



# Нагрузочное тестирование корпоративных информационных систем и систем обеспечения информационной безопасности с использованием комплекса INFORION-NAG

## Содержание

Что такое нагрузочное тестирование и для чего оно нужно .....	2
INFORION NAG: архитектура и функциональные возможности .....	7
Пример проведения нагрузочного тестирования .....	11
Исходные данные об объекте .....	11
Этапы проведения нагрузочного тестирования .....	12
Постановка задачи .....	13
Планирование тестирования .....	13
Инфраструктура сети Интернет-магазина .....	13
Анализ параметров тестирования .....	14
Источники статистики тестирования .....	15
Политики тестирования .....	16
Подготовка инфраструктуры .....	19
Тестирование .....	20
Оценка результатов .....	21
Точтовый сервер .....	22
Web-сервер .....	24
Межсетевой экран .....	24
Вывод по результатам тестирования .....	26
Заключение .....	28

## Что такое нагрузочное тестирование и для чего оно нужно

Сегодня неотъемлемой частью деятельности практически любой компании становится ИТ-инфраструктура. Отчетность, документооборот, бухгалтерия, учет имущества, отношения с клиентами и многое другое — все это выполняется с использованием средств вычислительной техники. Там же, где есть несколько компьютеров, рано или поздно появляется потребность объединения их в сеть с целью обмена информацией, получения доступа к общим информационным ресурсам компании, создания общекорпоративного информационного пространства, обеспечения других взаимодействий.

Другими словами, в настоящее время компьютерные сети стали обычным явлением. Важной их особенностью является тот факт, что современные корпоративные сети не являются изолированными, а подключаются к сетям более высокого уровня. Как наиболее распространенный пример - к глобальной сети Интернет. Возможности, которые предоставляет использование Интернет, крайне широки – это и общение с партнерами, и поиск клиентов, и проведения рекламных мероприятий и многое другое. Подключение к глобальной сети становится жизненно необходимым для деятельности любой компании, как крупной, так и масштаба SMB/SOHO. Более того, для некоторых компаний Интернет является основной средой ведения бизнеса — это Интернет-магазины, информационные и медиа-порталы, торговые площадки и прочие, основанные на предоставлении онлайн-сервисов.

Однако, наряду с множеством неоспоримых благ, подключение к компьютерным сетям общего пользования влечет за собой ряд требующих своего решения проблем. В первую очередь, речь идет о проблеме обеспечения **информационной безопасности**.

Например, если внутрикорпоративная локальная сеть подключена к сети Интернет, то администраторам локальной сети необходимо уделять внимание угрозам, исходящим из внешней сети. Наиболее распространенными угрозами можно назвать получение доступа к конфиденциальным данным, «заражение» корпоративной информационной системы злонамеренным программным кодом (компьютерными вирусами), атаки на отказ в обслуживании, в конце концов - просто сетевое хулиганство. При наличии перечисленных угроз есть и очевидная необходимость в применении средств защиты от них: межсетевых экранов, систем обнаружения и предотвращения вторжений, систем проактивной защиты, антивирусов.

В случае, если Интернет является основным ИТ-сервисом, используемым для ведения корпоративного бизнеса, то сетевые угрозы становятся критически опасными. Чем больше таких угроз, тем больше у конкурентов возможностей для нанесения ущерба и захвата преимущества на рынке. Следовательно,

использование систем обеспечения информационной безопасности, непрерывная поддержка их в актуальном состоянии — это неотъемлемая часть успеха «онлайновой» компании.

Вышесказанное приводит к такому выводу: на каждом этапе проектирования, внедрения, модернизации корпоративной сетевой инфраструктуры должны решаться вопросы оценки принятых технических решений со стороны производительности и устойчивости компонентов сети, средств системы обеспечения информационной безопасности (далее СОИБ) и информационных систем. Следует оценивать как работу в условиях штатной нагрузки, так и в условиях повышенной, а так же в условиях воздействия сетевых атак.

Рост компании, расширение пользовательской базы, ввод в эксплуатацию новых сервисов компании — все это ведет к усложнению и разрастанию ИТ-инфраструктуры, что может привести к проблемам с производительностью, к ухудшению показателей скоростных характеристик корпоративной информационной системы. Одной из важных задач становится недопущение ввода в эксплуатацию заведомо низкопроизводительных автоматизированных систем. Так же особое внимание следует обратить на контроль эффективности работы механизмов безопасности. Ведь недостаточно «декларативно» объявить об обеспечиваемом уровне защищенности СОИБ. Для заказчика необходимо иметь возможность проверить этот уровень, а для поставщика или разработчика решения — продемонстрировать его. Зачастую, эта задача требует высокого уровня квалификации и может оказаться весьма ёмкой, как по времени, так и по ресурсам, если нет специализированного средства для её решения.

Таким образом, часто возникает потребность в проведении нагрузочного тестирования, в ходе которого выполняется:

- контроль качества обслуживания прикладных сервисов;
- контроль обеспечиваемого уровня защищенности СОИБ;
- создание условий эксплуатации, отличающихся от прогнозируемых или штатных.

**Нагрузочное тестирование** - целенаправленное создание нагрузки на информационную систему для качественной и количественной оценки функционирования самой системы, а также её вспомогательных подсистем (в том числе и СОИБ).

В ходе нагрузочного тестирования система и/или ее подсистемы подвергаются различным нагрузкам, при этом цель такого тестирования — оценить способность системы правильно функционировать не только при штатных нагрузках, но и при некотором превышении нагрузок, планируемых при реальной эксплуатации. Такое тестирование позволяет убедиться, что система имеет некоторый «запас прочности». Также оно позволяет определить численные характеристики производительности (время отклика, число транзакций и пр.), а так же проверяет эффективность работы механизмов безопасности. Что же является объектом нагрузочного тестирования? Рассмотрим этот вопрос подробнее. В настоящее время в любой реальной корпоративной ИТ-инфраструктуре существует множество элементов, за счет которых обеспечивается ее

работоспособность. Таковыми элементами являются:

- средства вычислительной техники – рабочие станции и серверы;
- сетевое оборудование;
- сетевые сервисы (DNS, AD);
- средства защиты информации (системы обнаружения вторжений, системы защиты от вирусов и спама, межсетевые экраны, VPN-шлюзы и др.).

Производительность, корректность работы любого перечисленного элемента инфраструктуры может серьезно влиять на работоспособность всей системы в целом. В той или иной степени, конечно. Приведем несколько примеров:

- проблемы с сетевым оборудованием могут привести к тому, что нормальная работа отдельного сегмента сети компании, либо всей сети в целом, будет фактически невозможна. Если компания предоставляет какие-либо информационные сервисы, либо применяет внутрикорпоративные сервисы, необходимые для работы сотрудников, то недоступность их по причине проблем с сетевым оборудованием, способна надолго парализовать работу в компании:

- элементы СОИБ для обеспечения должного уровня защиты могут располагаться «в разрыв», а значит, проблемы с их функционированием могут открыть дорогу угрозам в корпоративную сеть, либо сделают работу в сети невозможной, хотя все остальные составляющие инфраструктуры в то же время будут функционировать идеально;

- нередко в нагруженных сетях используются балансировщики нагрузки для обеспечения эффективного распределения ресурсов между пользователями. Однако, некорректные настройки этих балансировщиков могут привести к тому, что пользователи не получат желаемого обслуживания из-за «нехватки ресурсов», хотя фактически ресурсов будет более чем достаточно.

Многие проблемы ИТ-инфраструктур проявляются не в режиме штатного функционирования, а при нагрузках, отличающихся от запланированных. И если эти проблемы возникнут на критических элементах, то работа всей инфраструктуры будет нарушена. Поэтому необходимо, используя нагрузочное тестирование, проверять и удостоверяться, что нестандартные нагрузки не приведут к нарушению работоспособности. К тому же, необходимо знать, при каких показателях сетевой нагрузки система будет функционировать нормально, а при каких начнет давать сбой.

Знание таких «граничных условий» работоспособности очень важно во многих ситуациях, например, при расширении компании ее ИТ-инфраструктуры или при увеличении базы пользователей. С другой стороны, «вредоносную нагрузку» могут создавать и конкуренты, а зная «запас прочности» системы имеется возможность предсказать, хватит ли у конкурента ресурсов, чтобы превзойти этот «запас».

Итак, очевидно, что *нагрузочное тестирование* ИТ-инфраструктуры в целом или ее компонентов — это мощное средство минимизации специфических рисков для бизнеса компании, а так же прогнозирования и предотвращения

ситуаций, грозящих потерей функциональности или нарушением безопасности.

Когда же необходимо применять этот инструмент, чтобы наиболее полно задействовать весь его потенциал?

Можно выделить следующие этапы в жизненном цикле ИТ-инфраструктуры в целом, либо отдельных ее составляющих, на которых нагрузочное тестирование целесообразно:

- выбор и обоснование технических решений;
- разработка и тестирование специализированного программного обеспечения;
- ввод в эксплуатацию;
- модернизация.

На каждом из этих этапов следует выполнять тестирование, чтобы убедиться в том, что выполняемые работы движутся в верном направлении и удовлетворяют предъявляемым требованиям.

При выборе технических решений или при разработке собственных, нагрузочное тестирование позволяет оценить количественно и качественно, насколько решение соответствует требованиям к функционалу и качеству.

В случае сложных систем, состоящих из множества различных компонентов, имеет смысл разделять тестирование по компонентам и тестирование всей системы в целом. Это обусловлено тем, что нередко производительность всей системы определяется самым слабым ее компонентом, а значит, выявление такого компонента и улучшение его характеристик позволяет повысить качество всей системы.

При вводе информационной системы (ИТ-инфраструктуры) в эксплуатацию нагрузочное тестирование позволяет принимающей стороне убедиться, что поставленные требования выполнены. Оценить «запас прочности» принимаемого решения. Интегратору же этот инструмент дает возможность продемонстрировать проделанную работу, наглядно показать, что все предъявляемые требования выполнены. Конечно, следует учитывать, что здесь говорится только о тех требованиях, которые можно проверить с помощью нагрузочного тестирования.

При модернизации системы, замене отдельных ее составляющих, изменении различных настроек, проведение набора эталонных тестов позволяет убедиться в том, что не произошло деградации как участка, подвергнувшегося модернизации, так и всей системы в целом.

Таким образом, в проведении нагрузочного тестирования могут быть заинтересованы любые компании, использующие или разрабатывающие как отдельные сетевые решения, так и выполняющие (внедряющие) сложные, комплексные ИТ-проекты. Особо следует выделить компании, для которых сетевые технологии и решения являются основой бизнеса: это операторы связи, сервис-операторы, провайдеры услуг Интернет, производители различного сетевого оборудования и промышленных комплексов, а также все предприятия и организации, заинтересованные в обеспечении устойчивости ИТ-инфраструктур и их отдельных компонентов к повышенным нагрузкам и сетевым атакам.

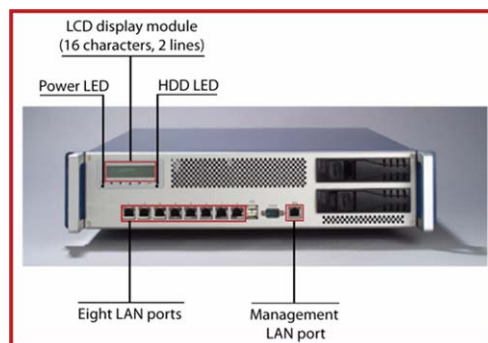
Следует отметить, что задача оценки качества и устойчивости может иметь как непрерывный, регулярный, так и разовый характер. Ведь далеко не для всех компаний, заинтересованных в проведении нагрузочного тестирования, имеет смысл закупать специализированные решения, проводить обучение сотрудников. Потребности многих компаний, осознающих важность отказоустойчивости ИТ-инфраструктуры, могут быть удовлетворены разовыми процедурами тестирования. В таких компаниях ИТ-инфраструктура, как правило, имеет «статичный» характер, модификации и изменения случаются достаточно редко, а значит, покупка услуги нагрузочного тестирования является для них оптимальным выбором.

В следующей части статьи будет рассмотрено специализированное решение – программно-аппаратный комплекс INFORION-NAG, предназначенный для проведения нагрузочного тестирования компонентов СОИБ, компонентов информационно-телекоммуникационной инфраструктуры и прикладных сервисов. Также будет рассмотрен пример применения этого комплекса.

## INFORION NAG: архитектура и функциональные

### ВОЗМОЖНОСТИ

INFORION-NAG – это программно-аппаратный комплекс, предназначенный для тестирования сетей, систем обеспечения информационной безопасности и их элементов путем создания легитимной и/или злонамеренной нагрузки на компоненты ИТ-инфраструктуры. При разработке этого инструмента мы ориентировались на решение с его помощью следующих задач:



- тестирование корпоративных информационных систем и средств обеспечения информационной безопасности на устойчивость к внутренним и внешним сетевым атакам, в том числе и распределенным;
- тестирование пропускной способности каналов передачи данных и сетевого оборудования;
- тестирование производительности сетевых сервисов и приложений.

Для успешного выполнения перечисленных задач в качестве аппаратной платформы для INFORION-NAG (далее NAG) выбрано специализированное решение от Advantech, предоставляющее возможность использования для выполнения задач тестирования восьми сетевых интерфейсов с поддержкой скорости передачи данных 1Гбит/с.

Несомненно, при тестировании сложных и больших систем может возникнуть потребность создания нагрузки одновременно с нескольких сегментов сети, поэтому такая возможность учтена при разработке клиент-серверной архитектуры программной составляющей комплекса. Основными компонентами этой архитектуры являются (см. Рисунок 1):

- **«мастер»** — сервер, реализующий управляющие функции;
- **«зонд»** — клиент мастера, реализующий исполняющие функции тестирования;
- **«консоль управления»** — предоставляет пользователю возможность создавать сценарии тестирования, выполнять их и вести мониторинг результатов.

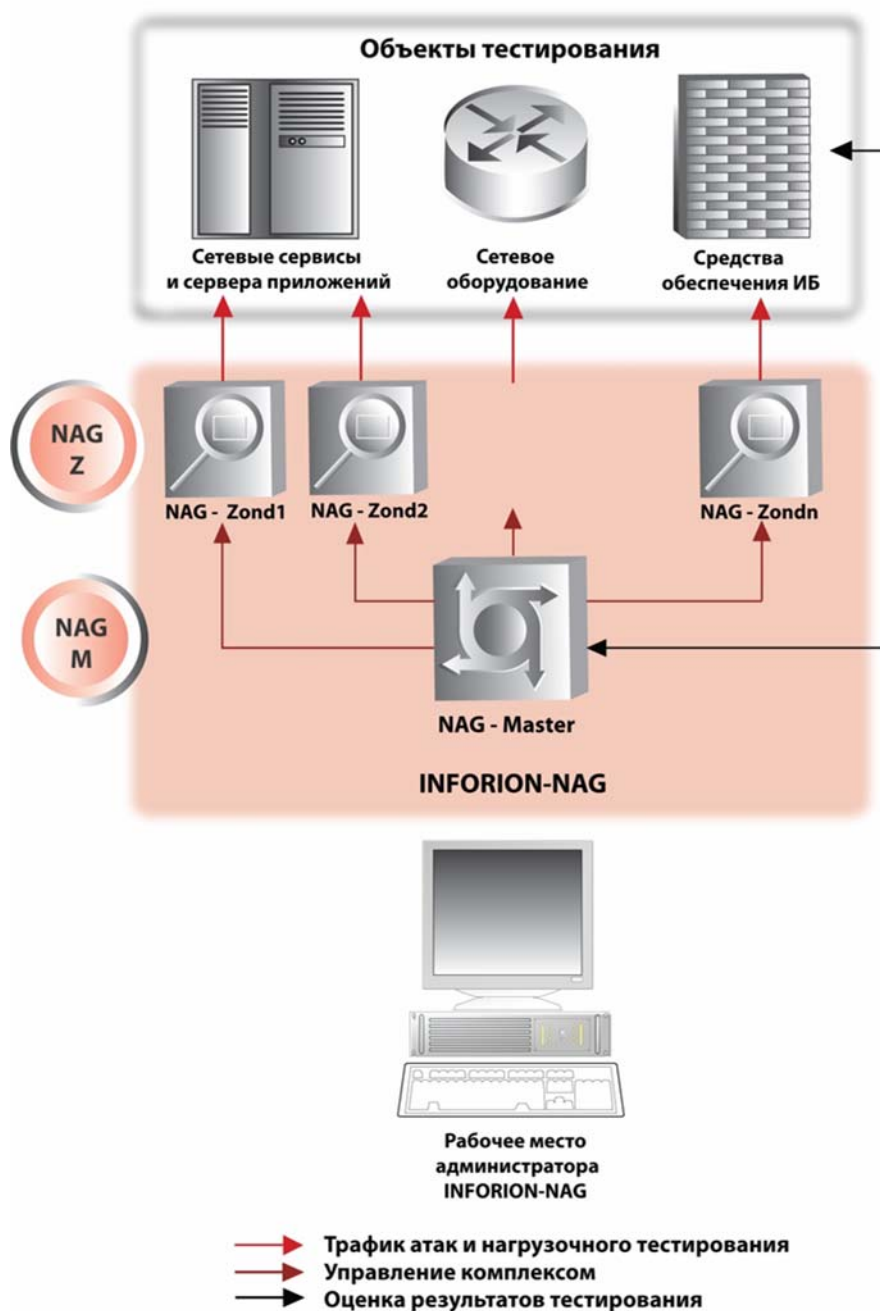


Рисунок 1. Архитектура комплекса

«**Мастер**» осуществляет координацию выполнения сценариев тестирования посредством выдачи задач зондам, управления ими и мониторинга условий прекращения тестов. Также мастер отвечает за сбор данных для генерации отчетов и выполнение ряда других задач. Он установлен на аппаратную платформу и не может быть развернут на других средствах администратором комплекса.

«**Зонд**» – компонент комплекса, непосредственно выполняющий генерацию трафика сетевых атак и тестов производительности. Зонды могут использоваться на аппаратной платформе комплекса совместно с мастером или устанавливаться

на выделенные платформы. На каждом из восьми сетевых интерфейсов аппаратной платформы можно запустить один или несколько зондов в зависимости от замысла тестирования. Зонды, установленные на внешних выделенных платформах, так же работают под управлением мастера. Такой подход обеспечивает возможность располагать зонды не только непосредственно на аппаратной платформе NAG, но также на любом компьютере в сети.

При необходимости, можно создавать распределенную сеть для направления на тестируемую систему произвольной нагрузки по сложным сценариям.

«**Консоль управления**» предоставляет возможность управлять комплексом практически с любой современной операционной системы, необходим лишь сетевой доступ к порту управления платформы.

Одной из основных проблем при проведении нагрузочного тестирования является координация действий различных разрозненных утилит. INFORION-NAG предлагает комплексный подход, осуществляя централизованную координацию действий зондов, располагаемых в разных сегментах сети.

Комплекс NAG предоставляет возможности создания гибких сценариев тестирования, а именно:

- атаки и нагрузочные тесты могут выполняться одновременно с различными параметрами из разных сегментов сети;
- продолжительность выполнения каждой задачи может задаваться пользователем или зависеть от измеряемых параметров;
- для каждой выполняемой задачи можно получить статистику (например, количество переданных пакетов, количество успешных транзакций и т.п.);
- злонамеренная нагрузка имитируется распространенными атаками типа flooding. Кроме того, может быть выполнена имитация передачи вредоносного ПО (вирусов) по распространенным прикладным протоколам;
- легитимная нагрузка является эмуляцией деятельности пользователей и создается для следующего набора прикладных сетевых сервисов: SMTP (с возможностью включения в трафик спама и вирусов), FTP, HTTP, SMB, Microsoft SQL Server, Oracle SQL Server.

Состав поддерживаемых сервисов и возможностей по их тестированию регулярно расширяется, увеличивается число поддерживаемых атак и измеряемых параметров. Реализация поддерживаемых функций тестирования в виде модулей также позволяет легко разрабатывать специфичные тесты и сценарии имитации атак для конкретных требований.

Сценарии тестирования могут сохраняться, что дает возможность неоднократно повторять процесс и отслеживать динамику изменения результатов. Ход тестирования и текущие возможности ресурсов аппаратного комплекса и внешних зондов отображаются с помощью специального монитора, интегрированного в графический интерфейс управления.

При выполнении сценариев тестирования осуществляется сбор статистики по ходу выполнения задач, которую, при желании можно включать в отчеты с

варьируемым уровнем детализации.

Проведение нагрузочного тестирования – это сложная организационно-техническая задача и один инструмент не может решить все потенциально возможные проблемы, однако использование продукта INFORION-NAG обеспечивает максимально простое развертывание средств нагрузочного тестирования. NAG позволяет реализовывать сложные стратегии контроля, пользуясь которыми регулярно, пользователь сможет получать ответы, например, на следующие вопросы:

- достаточно ли производительности используемой СОИБ для функционирования в условиях прогнозируемой нагрузки с должным уровнем обеспечения качества информационных сервисов? Достаточно ли производительность самих сервисов?

- как поведут себя в условиях обычных или распределенных атак отказа в обслуживании (DoS- и DDoS-атак) сетевые сервисы в целом и компоненты ИТ-инфраструктуры их обеспечивающие?

- правильно ли проведена настройка межсетевых экранов и средств обнаружения вторжений?

- с какой скоростью наполняются журналы регистрации событий средств СОИБ, операционных и информационных систем? Не приведет ли к отказу в обслуживании переполнение журналов событий? Есть ли необходимость в изменении правил протоколирования событий?

- успешно ли справляются со своими задачами антивирусные почтовые шлюзы и системы фильтрации спама?

Какими бы полными ни были теоретические выкладки, лучше всего суть нагрузочного тестирования и использование INFORION-NAG для этих целей продемонстрировать на конкретном примере. Такой пример будет рассмотрен в следующей части статьи.

## Пример проведения нагрузочного тестирования

### Исходные данные об объекте

Рассмотрим проведение нагрузочного тестирования с помощью INFORION-NAG на примере достаточно крупного Интернет-магазина (далее ИМ).

ИМ является хорошим примером современной онлайн-компании, чей бизнес основан на использовании Интернет-технологий, а значит, сетевые угрозы могут нанести ощутимый ущерб успеху компании, если она не готова к противодействию.

Но прежде чем приступать к проведению тестирования, необходимо получить некоторое представление об объекте внимания.

В штате ИМ состоит 537 сотрудников, работающих в офисе.

В компании имеется два сервиса, от которых зависит ее работоспособность и которые предоставлены пользователям напрямую или косвенно:

- WEB-сервер;
- почтовый сервер.

Согласно статистике за последний год работы для WEB-сервера:

- средняя посещаемость сайта порядка 35000 посетителей в день;
- наибольшая активность пользователей по дням недели — вторник;
- наибольшая активность пользователей по времени суток — с 13 до 16 часов (37%);
- наименьшая активность пользователей по дням недели — выходные (на 40-45% ниже);
- наименьшая активность пользователей по времени суток — с 3 до 8 утра (<10%);
- доля запросов к сервису со стороны офиса компании составляет 5-10%.

Для почтового сервера:

- средний объем сообщений — 12300 в сутки;
- наибольшая нагрузка по дням недели — понедельник и среда;
- наибольшая нагрузка по времени суток — с 17 до 19 часов (27-37%);
- наименьшая нагрузка по дням недели — выходные;
- наименьшая нагрузка по времени суток — с 22 часов до утра (<8%);
- доля сообщений со стороны офиса компании составляет до 20-30%.

Отдельно следует выделить нагрузку в предпраздничные недели, когда она

возрастает на 36-47% на WEB-сервер и 23-34% на почтовый сервер.

Таким образом, у нас есть вполне ясная картина использования сервисов компании за последний год, а в связи с разработкой проекта расширения бизнеса и его распространения в ряд регионов, появилась необходимость проанализировать существующие технические ресурсы на предмет стабильности работы при повышении нагрузки на предоставляемые сервисы.

В прорабатываемом проекте не планируется обеспечивать филиалы отдельными техническими площадками для сервисов, так как по расчетам проектировщиков должно хватить возможностей существующих.

Чтобы проверить, достаточно ли окажется располагаемых ресурсов для осуществления задуманного расширения или потребуются дополнительные мощности, решено произвести нагрузочное тестирование сервисов компании.

### ***Этапы проведения нагрузочного тестирования***

Проведение нагрузочного тестирования включает в себя несколько обязательных этапов, а именно:

1. ***Постановка задачи.*** Производится формулирование вопросов, ответы на которые необходимо получить по результатам нагрузочного тестирования.

2. ***Сбор исходных данных.*** В зависимости от задачи, набор исходных данных для проведения нагрузочного тестирования может варьироваться — статистика использования сервисов компании, отчеты систем обнаружения вторжений и т.д. Для конкретного случая, рассматриваемого в данной статье, исходные данные уже собраны и приведены выше.

3. ***Планирование тестирования.*** На основе поставленной задачи осуществляется выбор методов тестирования, задается объем тестов и состав инструментария. В процессе нагрузочного тестирования часто используется не какой-либо один продукт, а их комплекс, который может состоять из средств самого разного назначения (генераторы трафика, эмуляторы активности клиентов, средства мониторинга производительности, журналы регистрации событий). В процессе тестирования может быть задействован и персонал, осуществляющий контроль и выполняющий необходимые дополнительные действия. Во время планирования разрабатывается сценарий теста, его количественные и временные характеристики.

4. ***Подготовка инфраструктуры.*** На данном этапе производится подготовка инструментальных средств в соответствии с разработанным планом тестирования, обеспечивается возможность проведения процесса с учетом обеспечения бесперебойной работы информационной системы. При выборе времени и условий тестирования следует учитывать, что оно может создать проблемы пользователям, работающим с системой во время проведения тестирования.

5. ***Тестирование.*** Спланированные ранее действия производятся с применением комплекса программных и аппаратных инструментальных средств под управлением подготовленного персонала.

6. ***Оценка результатов.*** Показания всех инструментальных средств

анализируются и на их основе даются ответы на вопросы, поставленные ранее, или принимаются решения о модификации плана тестирования.

Согласно этим этапам далее и будет проиллюстрировано проведение нагрузочного тестирования.

### ***Постановка задачи***

Для обеспечения успешного расширения компании необходимо провести нагрузочное тестирование на предмет количественной и качественной оценки работоспособности сервисов компании при следующих прогнозируемых условиях их использования:

- увеличение числа посещений сайта в сутки на 75%;
- увеличение почтового трафика компании на 60%;

Также необходимо определить «запас» ресурсов сервисов, т.е. при каком превышении планируемой нагрузки сервисы компании смогут сохранить работоспособность и приемлемую скорость работы. Предположительно, сервисы должны выдерживать превышение запланированных показателей использования на 40-50%.

Также, необходимо проверить, что в случае осуществления атак из сети Интернет сервисы сохранят работоспособность и будут доступны работникам офиса компании.

Почему только работникам офиса? Здесь учитывается тот факт, что в ряде случаев (при масштабных DDoS атаках, да и при простых flood атаках) канал связи «забивается» мусорным трафиком и легитимным пользователям просто невозможно получить доступ к требуемому сервису.

Поэтому важно убедиться, что подобные атаки не приведут к выходу сервисов из строя, а также, что во время проведения атак работники офиса смогут продолжить свою работу с заказами, поскольку срыв выполнения уже полученных заказов нанесет компании гораздо больший ущерб, чем недоступность сайта Интернет-магазина в течении некоторого времени.

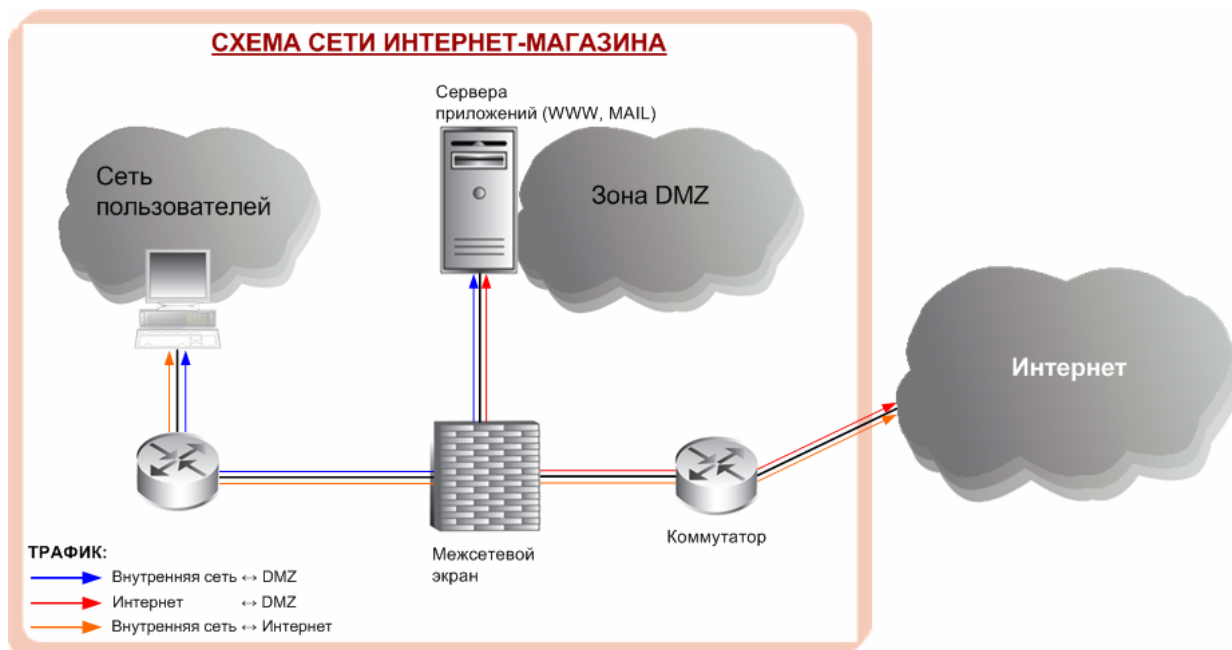
На основе поставленной задачи будет разработан план тестирования.

### ***Планирование тестирования***

Для разработки плана следует опираться на данные статистики использования серверов за прошедший год, а также на показатели повышения нагрузки на них, обозначенные при постановке задачи. Но прежде, чем приступить к анализу числовых параметров необходимой нагрузки, следует ознакомиться с инфраструктурой сети ИМ.

### **Инфраструктура сети Интернет-магазина**

Сеть ИМ довольно проста, все сервисы размещены в демилитаризованной зоне (DMZ) и доступны они как пользователям из сети Интернет, так и пользователям, находящимся в локальной сети. Структура сети представлена на иллюстрации (см. Рисунок 2):



**Рисунок 2. Схема сети Интернет-магазина**

Имея представление о структуре сети ИМ, можно приступить к анализу параметров тестирования, при выполнении которого будет определено, какие тесты при нагрузочном тестировании будут использованы и каким образом.

### Анализ параметров тестирования

Как было определено выше, за прошедший год была зафиксирована следующая средняя нагрузка на сервера:

- WEB-сервер, в среднем, обрабатывал запросы от 35000 посетителей в сутки;
- почтовый сервер принимал в среднем 12300 сообщений в сутки.

Тогда, исходя из планируемой нагрузки, при расширении эти показатели будут такими:

- WEB-сервер — 61250 запросов в сутки;
- почтовый сервер — 19680 сообщений в сутки.

Учитывая пиковые часы нагрузки, и предполагая, что в среднем скорость поступления запросов составляет 1 запрос/сообщение в минуту, получаются следующие предварительные параметры для нагрузочных тестов:

- Web-сервер — одновременно 400 конкурентных сессий, в рамках каждой из которых запросы идут постоянно. Значение выбрано исходя из того, что одновременно количество активных уникальных посетителей, согласно статистике, обычно не превышает 300-350 человек;
- почтовый сервер — одновременно 350 сессий с почтовым сервером, в рамках каждой из сессии отправка сообщений производится друг за другом без задержек.

Также необходимо учесть «предпраздничный» фактор, который заключается

в следующем:

- нагрузка на Web-сервер повышается на 47%, т.е. мы получаем 600 одновременных пользовательских сессий;
- нагрузка на почтовый сервер повышается на 34%, что создаст 470 одновременных сессий.

Таким образом, учитывая предположительный «запас прочности» инфраструктуры и долю участия в использовании сервисов со стороны офиса компании (10% и 30% для WEB- и почтового серверов соответственно), получаются следующие параметры для нагрузочных тестов, которые будут использоваться при тестировании:

- нагрузка на Web-сервер: 900 одновременных сессий, где 90 сессий идут со стороны работников офиса;
- нагрузка на почтовый сервер: 705 сессий, где 211 принадлежат офисным сотрудникам.

Эти цифры означают следующее: суммарно на сервисы будет создаваться указанная нагрузка (900 и 705 сессий соответственно), но источники ее будут разделены — меньшая часть будет исходить из локальной сети компании, большая часть — со стороны Интернета.

Для моделирования воздействий со стороны сети Интернет мы воспользуемся следующими шаблонами атак, входящими в состав INFORION-NAG:

- syn-flood;
- ping-flood.

Первая атака представляет собой незавершенный запрос на подключение к целевому сервису. Суть атаки в том, что при получении запроса на подключение, сервер резервирует место в памяти и ожидает завершения процедуры подключения в течение некоторого времени (обычно это несколько секунд). Посылая множество иницирующих запросов на подключение без продолжения самой процедуры подключения, можно вызвать отказ в обслуживании на целевой системе при относительно небольшом трафике.

Вторая атака достаточно проста. Следует отправлять большое количество ICMP-пакетов на целевую систему, создавая тем самым значительную нагрузку на канал. Эту нагрузку можно увеличить, указав определенным образом отправителя в заголовке пакета. Предлагается ограничиться просто потоком пакетов на целевую систему, без правки заголовков пакетов.

### **Источники статистики тестирования**

Проведение тестирования без сбора статистики не представляет особого интереса, кроме как получение качественного результата «будет работать, или не будет». Ведь по завершении тестирования не останется никаких данных о том, какую нагрузку вызвали тесты на сетевое оборудование, как вели себя средства обеспечения информационной безопасности, как реагировали сервисы, насколько были нагружены процессор, память, дисковая подсистема на интересующих

серверах.

Без сбора подобных данных самое большее, что можно будет сказать по результатам теста — завершились ли они в той или иной степени успешно (например, сервис не перестал отвечать на запросы) или нет. Но смысла в подобных ответах немного, ведь на их основании нельзя провести никакого анализа, планирования.

Поэтому сбор статистики необходим, для чего предлагается использовать следующие средства:

- отчеты INFORION-NAG по выполнению задач тестирования;
- статистика с интересующих нас узлов инфраструктуры, а это: WEB-сервер, почтовый сервер, межсетевой экран.

При проведении нагрузочного тестирования с помощью INFORION-NAG имеется возможность получить подробную статистику об объеме каждого проведенного теста. Например, для http-теста можно получить информацию о том, сколько было сделано запросов, какая часть оказалась неудачной, максимальное/среднее время загрузки страниц, время загрузки по зондам и т.п., для smtp-теста — сколько было отправлено писем, с какой скоростью, были ли ошибки.

Другими словами, статистика по выполненным тестам дает возможность оценить по каждой составляющей теста — в каком объеме, с какой скоростью, с ошибками или без отработали сценарии тестирования.

Статистика с узлов инфраструктуры нам понадобится для того, чтобы оценить, какую нагрузку на целевые системы создавали нагрузочные тесты, и справились ли узлы с ней. Исходя из этих данных, мы сможем также оценить «запас прочности» систем и определить узкие места.

Например, если в ходе тестирования при максимальной загрузке сервиса запросами утилизация ресурсов аппаратной платформы не достигла максимума, то это значит, что сервис может выдержать и большую нагрузку, но сетевое оборудование не справляется с ней или пропускная способность канала недостаточна.

Итак, были собраны и проанализированы все необходимые данные для того, чтобы разработать сценарии тестирования, которые в терминологии INFORION-NAG называются «политиками тестирования».

## Политики тестирования

В этой части статьи будут рассмотрены основные принципы построения политик тестирования (далее просто — политика) для INFORION-NAG. Для начала следует дать определение понятию «политика тестирования» в контексте его применения в INFORION-NAG.

*Политика тестирования* — это список задач с указанными пользователем параметрами, исполняемых заданной конфигурацией.

*Конфигурация* — это набор сетевых настроек комплекса, в рамках которых

также осуществляется привязка зондов<sup>1</sup> к сетевым интерфейсам. При создании конфигурации требуется указать:

1. Компьютеры, используемые в составе распределенной среды INFORION-NAG.
2. Используемые сетевые интерфейсы и их настройки.
3. Какие зонды и на каких интерфейсах будут работать.

**Задача** — функциональная единица политики, привязанная к одному или нескольким зондам. Каждая задача выполняет некоторое действие на указанных зондах (осуществляет запросы к серверу, измеряет что-то или просто осуществляет какую-то атаку). Существует условная классификация задач на три типа:

1. *Тест*. Такие задачи реализуют работу с прикладными сервисами. Например, http-тест — нагрузочный тест для WEB-сервера.
2. *Сенсор*. Данный тип задач реализует измерение какого-либо параметра и при наступлении заданных условий останавливается. Так сенсор-таймер отсчитывает время от запуска, connect-сенсор определяет возможность подключения на заданный порт и измеряет время этого подключения, и т.п.
3. *Атака*. Эти задачи реализуют механизмы «низкоуровневых» атак, например, syn-flood.

Несомненно, эта классификация весьма условна, ведь любой тест, при определенных условиях, может выступать и в роли атаки для выполнения DDoS, все зависит от того, какие мы преследуем цели. Это деление введено для того, чтобы было легче ориентироваться при работе с задачами.

Таким образом, политика — это просто руководство комплексу к действию, которое объясняет, когда и как проводить нужные тесты.

Для того чтобы лучше понять, что такое политика, рассмотрим, как они создаются на примере http-теста для ИМ.

Создание любой политики начинается с выбора конфигурации комплекса, подходящей для планируемых тестов. В случае если такой конфигурации еще нет — её следует создать.

Для тестирования ИМ предлагается использовать следующую конфигурацию:

- для нагрузочного тестирования используется только INFORION-NAG, внешние зонды не используются;
- 2 сетевых интерфейса с соответствующими настройками используются для работы из локальной сети ИМ. На каждом из интерфейсов размещаем по одному зонду;
- 3 сетевых интерфейса с соответствующими настройками используются для работы «из Интернета». На каждом из интерфейсов размещаем по одному зонду.

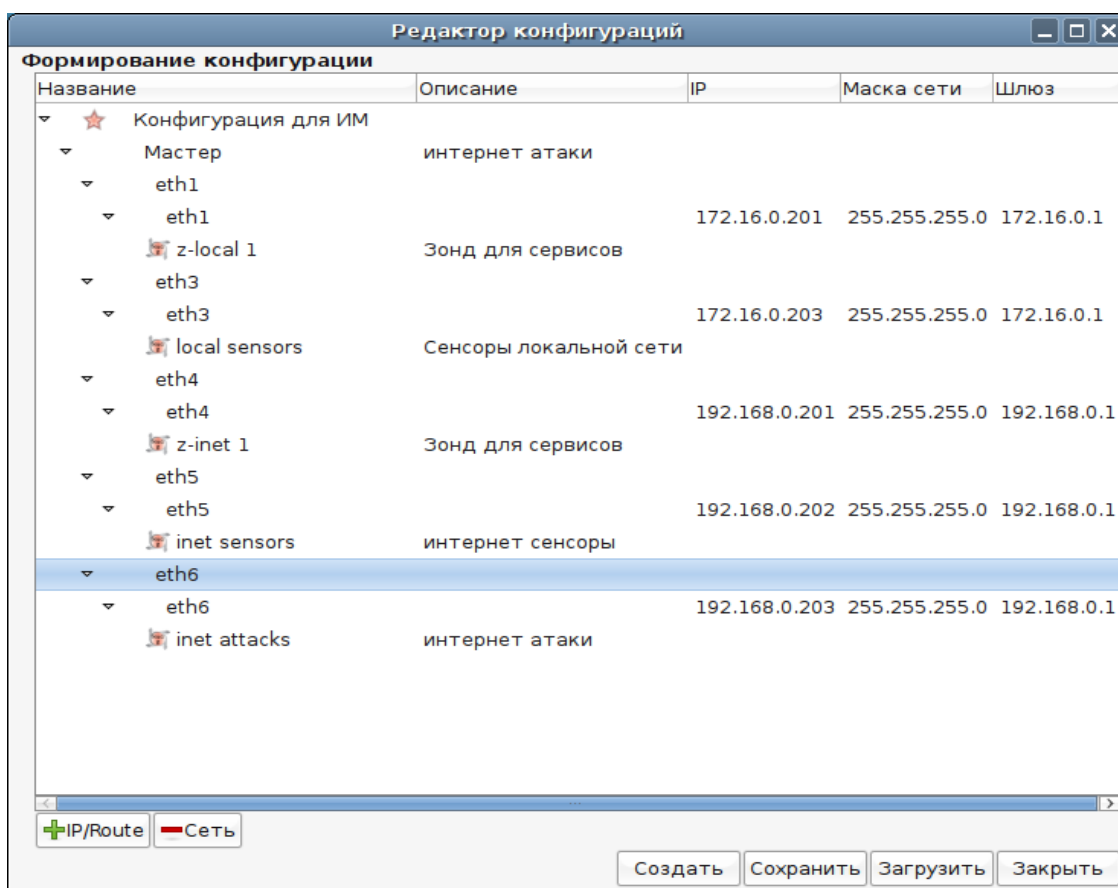
<sup>1</sup> См. п. INFORION NAG: архитектура и функциональные возможности

Для чего необходимо два интерфейса, подключенных в локальную сеть: один интерфейс для работы с WEB-сервером и почтой и один для работы сенсоров.

Для создания нагрузки со стороны сети Интернет нам понадобится еще один дополнительный интерфейс, который будет использоваться в других политиках для создания злонамеренного трафика, то есть атак.

Атаки, тесты и сенсоры были распределены по разным интерфейсам для того, чтобы они не «мешали» друг другу при использовании сети. Так, например, атака с того же интерфейса, с которого будет работать тест, может этот тест «парализовать». Во избежание подобных коллизий и выполняется разделение.

Итак, получившаяся конфигурация в редакторе INFORION-NAG выглядит следующим образом (см. Рисунок 3):



**Рисунок 3. Внешний вид окна редактора конфигураций INFORION-NAG**

Создав конфигурацию для тестирования ИМ, можно приступить к созданию простой политики, которая будет состоять из трех задач:

1. http-тест из локальной сети — в параметрах этой задачи мы указываем, что необходимо осуществлять запросы к web-сервису из 90 одновременных сессий и производить переходы по ссылкам. Таким образом, моделируется использование сайта работниками офисов. Эта задача назначается зонду, предназначенному для тестов из локальной сети.
2. http-тест из сети Интернет — здесь количество одновременных сессий

поднимается до 830, чем моделируется работа пользователей Интернет с ИМ. Эта задача назначается зонду, предназначенному для тестов со стороны сети Интернет.

3. Сенсор-таймер, который показывает, сколько времени должно продолжаться тестирование. Продолжительность теста будет составлять 10 минут.

Почему использовано всего три задачи и общее время выполнения теста ограничено десятью минутами? Цель этой политики — провести «предварительное» тестирование и выяснить, что заданную нагрузку система выдерживает, хотя бы непродолжительное время. Создав аналогичную политику для почтового сервиса и выполнив сначала одну, потом другую — мы можем убедиться, что сервисы готовы для настоящего тестирования, которое будет проводиться двумя дополнительными политиками.

Всего, для тестирования, предлагается использовать четыре политики:

- тестирование только web-сервиса. Продолжительность 10 минут;
- тестирование только почтового сервиса. Продолжительность 10 минут;
- одновременное тестирование и почтового и web-сервиса. Продолжительность 3 часа;
- одновременное тестирование почтового- и web-сервиса при наличии атак со стороны Интернет. Работа этой политики состоит из трех этапов: 30 минут до начала атак, 1 час под воздействием атак, 30 минут после атак. Итого — 2 часа.

Также, в состав комплексных тестов, можно дополнительно включить connest-сенсор, для снятия статистики по возможности установки соединения с почтовым и WEB-сервисами. Но в нашем случае в этом нет необходимости, так как сами тесты, выполняемые на протяжении всего тестирования, решают задачу проверки возможности подключиться.

В этой части было описано планирование сценариев тестирования, которые обеспечат решение поставленной задачи — убедиться в устойчивости информационной системы компании при ее расширении. Теперь предлагается перейти к подготовке инфраструктуры.

### ***Подготовка инфраструктуры***

В общем случае этот этап может быть одним из самых сложных и длительных. Например, в крупных сетях, разделенных на множество зон с различными правами доступа, не всегда очевидно, как лучше выполнять эти работы. Но в нашем примере сеть «классическая» и процесс тестирования прозрачен, так что подготовка инфраструктуры будет заключаться только в интеграции в нее комплекса INFORION-NAG. Для проведения такой интеграции в рассматриваемом примере достаточно подключить интерфейсы, ответственные за работу зондов локальной сети, к коммутатору локальной сети, и интерфейсы, на которых работают «Интернет-зонды», к коммутатору сегмента внешней сети.

Последним шагом перед проведением тестирования будет выбор времени тестирования.

Для тестируемого ИМ нам понадобится чистого времени 5 часов 20 минут. Учитывая «человеческий фактор», тестирование целесообразно провести в два этапа — в периоды наименьшей активности пользователей. Для этого мы выбираем выходные дни и интервал времени в период с 3 до 8 утра. В первый день будут проведены два предварительных теста по десять минут и один комплексный, без сетевых атак. Во второй день в это же время, будут повторены два предварительных теста и один комплексный с наличием сетевых атак.

Тестирование разбивается на два этапа не только из-за соображений «может не хватить времени», но из-за возможности выхода из строя каких-либо составляющих инфраструктуры из-за повышенной сетевой нагрузки. Поэтому необходимо иметь временной резерв, чтобы исправить возможные проблемы в случае их возникновения, так как нагрузочное тестирование не должно повлечь за собой ущерба бизнесу Интернет-магазина.

### ***Тестирование***

В ходе тестирования снимались показания статистики:

- сетевых интерфейсов межсетевого экрана;
- серверов сайта и почты — количество обработанных запросов и скорость принятия писем соответственно.

Также, по каждой из выполнявшихся задач в рамках комплексных политик, была собрана статистика о произведенной работе, используя которую на следующем этапе оценки результатов, мы сможем ответить вопросы, обозначенные при постановке задач тестирования.

Кроме этого в ходе тестирования проводилось наблюдения за показателями текущего состояния на главном окне INFORION NAG (см. Рисунок 4):

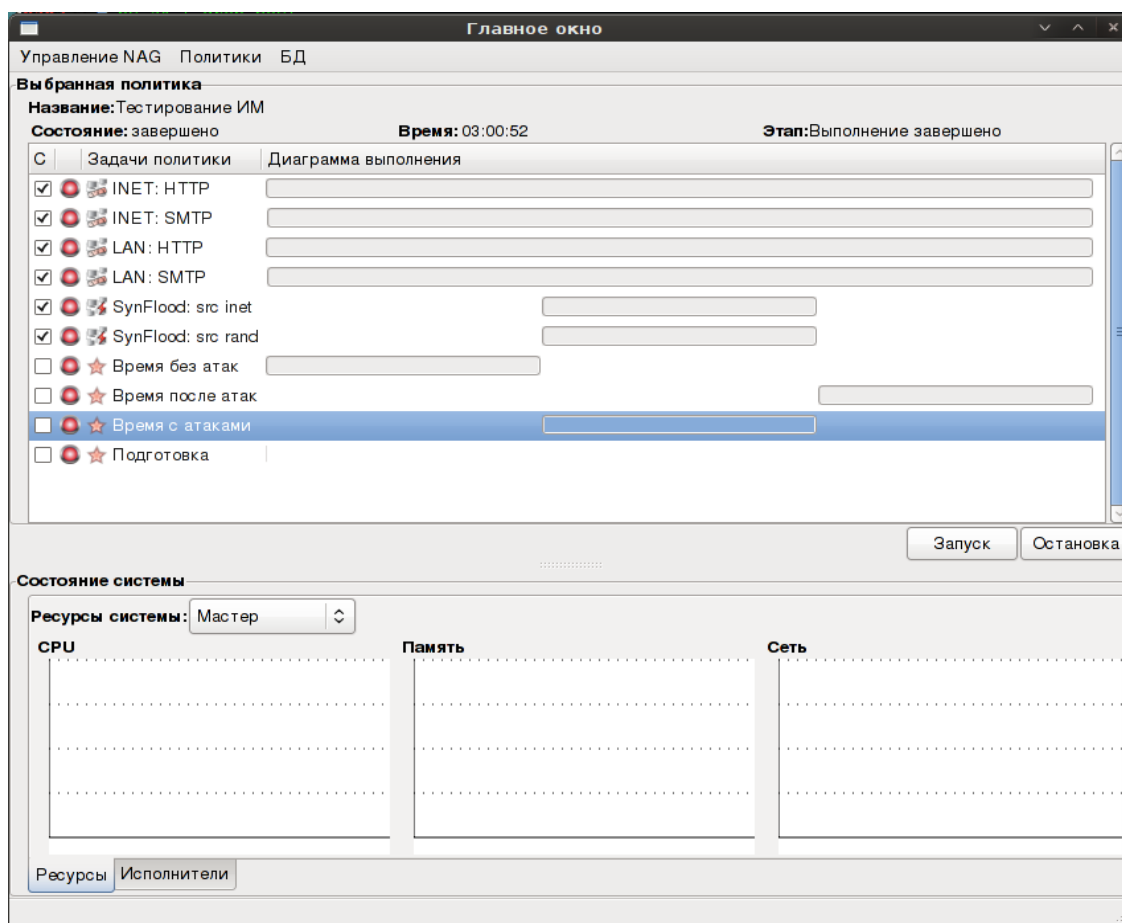


Рисунок 4. Внешний вид главного окна INFORION NAG

## Оценка результатов

Итак, после подготовки инфраструктуры, составления плана тестирования и, собственно, проведения тестирования — была собрана статистика, на основании которой можно ответить на поставленный вопрос:

***Хватит ли вычислительных и сетевых ресурсов ИМ при запланированной нагрузке?***

Анализ результатов проведенного нагрузочного тестирования позволяет ответить — ресурсов достаточно. К такому выводу приводит отчет о выполнении тестирования по разработанной политике, а также статистика обработки запросов почтовым и Web-сервисами (см. ниже, Рисунок 7). Так, наблюдались следующие значения показателей:

- средний объем входящих сообщений на почтовом сервере — 136 писем/с;
- среднее количество запросов, обрабатываемых в секунду Web-сервером — 172 запросов/с.

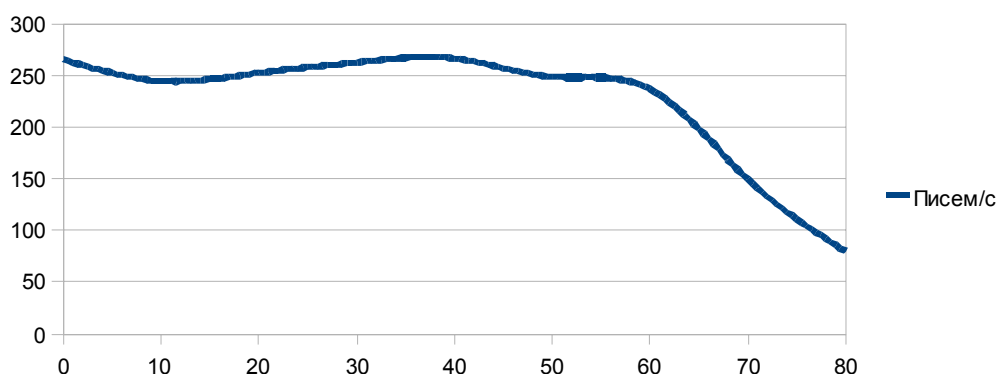
Несомненно, определенные искажения в приведенные усредненные значения внёс период атак. Но даже в то время, когда выполнялись атаки, сервисы оставались доступными, так или иначе.

Но, в реальной жизни редко бывает так просто — «да» или «нет». Часто

возникают детали, которые, на первый взгляд, были либо маловероятны, либо вообще не предусмотрены. Так и в рассматриваемом случае.

## Почтовый сервер

График зафиксированной нагрузки на почтовый сервис имеет следующий вид (см. Рисунок 5):



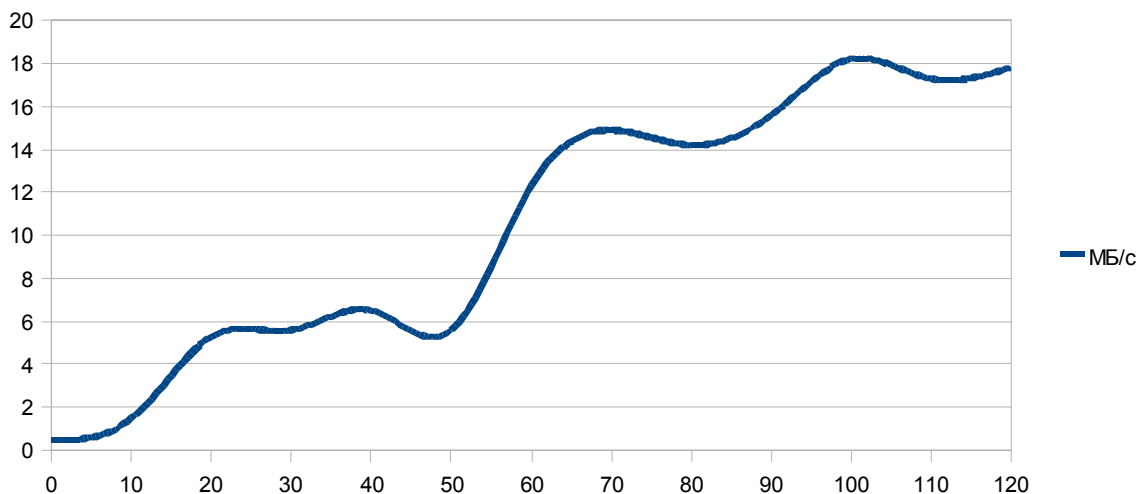
**Рисунок 5. График нагрузки на почтовый сервер**

Для удобства рассмотрения были взяты первые 80 минут тестирования, на которых и проявилась проблема с сервисом. В штатном режиме сервис без проблем справляется с заданным количеством одновременных обращений пользователей, и средний поток писем составляет около 250-300.

Но примерно через час после начала тестирования начинает наблюдаться регрессия показателей производительности сервиса. К концу теста скорость, с которой почтовый сервис принимает письма, падает до 50-80 писем в секунду.

Как видно, производительность падает более чем в 3 раза. Не смотря на то, что даже при таких показателях почтовая система удовлетворяет заданным требованиям, необходимо выяснить, что является причиной подобного поведения.

Для выяснения причины предлагается обратиться к средствам мониторинга ресурсов сервера. Обратив внимание на журнальные сообщения от почтовой службы и на график обращений к жесткому диску (см. Рисунок 6), становится ясно, почему происходит падение производительности:



**Рисунок 6. Частота обращений к жесткому диску почтового сервера**

Как видно на графике (Рисунок 6), со временем в процессе тестирования растет и нагрузка на дисковую подсистему. Проанализировав журнал событий почтовой службы, мы выяснили, что из-за некорректных настроек почтового сервиса на нем начинает накапливаться «мусорная» почта, которую невозможно куда-либо доставить вследствие ошибки в адресе получателя.

И все же сервис периодически пытается доставить эту почту, что приводит к незначительной нагрузке на сам сервер и сеть. Но в нашем случае мы подвергали сервис интенсивной (максимальной) нагрузке в течение нескольких часов, что привело к значительному увеличению количества писем в очереди «недоставляемых», сервис не успевал разбирать очередь, в то время как к нему поступали все новые и новые письма. Указанные обстоятельства и привели к резкой регрессии производительности сервиса.

Что характерно — после прекращения тестирования некорректные письма остаются на сервере и продолжают мешать штатной работе.

К чему может привести такая, незначительная на первый взгляд, проблема? Ошибки в настройках подобного рода могут привести к тому, что в какой-то момент сервер просто перестанет принимать новые письма. И прежде чем это случится — он может проработать год или два, в зависимости от интенсивности поступления на него «мусорных писем».

А интенсивность поступления «мусорных писем» напрямую зависит от активности «спамеров» по отношению к почтовому сервису ИМ. И это не единственная причина, по которой рекомендуется установить серьезную защиту от бесполезных писем.

Ввод в эксплуатацию такой системы не только снизит нагрузку на почтовый сервер и работников ИМ, которым не придется тратить время на фильтрацию входящей электронной корреспонденции, но также, например, снизит риски распространения вредоносного ПО в локальной сети.

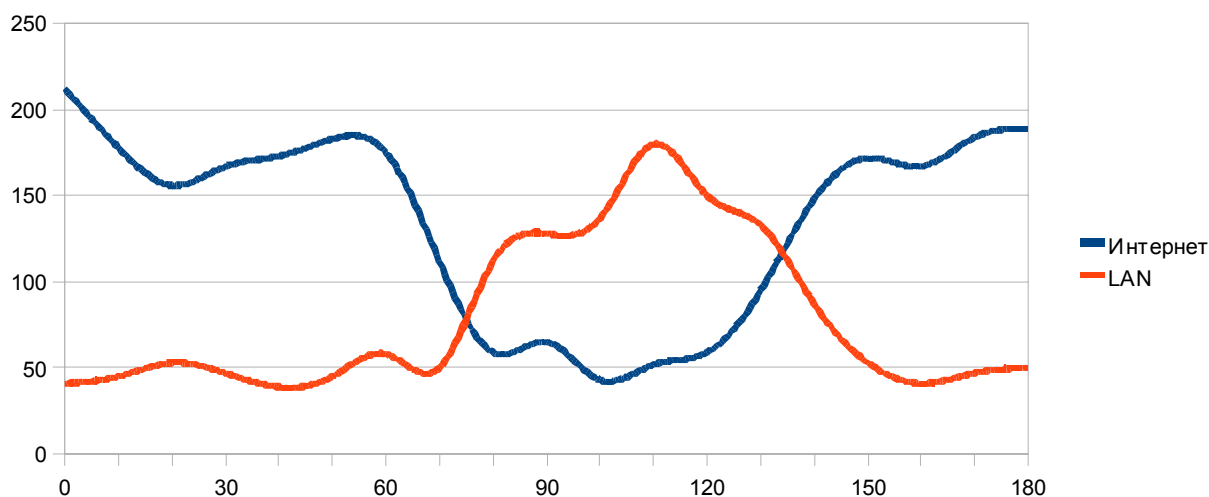
С другой стороны, система защиты от спама — это сервис, для которого проведение нагрузочных тестов является необходимым. Другими словами — это еще один сервис, нарушение работоспособности которого может принести

серьёзные проблемы, а значит необходимо использование средств, позволяющих исключить либо предупредить подобные угрозы.

## Web-сервер

Статистика по Web-сервису показала, что он справляется с 1000-1500 запросов в секунду вне зависимости от наличия/отсутствия внешних атак.

Следует отметить, что наличие атак со стороны сети Интернет не повлияло значительным образом на работоспособность сервиса, но сделало затруднительным получение доступа к сервисам из сети Интернет. Эту особенность можно видеть на графике (Рисунок 7):



**Рисунок 7. Сравнительные частоты обработанных сервисами ИМ запросов из локальной сети и из сети Интернет**

Здесь приведен график запросов, обрабатываемых сервисами компании из локальной сети и из внешней сети (Интернет).

Как видно — на тот момент, когда начинаются атаки со стороны Интернет (отметка «60 мин.») — работоспособность сервисов не нарушается, просто запросы из локальной сети начинают преобладать вследствие «недостаточной доступности» сервисов для пользователей из внешней сети.

Да, с одной стороны это негативный результат. Но с другой — от распределенных атак в обслуживании защититься крайне сложно. И в рассматриваемом случае администраторы ИМ настроили межсетевой экран вполне корректно — атаки внутрь сети не проникли, ограничившись лишь загрузкой канала до внешнего сетевого интерфейса МЭ.

## Межсетевой экран

Несомненно, при оценке результатов проведенных тестов нельзя пропустить анализ собранных данных с межсетевого экрана. И так как именно он разделяет Интернет и внутреннюю сеть, сервисы ИМ, то в случае возникновения проблем с этим узлом сети — работа компании практически встанет.

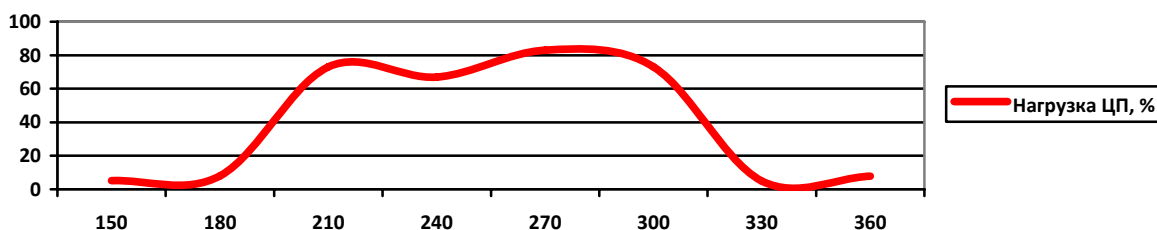
Более того, после расширения компании и открытия филиалов в других

городах планируется продолжить использовать техническую площадку основного ИМ, а значит недоступность сервисов становится критическим ударом по бизнесу всех филиалов, расположенных, в том числе, и в других городах.

Для оценки воздействия нагрузочных тестов на МЭ собиралась следующая статистика:

- нагрузка на сетевые интерфейсы;
- объем используемой оперативной памяти;
- нагрузка на ЦП.

Собранные данные не показали никаких аномалий в графиках по сетевым интерфейсам и используемой памяти, но следует обратить внимание на нагрузку ЦП (см. Рисунок 8):



**Рисунок 8. График нагрузки на ЦП МЭ**

Как видно на графике, с началом атак резко повышается нагрузка на ЦП. Очевидно, что такое поведение вызвано именно атаками, т.к. повышенная нагрузка до неблагоприятного воздействия и штатная нагрузка после – никак не повлияли на ЦП. Значит одна из атак, либо их сочетание стало причиной.

Для того чтобы это выяснить, понадобилось провести 3 непродолжительных дополнительных теста по 10 минут, содержащих:

- отдельно атаку ping-flood;
- отдельно атаку syn-flood;
- одновременно ping- и syn-flood.

Проанализируем результаты дополнительных тестов. Для этого нам потребуется рассмотреть и сопоставить статистику нагрузки на ЦП и сеть для каждого из тестов. Для удобства представим эти данные на одном графике (см. Рисунок 9):

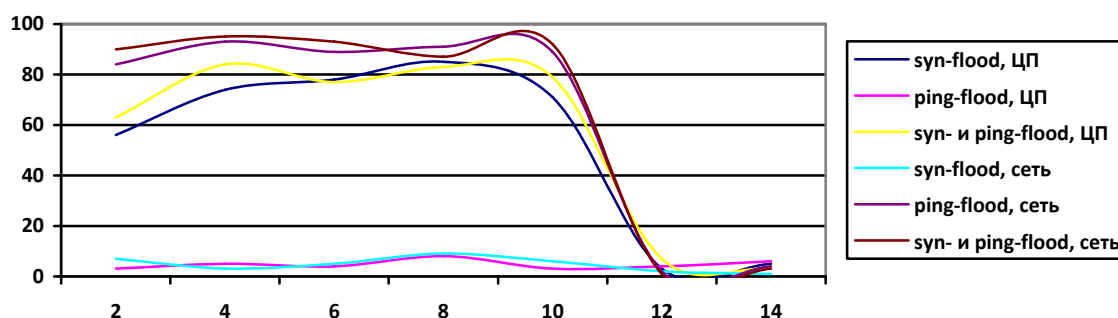


Рисунок 9. Статистика нагрузки на сеть и ЦП МЭ в дополнительных тестах

Анализируя этот график, мы находим подтверждение факта повышенной нагрузки на ЦП межсетевого экрана при одновременном выполнении syn- и ping-flood. Таким образом, убеждаемся, что обнаруженная проблема воспроизводима и является опасной угрозой для сети ИМ.

Теперь рассмотрим воздействие каждой атаки на межсетевой экран по отдельности:

- ping-flood – практически полностью утилизирует пропускную способность сети, но, при этом, не оказывает значительного воздействия на ЦП;
- syn-flood – не оказывает серьезной нагрузки на сеть, но при этой атаке как раз и возникает обнаруженная аномалия нагрузки на ЦП межсетевого экрана.

Итак, проведя 3 дополнительных теста на МЭ, мы обнаружили - атака syn-flood при исходных настройках МЭ вызывает высокую нагрузку (до 80-90%) на центральный процессор межсетевого экрана.

Для устранения обнаруженной проблемы необходимо внести изменения в настройки МЭ, а именно – требуется ограничить допустимое количество запросов со стороны сети Интернет на установку TCP-соединений с сервисами ИМ. Для того, чтобы определить указанное ограничение – можно взять за основу среднее количество запросов/с в часы пиковой нагрузки на сервисы ИМ и умножить это значение на некоторый коэффициент больше единицы, например, на 3.14.

Следует понимать, что выбор этого значения носит во многом эмпирический характер и необходимо учитывать возможность необычайной активности со стороны пользователей Интернет, например, в праздничные дни. Поэтому в ограничение необходимо заложить определенный «резерв», допускающий повышенную нагрузку на сервисы ИМ, но не допускающий угрозу «перегрузки» межсетевого экрана.

После выбора и применения указанного ограничения необходимо провести дополнительные нагрузочные тесты, чтобы убедиться в корректности выбранных настроек.

### **Вывод по результатам тестирования**

По результатам проведенных нагрузочных тестов и анализа полученных данных можно сделать следующие выводы:

- выявлены ошибки в настройках почтового сервиса, которые потенциально могли привести к полному отказу сервиса в будущем. Данные ошибки были

локализованы и устранены;

- проведенные сетевые атаки на сервисы ИМ существенного влияния не оказали и, что самое важное, не нарушили их работоспособность. Во время выполнения атак наблюдалось падение времени отклика сервисов для пользователей из сети Интернет, но это вызвано тем, что атаки практически полностью утилизировали пропускную ширину подключения Интернет. После завершения атак доступность сервисов была полностью восстановлена;

- сетевая атака syn-flood вызвала значительное повышение нагрузки на ЦП межсетевого экрана – до 80%. Даны рекомендации по корректированию настроек МЭ;

- рекомендуется установить систему защиты от СПАМа. Подобная система не только избавит от значительной части нежелательных писем, но и снизит нагрузку на аппаратную платформу почтового сервиса;

- создание повышенной нагрузки на сервисы ИМ в ходе тестов показало, что для планируемого расширения компании существующих ресурсов достаточно.

Таким образом, нагрузочное тестирование не только дало ответы на поставленные вопросы, но и позволило выявить скрытые проблемы, которые могли нанести заметный ущерб бизнесу ИМ в самый неожиданный момент.

Также, после расширения компании (разрастания ее ИТ-инфраструктуры) настоятельно рекомендуется провести как минимум еще одно комплексное тестирование.

## **Заключение**

Несомненно, рассмотренный случай тестирования инфраструктуры Интернет-магазина довольно прост, но тем он и показателен. Ведь мы смогли ознакомиться с основными этапами проведения нагрузочного тестирования, увидели – какие для этого необходимо решить задачи, какие могут возникнуть трудности, к каким результатам можно прийти.

Используя INFORION-NAG, мы не только ответили на поставленные вопросы, но и обнаружили серьезные проблемы в эксплуатируемой инфраструктуре. Более того, мы использовали INFORION-NAG не только как средство, способное помочь в создании требуемой нагрузки на сервисы компании, но и как средство, позволяющее обнаружить и исправить проблемы в их конфигурации и работе.

Рассмотренный пример показывает, что нагрузочное тестирование является средством, предоставляющим возможности:

- контроля качества обслуживания прикладных сервисов;
- контроля обеспечиваемого уровня защищенности СОИБ;
- создания условий эксплуатации, отличающихся от прогнозируемых.

Но сами по себе эти возможности теряют всю значимость, если нет решения, реализующего их. Одним из таких решений является программно-аппаратный комплекс INFORION-NAG.