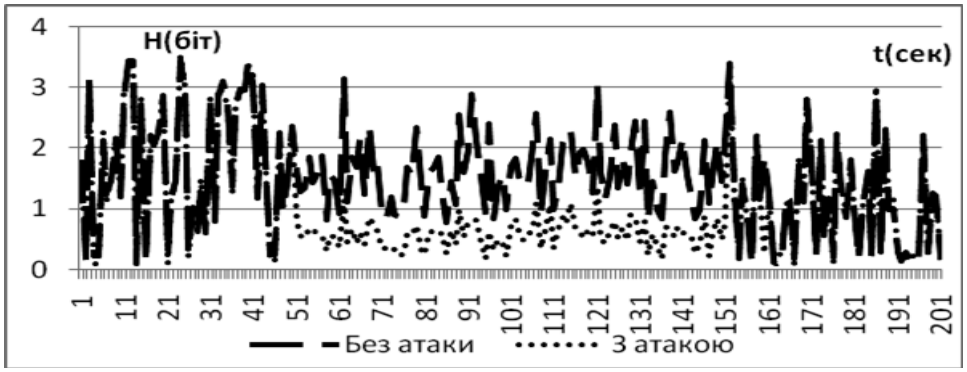


Рис. 4. Графік зміни значень ентропії

Таким чином, обчислення ентропії трафіку методом часового вікна та моніторинг кількості пакетів у часовому вікні можна використовувати для аналізу мережевої активності у режимі, наближенному до режиму реального часу,з метою виявлення мережевих аномалій.

Список літератури

1. Leland W.E., Taqqu M.S., Willenger W., Wilson D.V. On the Self-Similar Nature of Ethernet Traffic.IEEE Transactions on Networking, 1994, v. 2, Feb. p.1 – 15.

2. Feinstein L., Schnackenberg D. Statistical Approaches to DDoS Attack Detection and Response. Proceedingsof the DARPA Information Survivability Conference and Expostion (DISCEX'03), April 2003.

3. Борисов Д.Н. Энтропия как индикатор возникновения аномалий сетевого трафика. НауковіпраціДонНТУ, 2007, випуск 118, с. 43 – 49.

4. W.Lee, D.Xiang. Information-Theoretic Measures for Anomaly Detection.Conference: IEEE Symposium on Security and Privacy. – 2001, 130 – 143 p.

5. Шеннон К. Работы по теории информации и кибернетике. М.: Иностранная литература, 1963. – 830 с.

## РИСКИ, СВЯЗАННЫЕ С ПЕРЕНОСОМ РЕСУРСОВ В ВИРТУАЛЬНУЮ ИНФРАСТРУКТУРУ

О.Г. Горяная
(Украина, Днепропетровск, ГВУЗ «Национальный горный университет»)

Одна из основных характеристик виртуальной среды – динамичность – является как преимуществом для эксплуатирующих служб, позволяющим быстро выполнять операции развертывания и миграции виртуальных машин, так и недостатком для служб информационной безопасности, поскольку именно с этим связаны основные риски в виртуальной среде.

Перенеся производственные серверы на виртуальную платформу, нам следует осознать, что:

– ОС, приложения и данные больше не привязаны к одной физической платформе. Нельзя точно сказать на каком именно сервере работает то или иное приложение.

– Администратор может осуществить копирование/клонирование виртуальных машин и целых томов данных.

– Стандартные средства мониторинга и журналирования легко обойти. Ведь операционная система не сможет сообщить о том, что ее целиком клонировали или остановили средствами гипервизора [1].

**Гипервизор и средства управления**

Виртуальная инфраструктура помимо новых возможностей, несет еще и новые компоненты, по отношению к традиционной физической инфраструктуре. Этими компонентами являются собственно серверы виртуализации, а также средства управления и обслуживания виртуальной инфраструктуры.

Поскольку появились новые программные компоненты, то появляются вопросы обеспечения их безопасности. Более того, с точки зрения информационной безопасности, ценность всех новых компонентов крайне высока. Причины тут две:

1. Захват гипервизора или средств управления виртуальной инфраструктурой злоумышленником приведет к тому, что он сможет абсолютно незаметно для традиционных средств защиты информации (установленных в виртуальной машине) перехватывать данные, идущие через устройства ввода-вывода. Кроме конфиденциальности данных, он, разумеется, также сможет нарушить целостность и доступность виртуальных машин.
2. Поскольку основная концепция виртуализации состоит в консолидации информационных систем на одном оборудовании. Следовательно, вместе с плотностью растут и ставки потерь. Компрометация хоста будет приводить к компрометации всех виртуальных машин на нем, а захват централизованных средств управления виртуальной инфраструктуры, очевидно, приведет к компрометации всех виртуальных машин в рамках инфраструктуры.[2]

**Способы выявления инцидентов в виртуальной инфраструктуре**

Основное отличие при выявлении инцидентов в физической и виртуальной среде состоит в том, что в последней нельзя полагаться лишь на привычные механизмы журналирования и аудита гостевых ОС и приложений.

Для выявления подобных инцидентов необходимо производить мониторинг и аудит следующих компонентов:

– Гипервизора на уровне его ОС (ESX). Системные события, как правило, низкоуровневые и их невозможно напрямую связать с активностью на уровне виртуализации (копирование, перемещение виртуальных машин и т.д.), однако это необходимо для выявления сбоев, перезагрузок ESX-серверов и аутентификации в консоли ESX.

– Уровня виртуализации.

– Гостевой ОС и интересующих приложений.

– Физической инфраструктуры, обслуживающей виртуальные датацентры.

Кроме мониторинга, необходимо также реализовать правила выявления специализированных инцидентов, присущих виртуальной среде, то есть понять

логику проведения атак, подобных описанным выше, и, соответственно, формализовать правила их обнаружения.

Список литературы
1. http://www.virtualizationsecuritygroup.ru/publikatsii/obnaruzhenie-incidentov.html
2.http://www.virtualizationsecuritygroup.ru/publikatsii/bezopasnost-virtualnih-infrastruktur.html
3. http://www.virtualizationpractice.com

## МОДЕЛЮВАННЯ СИСТЕМИ ЗАХИСТУ З ВИКОРИСТАННЯМ МОДЕЛІ ГІПЕРГРАФІВ

Т.В. Бабенко, О.І. Авчиннікова
(Україна, Дніпропетровськ, ДВНЗ «Національний гірничий університет»)

Для математичного моделювання дискретних слабо структурованих процесів та систем, в яких присутня множина критеріїв, стохастичність, інтервальність одним з найбільш підходящих математичних інструментаріїв структурування об'єктів моделювання є інструментарій теорії гіперграфів [4].

Під даний різновид процесів може підпадати процес аналізу захищеності об’єкта інформаційної діяльності, що базується на структуруванні багатьох критеріїв.

Згідно [2,3], гіперграф – це таке узагальнення простого графа, коли ребрами можуть бути не лише двоелементні, а й будь-які підмножини вершин.

Нехай $V$ – кінцева непуста множина, $\mathcal{E}$ – деяке сімейство непустих (необов'язково різних) підмножин множини $V$. Пара $H = (V, \mathcal{E})$ називається гиперграфом з множиною вершин $V$ та множиною ребер $\mathcal{E}$.

Множину відносин "об'єкт-загроза" можна відтворити за допомогою гіперграфа$H = (O, T)$, рисунок 1, в якому множина вершин $O = \{o_1, \dots, o_5\}$ позначає множину об’єктів захисту, множина ребер $T = \{t_1, \dots, t_8\}$ позначає множину загроз, спрямованих на об’єкт захисту $o_i$.

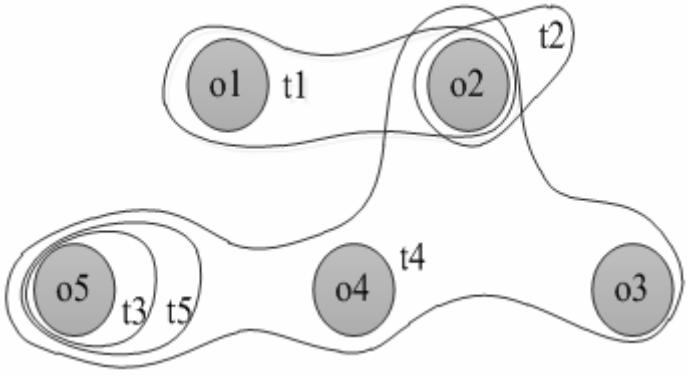


Рис. 1. Гіперграф $H = (O, T)$, діаграма Венна