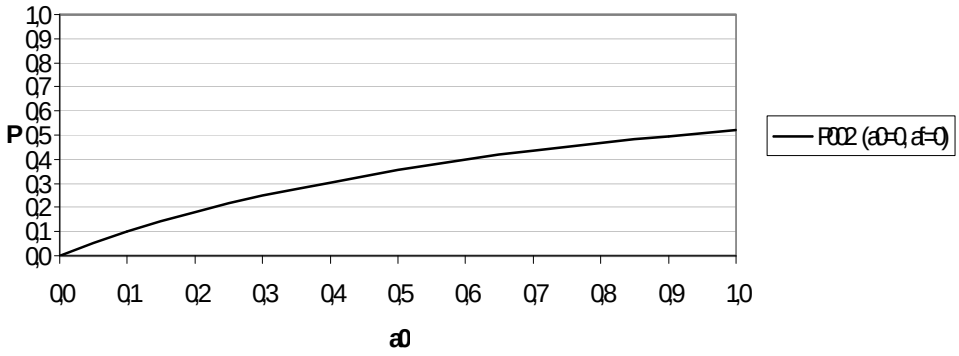

Рисунок 5

Графік на рисунку 6 відображає зміну ймовірності відбраковки фільтра , залежно від інтенсивності впливу негативного фактору, при завантаженій ($\lambda 1=0,9$) та незавантаженій ($\lambda 1=0,1$) системі.
(Рх2х- ймовірність відбраковки фільтром).

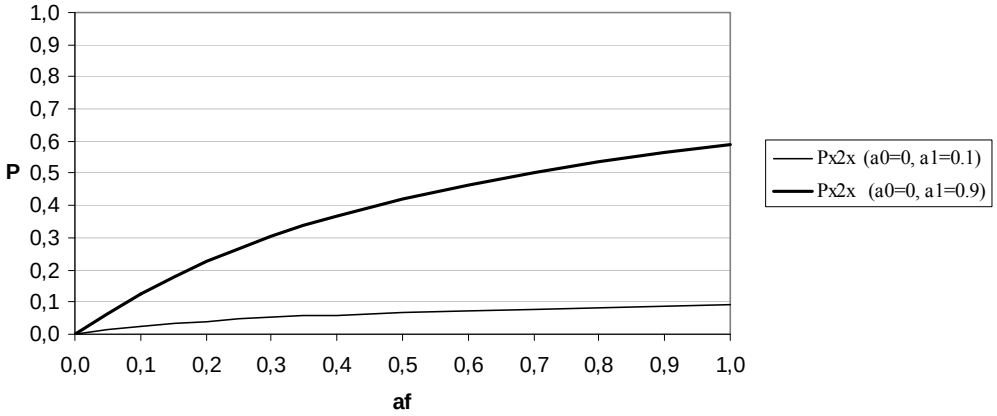

Рисунок 6

Запропонований в роботі підхід отримання числових характеристик впливу випадкових факторів на безпеку технологічного процесу банку дає можливість визначення впливу кожного з цих факторів та втрат від цього впливу.

УДК 638.253.231

АНАЛИЗ ТРЕБОВАНИЙ К ТОПОЛОГИИ И АРХИТЕКТУРЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ СЕТЕЙ ПОВЫШЕННОЙ БЕЗОПАСНОСТИ

Сергей Макаров
Военный институт управления и связи

Анотація: **Аналізуються вимоги до топології та архітектурі програмного забезпечения існуючих мереж й відмічаються ті з них, які підходять для мереж підвищеної безпеки.**
Summary: **Analysis requirements to topologies and architect software of existing network and markets that from them, which are an approach for increased safe networks.**
Ключові слова: **мережа підвищеної безпеки, трафік, топологія та архітектура ПО.**

Семиуровневая модель управления процессами глобальных сетей, как и принятые позднее четырех-пятиуровневые модели управления процессами локальных сетей, ставят своей целью обеспечение открытости,

гибкости и эффективности сетей. В сетях с повышенным уровнем безопасности на первый план выходит требование безопасности, и оно настолько превалирует над другими требованиями, что последнее имеет смысл считать не первостепенными. Этот факт оказывает существенное влияние, как на топологию сети, так и на архитектуру ее программного обеспечения.

Во избежание несанкционированного контроля трафика сети приходится отказаться от таких распространенных топологий локальных сетей, как «общая шина» и «кольцо». Остается топология «звезда» с жестким контролем сетевого трафика. Здесь наиболее эффективной является дисциплина планирования процессов (в данном случае - трафика) с несколькими очередями [1]. Устанавливается столько очередей, сколько имеется уровней приоритетности рабочих станций (РС), причем на каждом уровне используется две очереди – одна для передачи, другая – для приема сообщений (при постановке во вторую очередь может учитываться разность приоритетов источника и приемника сообщений, на низшем уровне приоритетности второй очереди нет). Не исключается нахождение на одном уровне лишь одной РС, особенно для верхних уровней приоритетности. В любой момент времени обслуживается непустая очередь с наиболее высоким уровнем приоритетности. Во избежание неприемлемых задержек трафика между РС нижних уровней приоритетности, а также для сокрытия факта наличия интенсивного трафика на верхних уровнях, приоритеты очередей нижних уровней периодически повышаются до уровня захвата их процессом обмена информацией между РС с последующим возвратом на свой основной уровень. Может скрываться и факт низкой нагрузки сети искусственным замедлением очередей низших уровней. Для оперативного создания некоторых льгот РС с большим объемом обмена в виде разрешения передачи за один раз более одного пакета можно использовать обратную связь по данному показателю [1], однако воздействие этой обратной связи должно быть умеренным, чтобы предотвратить возможность злоумышленной атаки типа «направленный поток сообщений» [2].

Процедура обмена сообщениями между центральным компьютером (ЦК), выполняющим функции планировщика и контролера трафика, почтового сервера и ретранслятора, с РС следующая. РС постоянно находится в режиме ожидания от ЦК команды на прием или разрешения на передачу. При необходимости передачи информации РС передает на ЦК служебный пакет – заявку, содержащий адрес приемника. ЦК принимает этот пакет и немедленно анализирует его на предмет постановки в соответствующую очередь. Контролируется количество неисполненных заявок от одной РС и при превышении лимита ЦК, послав один пакет-отказ, становится временно нечувствительным к таким заявкам. Адрес источника сообщения устанавливается автоматически при выходе из РС во избежание манипулирования им со стороны пользователя. Допускается только контролируемый (и регистрируемый) обмен между РС. На каждый переданный пакет должно быть получено подтверждение приема.

Сеть повышенной безопасности ориентируется на использование, в основном, бездисковых РС с исключением возможности разработки на них новых программ, что затрудняет внедрения в систему программ, поддерживающих атаки на сеть (например, программ предсказания и подбора номера пакета и т.п.).

Сеть повышенной безопасности является, по идее, сугубо локальной сетью, однако стеки протоколов существующих локальных сетей оказываются неподходящими для нее. Во-первых, протоколы не должны выполнять функцию «мультиплексирования – демультиплексирования», то есть не должно существовать альтернативных протоколов. Мультиплексирование может оставаться разве что на прикладном уровне, разрешая этим работу РС в мультизадачном режиме. Разделение управления сетевыми процессами на уровни может производиться только из соображений обеспечения достаточной гибкости при замене на более совершенную реализацию протокола и удобства администрирования. В таком случае целесообразно установить следующие четыре уровня управления сетевыми процессами:

а) прикладной уровень, генерирующий сообщения на передающей и потребляющей их на принимающей РС;

б) уровень обеспечения секретности, проверяющей на передающей РС допустимость соединения, а также соответствующие криптографические преобразования на обоих концах соединения, причем вид криптографического преобразования соответствует конкретному соединению;

в) транспортный уровень, выполняющий формирование и контроль прохождения пакетов;

г) уровень соединения, организующий передачу и прием пакетов.

Локальный перечень допустимых соединений имеется на каждой РС. Дополнительный контроль допустимости соединения выполняет ЦК в момент организации выполнения заявки на передачу информации.

Упомянутое выше распределение РС по уровням приоритетности при обмене информацией может никоим образом не корреспондироваться с правами доступа к информации и ключами шифрования пользователей этих РС. Распределение РС по уровням приоритетности при обмене информацией, как и таблица взаимной доступности станций, является более-менее статичным, в то время как права пользователей по доступу к информации и ключи шифрования являются более динамичными и устанавливаются соответствующими администраторами.

В сети повышенной безопасности существенно сокращается, по сравнению с открытыми локальными сетями, перечень возможных функций управления сетью со стороны РС. Собственно остаются только функции «Передать сообщение», «Почта», «Синхронизация таймеров РЧ и ЦК №, «Подсказка» (последняя в

соответственно ограниченном объеме). Функции определения конфигурации сети, администрирования и аудита, типичные для сетевых операционных систем, являются строго контролируемыми и выполняются централизовано.

Таким образом, выполненный анализ показывает существенное упрощение протоколов и связей между ними в сетях повышенной безопасности по сравнению с обычными сетями, но в то же время усложнение самих процедур связи. Топология же сети повышенной безопасности должна отличаться от топологии традиционных сетей.

Литература: 1. Кейлингерт П. Элементы операционных систем, 1985. 2. Медведовский И. Д. и др. Атака на Internet, 1999.

УДК 004.056.5

НАБЛЮДАЕМОСТЬ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ КАК НЕОТЪЕМЛЕМАЯ ЧАСТЬ КОМПЛЕКСА СРЕДСТВ ЗАЩИТЫ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

Денис Кудин
Общество с ограниченной ответственностью «АННА»
Запорожский государственный технический университет

Анотація: **У цій статті розглядається необхідність реалізації властивостей спостерігання обчислювальних систем у програмах захисту від персонала й основні вимоги до методів і технологій, забезпечующим цю властивість.**
Summary: **The necessity of computer systems accountability implementation in personnel security programs and general requirements to accountability technologies are discussed in this article.**
Ключевые слова: **обчислювальна система, автоматизована система, спостерігання, захист від персоналу, регістрація.**

I Введение

Защита от персонала – это большая проблема, которой в настоящее время уделяется огромное внимание во всем мире. В Украине она стоит особенно остро, так как отсутствие специализированных технических средств и программного обеспечения, а также некомпетентность ответственных лиц, создают благоприятную почву для развития различных форм промышленного и коммерческого шпионажа [1].

В программах защиты от персонала (Personnel Security Programs) используется два основных подхода. Первый связан с разработкой правил безопасного использования компьютеров при работе в сети, разграничением доступа к информации и т.д., а также разработкой физических мер защиты (охрана помещений, применение систем наблюдения и т.д.). Второй подход связан с определением состава программного (программно-аппаратного) обеспечения, которое используется администратором безопасности вычислительной системы для обеспечения ее *наблюдаемости* – свойства вычислительной системы, позволяющего фиксировать деятельность пользователей и процессов, использование пассивных объектов, а также однозначно устанавливать идентификаторы причастных к определенным событиям пользователей и процессов с целью предотвращения нарушения политики безопасности и/или обеспечения ответственности за определенные действия [2]. Именно это свойство, в зависимости от качества его реализации, позволяет в той или иной мере контролировать соблюдение сотрудниками предприятия установленных правил безопасной работы на компьютерах.

Однако многие предприятия Украины часто ограничиваются какой-либо одной мерой защиты, например, покупкой дорогостоящего межсетевого экрана, работающего на границе внутренней корпоративной сети и внешней глобальной сети Internet. При этом предполагается, что все компьютеры, объединенные в сеть, имеют выход в Internet через этот межсетевой экран. Между тем, крупнейшие корпорации мира ежегодно увольняют сотни сотрудников за то, что те приносят свои модемы и подключаются к внешней сети через телефонные линии со своих рабочих мест. Если произошла утечка критичной информации, то администратор безопасности, не имея дополнительных программных средств, практически не в состоянии выявить злоумышленника и определить, к какому компьютеру, в какое время был несанкционированно подключен модем, и какая именно информация была скомпрометирована. С этой точки зрения, межсетевые экраны не могут обеспечить надежную защиту от персонала.