

## Управление ИТ-ресурсами и рисками становится приоритетной задачей для бизнеса

*Лукашев В.М., СП ЗАО «Международный деловой альянс» (Минск)*

Государственным и отраслевым организациям необходимо обеспечивать соблюдение все большего количества регулирующих норм, касающихся конфиденциальности данных, безопасности и устойчивости бизнеса, поэтому организации осознают особую значимость управления ИТ-ресурсами, определения целевых показателей эффективности ИТ-активов и внедрения стратегий управления рисками для ослабления угроз безопасности и повышения устойчивости бизнеса.

Управление ИТ-ресурсами и рисками становится приоритетной задачей для лидеров глобального бизнеса. Результаты исследований, проведенных недавно корпорацией IBM, свидетельствуют о том, что 79% финансовых директоров намерены в течение ближайших трех лет внедрить структуры управления с целью интеграции информации и обеспечения более глубокого понимания бизнеса, а 64% руководителей ИТ-служб считают соблюдение требований к безопасности и защиту данных одними из наиболее серьезных проблем ИТ-подразделений.

В обзоре известной консалтинговой компании Ernst&Young /1/ отмечается, что в последнее время наметились положительные тенденции по снижению ИТ рисков и их влияния.

Этому способствовали усилия организаций направленные на:

- углубленную интеграцию информационной безопасности,
- расширение применения технологий и средств контроля за соответствием требованиям и стандартам и соблюдения правил в области информационной безопасности,
- расширение применения систем управления рисками контроля за соответствием для 3-х сторон (поставщики, партнеры)
- фокусирование на защите данных.

Обзор основан на результатах опроса около 1200 профессионалов в области информационной безопасности из 48 стран и на примерах решений в более чем 350 организаций из 38 стран.

В то же время результаты нового отчета известной в области ИБ компании Symantec /2/ указывают на то, что большинство респондентов ожидает в ближайшие пять лет какого-нибудь инцидента, связанного с безопасностью или соблюдением правил. В частности, по мнению 66% респондентов, как минимум раз в пять лет будет происходить крупный инцидент, связанный с регулирующими органами. А 58% ожидают в течение пяти лет крупной потери данных, вызванной такими событиями, как авария в вычислительном центре, повреждение данных или нарушение системы безопасности.

Отчет Symantec выявил заметную разницу в восприятии степени подверженности своей организации ИТ-рискам ИТ-персоналом и руководителями ИТ-подразделения. Особенно это касается восприятия риска, связанного как с бизнес-процессом, так и с соблюдением нормативов. Например, 8% ИТ-менеджеров и 22% ИТ-директоров считают важным для своего ИТ-подразделения риск, связанный с бизнес-процессами, и 23% ИТ-менеджеров и 16% ИТ-директоров считают важным риск, связанный с соблюдением нормативов.

Отчет Symantec призван помочь руководителям и ИТ-персоналу разобраться в критических элементах, влияющих на эффективную стратегию в отношении ИТ-рисков. Он основан на данных количественного и качественного исследования, проведенного в

течение 12 месяцев по октябрь 2006 года. Symantec собрала сведения от более чем 500 респондентов, начиная с ИТ-менеджеров и заканчивая высшими ИТ-руководителями, в международных организациях широкого спектра отраслей.

Учитывая важность и актуальность контроля и управления ИТ рисками, практически все ведущие компании в области ИТ технологий и информационной безопасности вышли с новыми инициативами и специализированными решениями.

Среди них мировой лидер в области ИТ корпорация IBM, которая вышла с новыми технологиями и услугами на рынок специализированных решений IT Governance and Risk Management (управление ИТ-ресурсами и рисками), объем которого, по прогнозам, к 2008 году превысит 30 млрд. долларов /3/.

### **Управление ИТ-ресурсами в масштабе всей организации**

Основываясь на самом обширном в отрасли портфеле сервисных и технологических решений, IBM представила новые предложения, позволяющие решать проблемы клиентов, связанные с повышением эффективности и устойчивости бизнеса на основе более эффективного управления ИТ-ресурсами и рисками. Подход IBM к оказанию клиентам помощи в смягчении рисков и эффективном управлении ИТ-ресурсами предусматривает реализацию важнейших стратегических ИТ-инициатив, обеспечение более тесной согласованности ИТ-активов и потребностей бизнеса, а также полный контроль над ИТ-ресурсами на протяжении всего их жизненного цикла. Основное внимание IBM уделяет повышению эффективности и устойчивости бизнеса на основе оптимизации управления сервисами, поддержки непрерывности бизнеса и повышения уровня безопасности.

Кроме того, приобретение компаний Internet Security Systems, Consul, FileNet и Micromuse позволило IBM расширить свой ассортимент решений для управления ИТ-ресурсами и рисками.

### **Управление ИТ-ресурсами в масштабе всей организации**

Комплекс сервисов Business of IT Dashboard позволит клиентам оценить свои сильные и слабые стороны в критически важных областях правления ИТ-ресурсами и рисками, а также связать эффективность ИТ-ресурсов с эффективностью бизнеса. В отличие от других инструментов ИТ-мониторинга, которые, как правило, обеспечивают лишь ограниченное представление о конкретных системах, услуги и программные продукты Business of IT Dashboard (основывающиеся на технологиях IBM Tivoli Netcool) предоставляют всю необходимую информацию, ориентированную на различные категории пользователей, как в ИТ-подразделении, так и за его пределами. Клиенты могут оценивать, планировать, проектировать, внедрять и администрировать приложения реального времени, позволяющие обеспечивать мониторинг ИТ-ресурсов и их использование для повышения эффективности и результативности бизнеса. Кроме того, информационная панель позволяет клиентам согласовывать ИТ-инвестиции с приоритетами и требованиями бизнеса, автоматизировать ИТ-процессы для повышения эффективности, а также оценивать и ослаблять риски нарушения безопасности.

Предложение IT Lifecycle Management and Governance Services for Tivoli Service Desk позволяет клиентам оперативно и легко развертывать комплексные решения для организации службы поддержки пользователей, позволяющие объединить процессы поддержки, обеспечить единую точку контактов для решения ИТ-проблем, повысить уровень доступности средств формирования бизнес-отчетов, а также определять ключевые показатели эффективности. Зачастую служба поддержки является

единственным каналом взаимодействий между ИТ-подразделением и конечными пользователями, поэтому так важно внедрить единый, интегрированный процесс.

### **Принятие обоснованных решений на основе более совершенного управления сервисами**

Новое ПО Tivoli Business Service Manager позволяет повысить эффективность процедур принятия решений, предоставляя специалистам по бизнес-процессам и операциям в реальном времени информацию о важнейших бизнес-сервисах. Это программное обеспечение является первым полностью интегрированным продуктом, объединившим технологии Micromuse с решениями Netcool/Realtime Active Dashboards и Tivoli Business Systems Manager. Tivoli Business Service Manager позволяет получать более полное представление о различных сервисах и процессах в организации с использованием систем показателей для сервисов и ключевых индикаторов эффективности. Специалисты по операциям могут в реальном времени наблюдать за состоянием конкретных устройств или систем, а также обнаруживать ошибки транзакций, узкие места в процессах, отклонения от обычного объема доходов и многие другие проблемы

Управление угрозами безопасности в реальном времени IBM Tivoli Security Operations Manager v4.1 — это платформа для управления событиями в системе безопасности, предлагающая информационную панель реального времени, которая поможет организациям поддерживать работоспособность своих компьютерных сетей и систем, несмотря на угрозы безопасности, вызванные действиями внешних злоумышленников, постоянных или временных сотрудников. Это программное обеспечение в автоматическом режиме анализирует данные, поступающие от всех компонентов ИТ-инфраструктуры, позволяя выявлять угрозы безопасности, оптимизировать и автоматизировать процессы обнаружения инцидентов, их анализа и выполнения необходимых ответных действий. Обеспечивая мониторинг соблюдения политик сетевой безопасности и выполнения мер контроля над ИТ-ресурсами, это решение помогает пользователям быстро выявлять и исключать угрозы безопасности и случаи нарушения политик, до того как они превратятся в инциденты, а также формировать специализированные отчеты об операциях и соблюдении нормативных требований.

### **Регулирование инвестиций в рамках жизненного цикла ИТ-сервисов**

IBM Rational Portfolio Manager v.7.1 является корпоративным решением для управления проектами, которое может использоваться любым сотрудником организации — руководителями ИТ-подразделения, менеджерами проектов, бизнес-аналитиками, разработчиками, — для регулирования ИТ-инвестиций и определения приоритетов в обслуживании. Новый интерфейс на базе технологий Web 2.0 позволяет участникам коллектива управлять своей работой и представлять отчеты о графиках и расходах, а тесная интеграция между ПО Rational Portfolio Manager и портфелем технологий IBM Rational помогает соблюдать графики разработки, тестирования, развертывания и ввода в эксплуатацию программного обеспечения. Аналитический компонент Rational Portfolio Manager поддерживает автоматизированные циклы принятия и утверждения решений в группах разработчиков программного обеспечения, а также позволяет выявлять тенденции и пересечения в рамках проектов. Проектные коллективы могут повысить эффективность, используя новые шаблоны и лучшие методики, позволяющие формировать отчеты о соблюдении требований и упростить запуск проектов.

## Централизованное управление защитой предприятия

Многие предприятия в мире находятся на этапе преобразования, который подразумевает обеспечение использования новых возможностей Интернета и электронного бизнеса. В последнее время было развернуто множество систем электронного бизнеса, что привело к тому, что все больше корпоративных систем, приложений и данных становятся доступными из Глобальной сети, вследствие чего компании сталкиваются с возрастающим числом различных угроз для информационной инфраструктуры — вирусной опасностью, несанкционированным доступом, атаками типа «отказ в обслуживании» и другими видами вторжений, мишенью для которых становятся приложения, сети, инфраструктура хостинга, серверы и рабочие станции. В условиях жесточайшей конкуренции заказчики предъявляют высокие требования к поставщикам решений, а их ожидания в части обслуживания, конфиденциальности и безопасности также имеют очень высокий уровень. Реализации решений для электронного бизнеса должны обеспечивать хорошую защиту, конфиденциальность транзакций, предоставлять защиту целостности выполнения деловых операций и данных заказчиков, а также гарантировать постоянный непрерывный доступ к данным. Компании, приложившие значительные усилия для создания надлежащего имиджа и получения признания на рынке, отдают себе отчет в том, что успешная атака на Интернет-ресурсы компании может свести на нет все эти усилия. Программное решение IBM Tivoli Risk Manager позволяет централизованно управлять и реагировать на различные угрозы для защиты системы и попытки вторжения, направленные на информационные ресурсы предприятия.

## Централизованное управление рисками

Tivoli Risk Manager позволяет обрабатывать уведомления об угрозах посредством одной консоли защиты. С помощью центра управления и обеспечения связи можно централизованно управлять наиболее незащищенными компонентами системы, выявлять и пресекать атаки, угрозы и различные внешние воздействия благодаря наличию средств сбора информации и данных об угрозах от брандмауэров, маршрутизаторов, сетей, систем обнаружения проникновения для приложений и узлов, рабочих станций, а также средств сканирования незащищенных компонентов системы. Программное обеспечение Tivoli Risk Manager содержит следующие функции, позволяющие централизованно управлять рисками:

- централизованная обработка сообщений о вторжениях;
- централизованное архивирование сообщений защиты в реляционной базе данных;
- масштабируемая инфраструктура управления событиями, позволяющая управлять событиями на тысячах различных устройств;
- единая консоль предприятия, позволяющая аналитикам, обрабатывающим сообщения от средств защиты, работать со всеми сообщениями и быстро создавать реализации стратегий управления рисками;
- поддержка принятия решений, в состав которой входят подготовленные отчеты для управления брандмауэрами, определения вторжений, управления рисками, борьбы с вирусами и создания шаблонов отчетов Tivoli Ready.

## Tivoli Network Intrusion Detection System

Мощная система обнаружения вторжений Tivoli Network Intrusion Detection System распознает более 200 различных типов атак и занимает весьма мало места на диске. Основным преимуществом данной системы является тесная интеграция с Tivoli Enterprise

Console и платформой управления Tivoli. Администраторы системы могут развернуть систему обнаружения вторжений, создавать новые шаблоны и стратегии, а также централизованно рассылать защитный код с помощью центральной консоли.

### **Tivoli Web Intrusion Detection System**

В состав программного обеспечения Tivoli Risk Manager входит высококлассная система обнаружения вторжений Tivoli Web Intrusion Detection System (Tivoli Web-IDS), которая позволяет отслеживать факты несанкционированного проникновения в систему и различные виды атак на Web-серверы. Сегодня при проведении атак часто используются сложные средства, с помощью которых обращение к Web-серверам выполняется по протоколам HTTP или HTTPS. Как правило, такие атаки невозможно заблокировать с помощью брандмауэров и специальных средств обнаружения вторжений. Система Tivoli IDS предназначена для обработки следующих событий: проникновение в систему, атаки на средства обслуживания заказчиков, разрешенные, но нежелательные действия. Кроме того, Tivoli IDS повышает степень защиты объектов CGI. Система Tivoli WebIDS поддерживается рядом популярных программных Web-серверов.

### **Поддержка продуктов Tivoli Ready**

Программное обеспечение Tivoli Risk Manager поддерживает работу с рядом продуктов для обеспечения безопасности систем нескольких основных поставщиков услуг. Tivoli Risk Manager также предоставляет поддержку внешнего программного обеспечения и агентов ISS Real Secure Network, Cisco Secure IDS, маршрутизаторов Cisco, продуктов Check Point FireWall-1, McAfee Acitve Virus Defense Suite и Symantec Norton AntiVirus. Решения, поддерживающие работу с Tivoli Risk Manager и имеющие соответствующий логотип, поставляются несколькими независимыми производителями программного обеспечения и услуг: Argus System Group, Click Net Security Technology, LockStep Systems, Deloitte & Touche, Zone Labs, Compaq, SRA International и IBM eServer pSeries. Набор этих решений помогает создать реализацию полной инфраструктуры защиты информационной системы предприятия и обеспечить безопасность всех приложений электронного бизнеса и информационных ресурсов на случай информационных атак.

### **Необходимость совершенствования и проверки систем безопасности**

Твердо проводя в жизнь целостную политику защиты в масштабах предприятия, удается избежать до 90 процентов инцидентов, связанных с безопасностью. Пакет IBM Tivoli® Security Compliance Manager действует как система раннего предупреждения, помогая малым, средним и крупным предприятиям идентифицировать нарушения политики защиты и потенциальные системные уязвимости задолго до появления реальной угрозы. Он предлагает предприятиям быстрый, рентабельный и действенный способ сбора и обработки информации о состоянии защиты корпоративных систем.

Предприятиям также приходится все больше внимания уделять соблюдению корпоративной политики, отражающей растущее число правительственных нормативных актов, нацеленных на поддержание целостности и безопасности данных. Необходима специальная система, проверяющая соблюдение корпоративной политики.

## **Автоматизированная проверка систем защиты на соответствие требованиям безопасности**

Ручные проверки системы защиты часто занимают несколько дней и требуют значительных материальных и трудовых затрат. К сожалению, они подвержены человеческим ошибкам и не всегда выполняются с нужной степенью полноты. Tivoli Security Compliance Manager построен на основе концепции автоматизации по требованию, которая является одной из центральных программных стратегий IBM, завоевавших широкое признание и выдержавших проверку временем. Автоматизированные централизованные проверки систем защиты обычно занимают всего лишь несколько минут. Это освобождает администраторов от выполнения отнимающих массу времени рутинных функций, помогая максимизировать эффективность, сэкономить средства и минимизировать риск человеческих ошибок. Для того, чтобы быстро начать работу, Tivoli Security Compliance Manager содержит шаблоны политик безопасности. Клиенты могут легко изменить эти политики или создать новые в соответствии с потребностями своей организации.

## **Проверенные практикой лучшие политики – составная часть пакета Tivoli Security Compliance Manager**

Вместе с пакетом Tivoli Security Compliance Manager поставляются проверенные практикой лучшие политики безопасности и готовые к использованию отчеты. Построенный на гибкой, масштабируемой платформе Java, пакет позволяет пользователям настраивать имеющиеся шаблоны, формируя тщательно выверенные и хорошо осмысленные политики безопасности. При помощи графического интерфейса администратор безопасности может эффективно получить “снимки” политики, чтобы проверить ее соблюдение в рамках предприятия, выявить нарушения защиты, предупредить виновников и принять меры к ее восстановлению. Пакет использует цветовое кодирование – выявленные нарушения выделяются красным, желтым и зеленым цветом, подобно сигналам светофора. Администратор с первого взгляда может определить, какие системы в рамках предприятия имеют неверно установленные пароли, устаревшие файлы вирусных сигнатур, устаревшие системные обновления, опасные или ненужные службы и т.д. Проверка соответствия дает полную картину того, где и как были устранены нарушения, и позволяет убедиться в соблюдении политик.

## **Сокращение числа сложных и дорогостоящих процессов при оптимизации производительности**

Поставляемые вместе с пакетом шаблоны политик безопасности помогают свести к минимуму отнимающие много времени и дорогостоящие процессы, обычно связанные с созданием набора процедур проверки соответствия. Эти готовые политики обеспечивают администратору безопасности хороший задел и позволяют избежать синдрома “начала на пустом месте”, который в начале проекта может стать столь обескураживающим. Tivoli Security Compliance Manager осуществляет автоматизацию по требованию, заменяя дорогостоящую и утомительную ручную проверку безопасности серверов автоматизированной проверкой политик безопасности. Благодаря автоматизации удастся существенно сократить затраты времени на управление политиками безопасности, проверку соответствия и ревизию систем защиты.

Дополнительная экономия может также проявиться в результате обнаружения потенциальных дефектов защиты в системах IBM AIX®, Solaris, HP-UX, Microsoft®

Windows®, Linux и Linux для zSeries прежде, чем произойдет дорогостоящий инцидент нарушения безопасности.

Принципы Autonomic computing, заложенные в основу пакета Tivoli Security Compliance Manager, включают функцию самопроверки, которая автоматически посылает периодические импульсы с контролируемых конечных точек на центральный сервер, сигнализируя о том, что все системы функционируют должным образом. Концепция Autonomic computing создает программной системе условия для самоуправления и автоматического обновления конечных точек, построенных по технологии Java. Являясь частью инициативы IBM для электронного бизнеса по требованию, этот автоматизированный подход к проверке политики безопасности помогает нашим клиентам сохранять устойчивость и адаптироваться к угрозам.

### **Интеграция с продуктами IBM Tivoli для автоматизированного управления средствами безопасности**

Tivoli Security Compliance Manager обменивается информацией, относящейся к нарушениям защиты или несоблюдению политик, с другими автоматизированными инструментальными средствами управления безопасностью, входящими в семейство продуктов Tivoli, что помогает устранить нарушения политик безопасности и связанные с ними риски. Используя Tivoli Security Compliance Manager совместно с другим программными средствами Tivoli, такими как IBM Tivoli Risk Manager, IBM Tivoli Enterprise Console® и IBM Tivoli Configuration Manager, предприятие может принять меры, направленные на предотвращение ущерба и устранение нарушений политики безопасности. Tivoli Security Compliance Manager может работать в тандеме с этими решениями Tivoli, останавливая ненужные службы, изменяя полномочия, обновляя ПО и развертывая пакеты обновлений.

Кроме того, в 2007 году IBM представила ряд технологий и услуг, позволяющих удовлетворить потребности в передовых решениях для управления ИТ-ресурсами и рисками, в том числе:

- усовершенствования архитектуры безопасности мэйнфрейма System z™;
- сотрудничество с Cisco с целью предоставления средств реагирования на чрезвычайные ситуации впервые в виде комплексного управляемого сервиса;
- сервисы цифрового видеонаблюдения;
- расширенный ассортимент систем предотвращения вторжений IBM Internet Security System (ISS) и портфель Managed Security Services с новыми сервисными продуктами для компаний малого и среднего бизнеса;
- программная платформа IBM FileNet P8 4.0 Enterprise Content Management;
- новые предложения подразделения IBM System Storage, позволяющие более эффективно справляться с ростом объемов информации, контролировать расходы и обеспечивать хранение информации для целей управления данными или соблюдения нормативных требований.

### **Резюме**

Управление ИТ-ресурсами и рисками становится приоритетной задачей для лидеров глобального бизнеса. Основываясь на самом обширном в отрасли портфеле сервисных и технологических решений, IBM представила новые предложения, позволяющие решать проблемы клиентов, связанные с повышением эффективности и

устойчивости бизнеса на основе более эффективного управления ИТ-ресурсами и рисками.

Компания «Международный деловой альянс», являясь Премьер партнером IBM, активно продвигает комплексные решения на основе технологий IBM для углубленной интеграции ИТ и бизнес систем и минимизации влияния и снижения ИТ рисков на бизнес предприятий. Эти решения включают построение отказоустойчивых, высокодоступных и катастрофоустойчивых центров обработки данных для критически важных бизнес систем, хранилищ данных, электронных архивов, комплексных систем безопасности, комплексных систем управления ИТ ресурсами и автоматизированных систем контроля за соответствием современным требованиям.

Кроме того, компания «Международный деловой альянс» активно участвует в разработке решений IBM в рамках новых инициатив, среди которых можно выделить участие в разработке и внедрению автоматизированной системы контроля за соответствием Политик безопасности IBM Tivoli® Security Compliance Manager.

Обзор технологий и решений подготовлен по материалам компании IBM,. Дополнительную информацию о решениях, представленных технологиях и сервисах управления ИТ-ресурсами и рисками можно найти на Web-страницах:

<http://www.ibm.com>

<http://www-03.ibm.com/press/us/en/presskit/21544.wss>,

[http://belarus.iba.by/iba\\_web/main.nsf/solutions/ru.sit.html](http://belarus.iba.by/iba_web/main.nsf/solutions/ru.sit.html)

### **Использованная литература**

1. Отчет компании Ernst&Young: Global Information Security Survey 2006 «Achieving Success in a Globalized World: Is Your Way Secure?»
2. Отчет Semantec «IT Risk Management Report», Trends Through December 2006, v.1, February 2007.
3. Аналитический отчет AMR Research «Market Demand for Governance, Risk Management and Compliance, 2007-2008».
4. Лукашев В.М., Трубачев С.В., Томко Д.В. Решение ИВА в области контроля политик безопасности корпоративных информационно-вычислительных систем // Управление защитой информации. – 2005.Т.9. № 4 С. 446-451.