P_н$ – нижня межа ймовірності атаки,

$P_в$ – верхня межа ймовірності атаки.

Подальша обробка проводиться роздільно для кожного з видів атак. Тимчасова вісь t розбивається на інтервали аналізу Δt. Довжина інтервалу Δt визначається виходячи з типу атаки і швидкості її виявлення підсистемами СВВ. У кожному інтервалі проводиться аналіз повідомлень з метою оцінки узагальненої ймовірності атаки. У ряді робіт, виконаних у суміжних областях, показано, що вироблення оптимального методу об'єднання статистичних гіпотез про виявлення різнорідних об'єктів в практичній ситуації неможлива. Для систем виявлення атак це пояснюється відсутністю даних про апріорні ймовірності атак різних видів, різною природою проаналізованих ознак, неможливістю оцінки спільних рис розподілу значень цих ознак, рознесенням в часі моментів повідомлень про атаки [7].

Збільшення ймовірності виявлення атаки веде до зростання ймовірності „помилкової тривоги". Для того щоб ймовірність „помилкової тривоги" залишалася в допустимих межах, пропонується використовувати мажоритарний критерій для прийняття рішень. Якщо в системі присутні кілька виявників атак, які виявлятимуть заданий вид атаки, то рішення про наявність атаки приймається в випадку, якщо вона виявлена більш ніж половиною СВА.

Розвитком мажоритарного підходу є вимоги трудомісткої експертної роботи та застосування при обчисленні ймовірності атаки апріорної інформації про властивості підсистем, які реалізуються на основі обчислення зваженої суми значень P_i, де в якості ваги застосовується ступінь довіри до того чи іншого виявника (підсистемі СВВ) при розгляді даної конкретної атаки. Тоді ймовірність виявлення атаки (класу або групи атак) k може бути представлена виразом:

$$P_{КОБ}(\Delta t_i) = \sum_{j=1}^{m} W_{kj} \cdot P_{kj}, \tag{2}$$

де m – число аналізаторів, що використовуються в СВВ,

P_{kj} – ймовірність атаки k, передана j-м аналізатором на інтервалі Δt_i,,

W_{kj} – ступінь довіри результатам роботи аналізатора j при виявленні k атаки , причому:

$$\sum_{j=1}^{m} W_{kj} = 1$$

Якщо повідомлень про атаки в інтервалі аналізу Δt_i не зафіксовано, то: $P_{КОБ}(\Delta t_i) = 0$.

Відповідно застосування ймовірнісної оцінки виявлення атак, залежить від числа аналізаторів, ймовірності атаки і ступеня довіри аналізаторам при виявленні атаки. Для опису платформи безпеки (ПБ) розподілених ІС використовують формалізм семантичних мереж фреймів [7]:

В основі мережевих моделей лежить конструкція виду 3:

$$H = \{I, C_1, C_2, ..., C_n, \Gamma\}, \tag{3}$$

де: I – множина інформаційних одиниць,

C_i, C_2, ..., C_n – множина типів зв'язків між елементами;

Γ – відображення, що задає зв'язок з прийнятого набору між інформаційними одиницями.

Проведена робота показала, що системи виявлення вторгнень, які використовуються на сьогодні, значною мірою базуються на емпіричних схемах. Тому, проаналізувавши структури СВВ, методи, які використовуються, їх переваги та недоліки, проаналізувавши підходи до розробки СВВ можна зробити висновок, що в подальшому, орієнтуючись на проведене дослідження, можна буде налаштувати якісну та надійну систему для впевненості, що конфіденційна інформація яка обробляється різними інформаційними процесами не буде змінена, викрадена або спотворена.

Приклад системи виявлення мережевих вторгнень і виявлення ознак комп'ютерних атак для підприємства.

В ході проведення дослідження пропонується ешелоноване рішення віртуальної компанії яка є інтегратором новітніх технологічних рішень для бізнесу, що пропонує інтегрувати та налаштувати мережеве обладнання передових виробників (Cisco Systems, Aruba Networks та інших), що забезпечує максимальний захист серверів та баз даних [8].

В системі реалізована як технологічна, так і експлуатаційна безпека. Реалізація вимог технологічної та експлуатаційної безпеки яка ґрунтується на спеціально розробленому для мережі комплексі організаційних, організаційно-технічних і технічних заходів щодо захисту інформації та ресурсів мережі. Необхідно розглянути типовий варіант побудови корпоративної системи безпеки з урахуванням рекомендації SAFE компанії на базі корпоративної СВВ Cisco Systems (рис. 5).

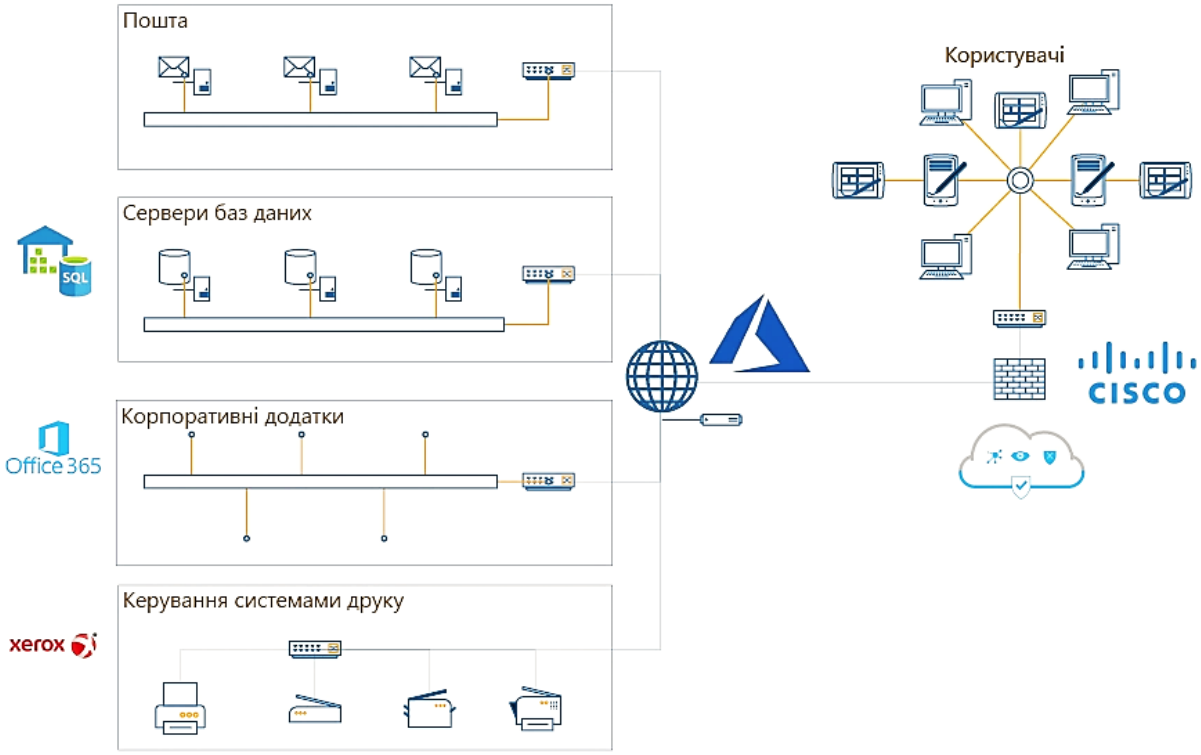

Рис. 5. Загальна схема побудови СВВ

Для побудови такої системи в центральному офісі рекомендується використовувати моделі «міжмережевих екранів» з функцією резервування серій Cisco PIX-515E, Cisco PIX-525 або Cisco PIX-535 з підтримкою декількох портів Fast Ethernet або Gigabit Ethernet. Міжмережеві екрани цієї серії дозволяють здійснювати гнучке налаштування політик безпеки, створення великої кількості нейтральних зон (DMZ), поряд з високою продуктивністю і надійністю цього критичного вузла мережі. У нейтральних зонах традиційно розміщують важливі вузли корпоративної мережі, сегмент доступу до корпоративної мережі, сегмент віддаленого доступу клієнтів або користувачів мережі та ін.

З метою забезпечення комплексного управління всіма елементами забезпечення безпеки рекомендується використання спеціалізованої системи управління Cisco VPN Management Solutions (VMS), що розміщується в зоні DMZ 1 «Сервери аутентифікації і управління». Для забезпечення аутентифікації користувачів, мережевих пристроїв використовуються сервера аутентифікації. Наприклад, Cisco ACS розміщується в зоні DMZ 1 «Сервери аутентифікації і управління». Для підключення користувачів корпоративної мережі також рекомендується використовувати підключення в окрему демілітаризовану зону, що дозволить забезпечити необхідний рівень внутрішньої безпеки мережі («Маршрутизатор КС»). Для організації підключення віддалених мобільних користувачів, рекомендується використання зовнішнього VPN концентратора, Cisco PIX Firewall або маршрутизатора зі спеціалізованим ПЗ в центральному офісі та програмне забезпечення Cisco VPN клієнтів, на робочих місцях користувачів, що дозволяє забезпечити безпечне і захищене підключення, в тому числі і по публічним каналам зв'язку Інтернет, з організацією шифрованих IPSec тунелів.

Слід зазначити, що дане рішення є дійсно типовими і в реальних проектах можливе використання інших схем і методик забезпечення безпеки в залежності від бажаного результату, поставлених цілей і бюджету проекту.

Висновок

Безпека мереж і мережевих сервісів стала дійсно нагальною проблемою практично кожного користувача підприємства. Тож в статті були розглянуті характеристики та методи систем виявлення мережевих вторгнень і виявлення ознак комп'ютерних атак на підприємстві які дозволили детально вивчити як саме зможуть діяти зловмисники та якими способами центр інформаційної безпеки зможе протидіяти атакам на інформаційну мережу. Проведення даного дослідження та обробка результатів показало можливості для здійснення оптимального вибору засобів для комплектування перспективної системи та підтвердило важливість встановлення підтримуючої системи яка в моменти атаки буде здатна протидіяти або стримувати можливих порушників.

Перелік посилань

1. Головний сайт центру виявлення кіберзагроз URL: http://cert.gov.ua
2. Завада А. А. Аналіз сучасних систем виявлення атак і запобігання вторгненням / А. А. Завада, О. В. Самчишин, В. В. Охрімчук // Інформаційні системи. Житомир: Збірник наукових праць ЖВІНАУ, 2012. Т. 6, No 12. С. 97-106. URL: http://ela.kpi.ua/bitstream/123456789/17609/1/meshkov.pdf
3. Толюпа С. В., Плющ О. Г., Пархоменко І. І. Побудова систем виявлення атак в інформаційних мережах на нейромережевих структурах / Толюпа С. В., Плющ О. Г., Пархоменко І. І.// К.:К1БЕРБЕЗПЕКА: освіта, наука. Техніка № 2 (10), 2020. С.169-181. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/217/194
4. Колодчак О. М. Сучасні методи виявлення аномалій всистемах виявлення вторгнень / О. М. Колодчак // Вісник Національного ун-т «Львівська політехніка».
5. Олифер В. Компьютерные сети. Нисходящий подход. / В. Олифер, Н. Олифер, Д .Куроуз, К. Росс.//. URL: https://holodoks.blogspot.com/2017/12/blog-post.html
6. 6Литвинов В. В. Аналіз систем та методів виявлення несанкціонованих вторгнень у комп'ютерні мережі /В. В. Литвинов, Н. Стоянов, І. С. Скітер, О. В. Трунова, А. Г. Гребенник// М.: – 2018. URL: http://www.immsp.kiev.ua/publications/articles/2018/2018_1/01_2018_Lytvynov.pdf
7. Радченко М. М. Аналіз системи виявлення вторгнень та комп'ютерних атак / М. М. Радченко, О. І. Іванов, С. І. Прохорський, К. К. Мужеський// М.: 2013. URL: https://revolution.allbest.ru/programming/00880596_0.html
8. Сєвєрінов О. В. Аналіз сучасних методів атак на автоматизовані системи управління військами та інформаційні мережі /О. В. Сєвєрінов, А. Г. Хрєнов, А. О. Поляков //. Харків: Системи обробки інформації, випуск 9, 2015 - С.101-104
9. Отчет: 2021 год стал рекордным по количеству кибератак в мире URL: https://hightech.fm/2021/10/06/hacker-attack-year

Надійшла: 21.05.2022 Рецензент: д.т.н., професор Савченко В.А.