*Насипаний А.*

*Науковий керівник – проф. Горбатюк Р. М.*

# УДОСКОНАЛЕННЯ СПОСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ ВІД КОМП'ЮТЕРНИХ ВІРУСІВ

Створення високоефективних і багатофункціональних інформаційних систем дозволяє на сьогоднішній день реалізувати їх в самих різних сферах життя сучасного суспільства. Інформаційні системи дозволяють автоматизувати та підвищити ефективність обробки інформації шляхом застосування відповідного програмного і апаратного забезпечення. Проте використання ІС одночасно загострює і проблеми захисту ресурсів цих систем від загроз інформаційної безпеки. Для протидії інформаційним атакам в даний час все частіше застосовуються спеціальні системи захисту – системи виявлення вторгнень.

**Актуальність дослідження.** В даний час інтенсивна поява і розростання інформаційного простору призводить до необхідності контролювати і управляти процесами, які протікають в ньому. Для цього використовується, так звана, інформаційна зброя, яка представляє собою засоби знищення, перекручення або розкрадання інформації; обмеження санкціонованого допуску користувачів. Обороноздатність від такої атакуючої інформаційної зброї як комп'ютерні віруси, засоби придушення інформаційного обміну в телекомунікаційних мережах, фальсифікації інформації в каналах державного та військового управління, безпосередньо залежить від правильності і надійності систем мережевого захисту інформації, у тому числі засобів виявлення і запобігання мережевих атак.

Звісно, в сучасних операційних системах та іншому програмному забезпеченні використовуються технології, що забезпечують безпеку системи та попереджують про її можливий вихід із ладу. Але, як свідчить світовий досвід, цього не достатньо для забезпечення оперативного реагування на комп'ютерні атаки. Перегляд докладного звіту подій в системі виявлення вторгнень вручну через консоль це трудомісткий рутинний процес, що уповільнює аналіз даних та реагування на події в системі виявлення вторгнень. У зв'язку з цим розробка графічних інтерфейсів розподілених систем виявлення комп'ютерних атак із використанням методів візуалізації даних, набуває все більшого та перспективного розмаху у інформаційних технологіях.

Усе вище наведене дозволяє зробити висновок щодо необхідності підвищення ефективності роботи адміністратора безпеки інформаційної мережі за рахунок автоматизації процесів обробки та аналізу даних, що поступають з підсистеми моніторингу даних шляхом побудови та впровадження підсистеми взаємодії адміністратора безпеки з системою виявлення вторгнень Prelude.

**Мета роботи-** розробити спеціальне програмне забезпечення у вигляді інтерфейсного модулю взаємодії користувача з системою виявлення вторгнень Prelude та впровадженням в процес діяльності адміністратора безпеки методів інтелектуального аналізу даних, які збирає система виявлення вторгнень.

В даній статті знайдено опис функціональних можливостей системи Prelude, та опис можливостей для удосконалення.

Система Prelude є системою з відкритими вихідними текстами. початок розробки – 1998 рік. Вона спочатку замислювалася як гібридна СВВ, яка могла б допомогти адміністратору мережі відстежувати активність як на рівні мережі, так і на рівні окремих вузлів. Система розподілена і складається з наступних компонентів [8]:

- мережеві сенсори – різні сенсори, що аналізують дані на рівні мережі на основі сигнатурного аналізу. Сенсори генерують повідомлення про виявлення атак і відправляють їх модулям управління. Система Prelude використовує в якості мережевого сенсора систему Snort;
- вузлові сенсори – різні сенсори рівня системи, що аналізують журнали реєстрації ОС, додатків. Сенсори генерують повідомлення про виявлення аномалій і відправляють їх модулям управління. Існуючий набір сенсорів дозволяє аналізувати дані журналів реєстрації таких систем і додатків, як міжмережевий екран IPFW, що входить до складу ОС FreeBSD, NetFilter ОС Linux 2.4.x, маршрутизатори Cisco і Zyxel, GRSecurity, і типові сервіси операційної системи UNIX;
- модулі управління – процеси , які отримують і обробляють повідомлення сенсорів. Розрізняють наступні види модулів управління:

 модулі журналізації – відповідають за реєстрацію повідомлень в журналах реєстрації або базах даних. В даний час реалізовані модулі для MySQL, PostgreSQL;

 модулі реагування – аналізують повідомлення і генерують можливу відповідну реакцію СВВ на атаку. Можливі такі види реакції як блокування порушника на міжмережевому екрані (NetFilter, IPFilter). Надалі можливі такі типи реакції як ізоляція порушника і звуження пропускної здатності каналу порушника;

 агенти реагування – реалізують згенеровану менеджером реакцію на атаку інформаційної мережі.

Пропонується, досить гнучка система конфігурації і широкі можливості налаштувань. При першому знайомстві з програмою, система налаштування дається не відразу, але при подальшому знайомстві з налаштуваннями і документацією по ним, як виявилося не є дуже складною і відкриваються широкі можливості моніторингу. Оскільки ця IDS в останні роки практично не розвивається, то на даний момент «web-візуалізація» для конфігурації від розробників відсутня, але є варіанти розроблені сторонніми програмістами.

СВВ Prelude дозволяє:

 реагувати в режимі реального часу на внутрішні і зовнішні загрози;

 збирати, аналізувати і готувати звіти про стан РІС;

 проаналізувати дані, які стосуються безпеки подій;

 сприяти дотриманню нормативних вимог;

 уникнути пошкодження даних і ресурсів компанії;

 забезпечити сумісність внутрішніх та зовнішніх політик безпеки;

 отримувати інформацію про потенційні загрози і підозрілі події в ІМ;

 негайно встановити причинно-наслідкові зв'язки між інформацією і подіями та їх наслідками;

 контролювати мережеву активність і управляти ризиками в оптимізованому режимі.

Адміністратори безпеки використовують системи виявлення вторгнень як інструмент управління безпекою інформаційної мережі, тому доцільно для полегшення роботи та пришвидшення реагування на події в СВВ використовувати методи візуалізації даних для покращення аналізу інформації. Візуальне представлення даних є набагато інформативнішим за інші методи отримання та сприйняття інформації, більш зручним і легшим для сприйняття та розуміння ніж наприклад представлення даних у таблицях, схемах, математичних матрицях, або просто в числах.

**Висновки.** Отже, в сучасних умовах постійного зростання інтенсивності атак на інформаційно-телекомунікаційні системи важливе місце в системі інформаційної безпеки відводиться системам виявлення вторгнень. На сьогоднішній день неможливо організувати ефективний захист інформації без використання СВВ. У результаті проведеного дослідження було розроблено удосконалену структуру системи виявлення вторгнень Prelude, яка включає графічну підсистему взаємодії адміністратора безпеки з системою. Операції обробки великої кількості подій щодо реагування на невідомі досі події в системі виявлення вторгнень вручну є трудомістким рутинним процесом, що уповільнює роботу адміністратора безпеки. Тому розроблене програмне забезпечення дозволяє підвищити обгрунтованість рішень, які приймає адміністратор безпеки під час аналізу ситуацій щодо виявлення вторгнень в інформаційну мережу.

**Перспективи подальших досліджень** полягають у використанні системи Prelude на підприємствах, державних установах, де є власна локальна комп’ютерна мережа і потреба у захисті інформації.

**ЛІТЕРАТУРА:**

1. ЛукацкийА.В. Обнаружение атак / ЛукацкийА.В. – СПб. : БХВ –Петербург, 2003. – 256 с.
2. Норткат С.А. Обнаружение нарушений безопасности в сетях. / Норткаг С.А. / Пер. с англ. – М.:ДМК Пресс, 2003. – 200 с.
3. Хоменко Д.О. Система виявлення вторгнень Prelude. Тактико-технічні характеристики. Шляхи удосконалення / Хоменко Д.О. / XIII воєнно-наукова конференція курсантів (студентів) – К: ВІТІ ДУТ. – 2014. – 24 с.
4. Сердюк В.А. Перспективы развития новых технологий обнаружения информационных атак / В.А. Сердюк // Системы безопасности связи и телекоммуникаций. – 2002. – №5. – С.5–7.
5. Пауер Р.А. Експерти дискутують про сьогодення і майбутнє систем виявлення атак / Пауер Р.А.; пер. з англ. О.І. Лукацкого. – Днепропетровск : Computer Security Journal, 2002. – XIV, 10 с.

6. Біячуєв Т.А. Безпека корпоративних мереж. / під ред. Л.Г.Осовецкого – СПб: СПб ГУ ІТМО, 2004.– 161 с.

*Оліяр О.*

*Науковий керівник – доц. Франко Ю.П.*

## СТВОРЕННЯ СИСТЕМИ ВІЗУАЛІЗАЦІЇ ТА МОДЕЛЮВАННЯ БЕЗПРОВІДНИХ СЕНСОРНИХ МЕРЕЖ

З розвитком науки та технологій відкрились нові перспективи у сфері збирання, передавання та обробки інформації. В даний час одним з нових актуальних напрямків в області інформаційних технологій є створення нового виду мережевих систем - сенсорних мереж (СМ, англ. - WSN). Безпровідна сенсорна мережа (WSN – Wireless Sensor Network) - це розподілена, самоорганізована, стійка до відмов елементів система, що складається з багатьох вузлів, з'єднаних між собою радіоканалом. Безпровідникова сенсорна мережа може розміщуватись на практично необмеженій території і за сучасними оцінками може містити до 65000 вузлів.

Безпровідні сенсорні мережі (Wireless Sensor Network) складаються з маленьких вузлів (сенсорів), з інтегрованими функціями моніторингу навколишнього середовища, обробки і передачі даних.

**Актуальність дослідження.** Задача візуалізації графових структур БСМ є надзвичайно актуальною та потребує з кожним роком більш якісного розв'язку. Адже із розповсюдженням Web-технологій, розвитком нових напрямків у науці та впровадженням новітніх підходів до організації освітнього і управлінського процесів, все частіше і частіше виникає потреба у графічному представленні графових структур даних різного походження. Особливо актуальною ця задача стає при потребі візуалізації структур значних розмірів – зокрема при вирішенні різнорідних проблем наукового, корпоративного та навіть державного характеру. Актуальність даної теми додатково підсилюється тим, що вона не є вузько спеціалізованою, тобто не орієнтована для застосування лише у певній галузі або сфері, а навпаки є легко застосовною в багатьох галузях людської діяльності. Програмне забезпечення для візуалізації графових структур БСМ створюється з метою вирішення цих проблем.

В загальному проектування і реалізація сенсорних мереж потребують вирішення безлічі складних проблем, що відносяться до різних областей досліджень.[5]

**Аналіз останніх досліджень та публікацій.** Дослідження і розробки в області СМ інтенсивно ведуться за межами нашої держави, причому результати останніх вже використовуються в конкретних програмах. Найбільш успішними дослідженнями в цій галузі були дослідження професора університету штату Каліфорнія - Крістофера Пістера.

Тематика робіт простягається від вузькоспеціальних питань, пов'язаних зі створенням окремих компонентів об'єктів мережі (мікроконтроллерів, датчиків і т.д.) з низькою ціною і низьким енергоспоживанням до проблем, які виникають при експлуатації сенсорних мереж (питання пов'язані з організацією роботи мережі, розробка програмного забезпечення, прив'язка місця розташування об'єктів мережі до географічних координат та ін.) [7].

Результатом робіт по стандартизації БСМ стало сімейство стандартів IEEE 802.15.4.

БСМ як системи моніторингу параметрів об'єктів на базі дискретних бездротових сенсорних мереж описані в роботах М. Н. Терентьєва. Вирішенням завдань, пов'язаних з оцінкою, аналізом і ефективним управлінням інформаційними потоками в БСМ, займалася І. А. Іванова.

Дослідженню енергоспоживання та створенню програмних і апаратних засобів БСМ велику увагу приділяє американська компанія Texas Instruments (радіомодулі CC2530 та ін.). Також виробництвом радіомодулей займаються компанії Atmel, Digi International, Ember, Freescale, Samsung, STMicroelectronics, Microchip Zigbee [3].

**Мета статті** – вивчення та обґрунтування функціональних можливостей комп'ютерних технологій для моделювання та візуалізації сенсорних мереж.

Для досягнення мети необхідно розробити узагальнений алгоритм реалізації модифікованого пружинного методу, який, порівняно з оригінальним методом, дозволяє отримувати простіші для сприйняття подання графів за рахунок зменшення кількості перетинів ребер шляхом уникнення локальних мінімумів енергії фізичної системи.

**Виклад основного матеріалу.** Візуалізація складних концептуальних структур є ключовою компонентою в багатьох додатках в науці і техніці. Граф– це абстрактна структура, яка