El futuro sique siendo inseguro, ya que los ´más grandes´, no pueden prometer mantener el marco de regulación financiera, incluyendo el capital bancario, estándares de liquidezm así como medias para regular y resolcer efectivamente instituciones financireas de naturaleza sistémica, complementadas con unsa sepervisión más efectiva.

Bibliografia:

1. http://www.elcorreo.com/agencias/20101112/mas-actualidad/mundo/declaracion-final-lideres-tras-cumbre_201011121442.html
2. http://www.europarl.europa.eu/intcoop/eurolat/committees/trade/meetings/2010_13_15_05_seville/work_doc_dario_v2/814350es.pdf-mirarlo
3. http://www.bancomundial.org/temas/crisisfinanciera/
4. http://www.elpais.com/articulo/economia/global/decoupling/elpepuecong/20080302elpnegeco_5/Tes

Су Цзюнь
Тернопольский национальный экономический университет
Украина, г. Тернополь
Университет Янцзы, Китай, г. Цзинчжоу
sjhosix@gmail.com

ИММУННАЯ СИСТЕМА ДИНАМИЧЕСКОЙ БЕЗОПАСНОСТИ КОМПЬЮТЕРНОЙ СЕТИ

Хотя динамическую безопасность сети считают известной и достаточно изученной проблемой [1], сегодня безопасность компьютерных сетей подвергается новому виду распределенных DoS атак, которые часто достигают своей цели. Для того чтобы справиться с этой новой угрозой, автором представлено новую распределенную структуру безопасности – иммунную систему динамической безопасности сети (Dynamic Network Security Immune System, DNSIS), основанную на динамических сетях.

Кроме обнаружения любых DoS атак в том числе новых типов вирусов-червей, DNSIS также имеет высокий уровень обнаружения с низким уровнем ложных срабатываний. При этом может быть решена проблема проникновения атакующих пакетов и распространения червей между компьютерами, подключенными к тому же коммутатору. Механизмы DNSIS ответа на нападение включают фильтр вредоносных пакетов, обновление базы данных сигнатур и систему восстановления, которые функционируют автоматически подобно иммунной системе живых созданий.

DNSIS содержит брандмауэр, группы систем определения обнаружения (IDS), сервер менеджер, динамический маршрутзатор, динамический коммутатор, статический коммутатор и компьютеры. Эти компоненты обеспечивают такие сетевые услуги как служба фильтров, служба основных фильтров, служба тревоги, служба обнаружения и PLAN сервис интерпретатора (рис.1).

Автором предложен алгоритм динамического обнаружения на внешнюю компьютерную сеть, который можно иллюстрировать следующими шагами:

1. Сканирование и атакующих пакетов из внешней сети.

2. Межсетевые экраны могут предотвратить большинство вредоносных пакетов, так как их источник или адрес назначения или порт является незаконным.

3. Сервис выявления передает команду в фильтр служб (на том же динамическом узле) заблоковать пакет сразу при обнаружении вредоносных пакетов.

4. Сервис выявления отправляет сигнатуры пакета серверу – менеджеру.

5. Сервис управления обновляет подписи на IDS и базе данных брандмауэра при получении подписи.

6. Сервер – менеджер формирует команду сервисам основных фильтров блокировать эти пакеты, с тем чтобы решить проблемы пропускной способности вызванные атакующими пакетами.

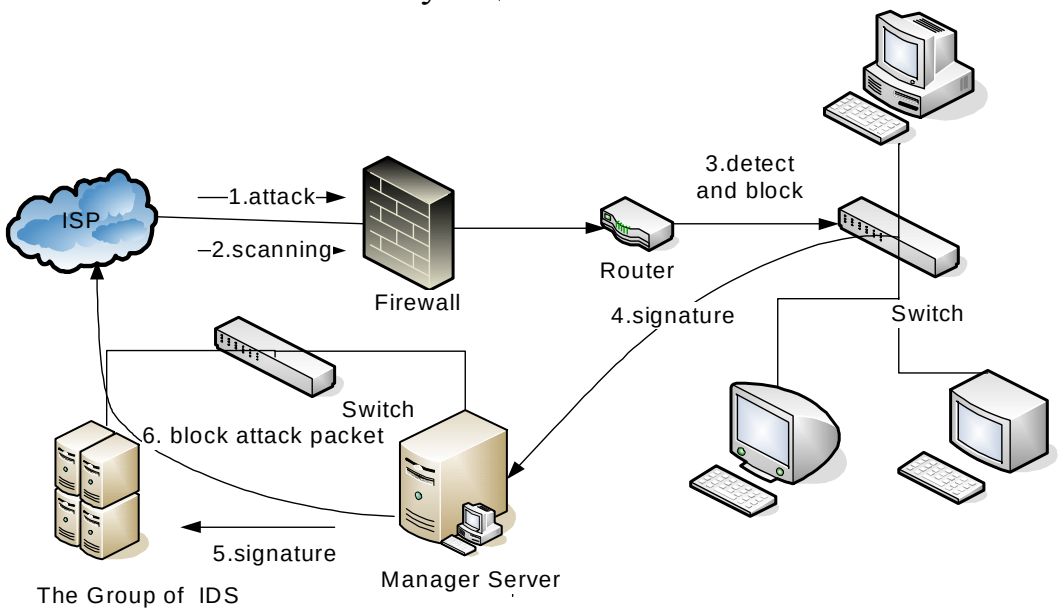

Рис.1 Иммунная система динамической безопасности сети.

Предлагаемый подход имеет высокий уровень обнаружения с таким механизмом реакции как динамические сетевые системы. При этом могут быть обнаружены новые нападения, с использованием неизвестных ранее вирусов-червей, и решить данную проблему не под силу даже типичным системам обнаружения вторжения. Экспериментальные результаты пока-

зывают, что предлагаемые сервисы тестирования и фильтры могут блокировать действие всех вирусов, без каких-либо ложных пакетов. Таким образом, разработанная DNSIS является совместимым, масштабируемым и практическим инструментом компьютерной сети, который может применяться в различных сферах, в том числе в экономических системах. При этом не только существенно повышается безопасность компьютерной сети, но и сокращаются расходы на управление и техническое обслуживание.

Литература:

1. Kai Hwang. Micro-Firewalls for Dynamic Network Security with Distributed Intrusion Detection / Kai Hwang Muralidaran Gangadharan // Proceedings of the IEEE International Symposium on Network Computing and Applications (NCA'01). ─ Cambridge (Massachusette), 2001. ─ P. 68-79.

Ярослав Мех, *к.е.н., професор*
Роман Чорний, *к.е.н., доцент*
Тернопільський національний економічний університет
м.Тернопіль, Україна

СОЦІАЛІЗАЦІЯ СИСТЕМИ ОБЛІКУ В КОНТЕКСТІ КОНТРОЛЮ ЗА ВИКОРИСТАННЯМ ВНУТРІШНІХ РЕЗЕРВІВ ПІДПРИЄМСТВ

У загальному вигляді проблема може бути сформована так – сучасний облік у сфері виявлення і використання внутрішніх резервів на підприємстві, як форма прояву суспільного призначення не виконує контрольну функцію, внаслідок чого облікова інформація втратила соціальне значення. Необхідністю є поєднання функцій обліку між собою, що дозволить найбільш повно реалізувати завдання, поставлені суспільством перед бухгалтерським обліком взагалі, вдосконалити нормативне регулювання та забезпечити захист суспільних інтересів. Зрозуміло, що така постановка проблеми зумовлює її тісний зв'язок як з питанням змісту і способів формування інформаційних систем, функціями управління, так і системою обліку – об'єктивного і незалежного джерела наповнення інформаційних систем.

Вирішення наукової проблеми, яка полягає у невідповідності існуючих теоретико-методологічних основ бухгалтерського обліку використання внутрішніх резервів на підприємстві сучасним економічним реаліям глобального ресурсозбереження, економії тощо, сприятиме необхідності розробки нової концепції обліку і внутрішньогосподарського контролю,