УДК 004.056.5: 004.775

Б.А. БАБИЧ, А.В.САГУН, канд. техн. наук, О.А. КОЖУХОВСКАЯ, канд. техн. наук, А.Д. КОЖУХОВСКИЙ, д-р техн. наук

СИНТЕЗ СИСТЕМЫ МНОГОУРОВНЕВОЙ ЗАЩИТЫ КОРПОРАТИВНЫХ ПОРТАЛОВ НА ПЛАТФОРМЕ MS SHAREPOINT

Введение

Для IT, развивающихся в режиме нон-стоп, очень характерна проблема определения лидирующей платформы корпоративного портала, когда маркетинговая информация о продукте или технологии преобладает над какой-либо другой. Эта проблема особенно остро ощущается в сегменте программного обеспечения (ПО) для бизнеса. Яркий пример – *корпоративный портал* [1].

Под корпоративным порталом будем понимать видимую для пользователей внутреннюю часть сети организации. Корпоративный портал может включать в свой состав корпоративный сайт либо персональные сайты для сотрудников компании, может быть частью корпоративной информационной системы (КИС) и, собственно, КИС, обеспечивая одновременно единый доступ к информации и приложениям компании, совместную работу и управление знаниями, защиту и конфиденциальность коммерческой информации и коммерческой тайны [2].

Платформа MS Share Point представляет собой лидирующий на рынке продукт, который обеспечивает всё необходимое для развитого корпоративного портала – набор технологий, основанных на серверной операционной системе MS Windows Server, Internet Information Server, Windows Share Point Services. В качестве хранилища данных, предоставляющего возможность масштабируемости и надежности, используется MS SQL Server.

Цель исследования – изучение вопроса построения многоуровневой системы защиты для корпоративных порталов на платформе MS Share Point при помощи интегрируемого программного обеспечения Microsoft; определение алгоритма построения защищенной облачной системы универсального типа.

Моделирование защищенного корпоративного портала

На базе универсальной топологии Share Point, которая сочетает три различные архитектуры (IIS, .NET и SQL Server) [2] разработана оптимальная топология корпоративного портала с наиболее полным функциональным набором компонент [3] (рис. 1), которая может обеспечить выполнение задач сотрудников компании среднего бизнеса с учётом требований защиты информации.

Режим изоляции рабочих процессов используется в IIS по умолчанию. Режим изоляции рабочих процессов позволяет использовать преимущества архитектуры IIS 6.0 при определении групповых политик безопасности: устойчивая работа приложений в группах; учитывать автоматические перезапуски, масштабируемость, отладку и точную настройку производительности системы. Веб-приложения выполняются с удостоверением сетевой службы, которое обеспечивает повышенную безопасность в рамках субъект-субъективной модели доступа: учетная запись сетевой службы имеет меньшие права доступа, чем учетная запись локального компьютера. Актуальность включения данного режима особенно актуальна при синтезе систем многоуровневой защиты корпоративных порталов на базе продуктов Microsoft. Такой режим нужно использовать при изоляции рабочих процессов, если не требуется запуск приложений, которые могут конфликтовать с ним, что характерно для защиты корпоративных порталов.

Таким образом, определены основные узлы системы:

- Front-end Web Server (Share Point server 2010; обработка запросов пользователей);
- Application Server (Share Point server 2010, средства аналитики; обработка запросов пользователей);
- SQL Server (Share Point Data Bases, Data Warehouses, средства аналитики; хранение информации, статистическая обработка);
- Domain Controller Server (Active Directory; учет пользователей Share Point фермы).

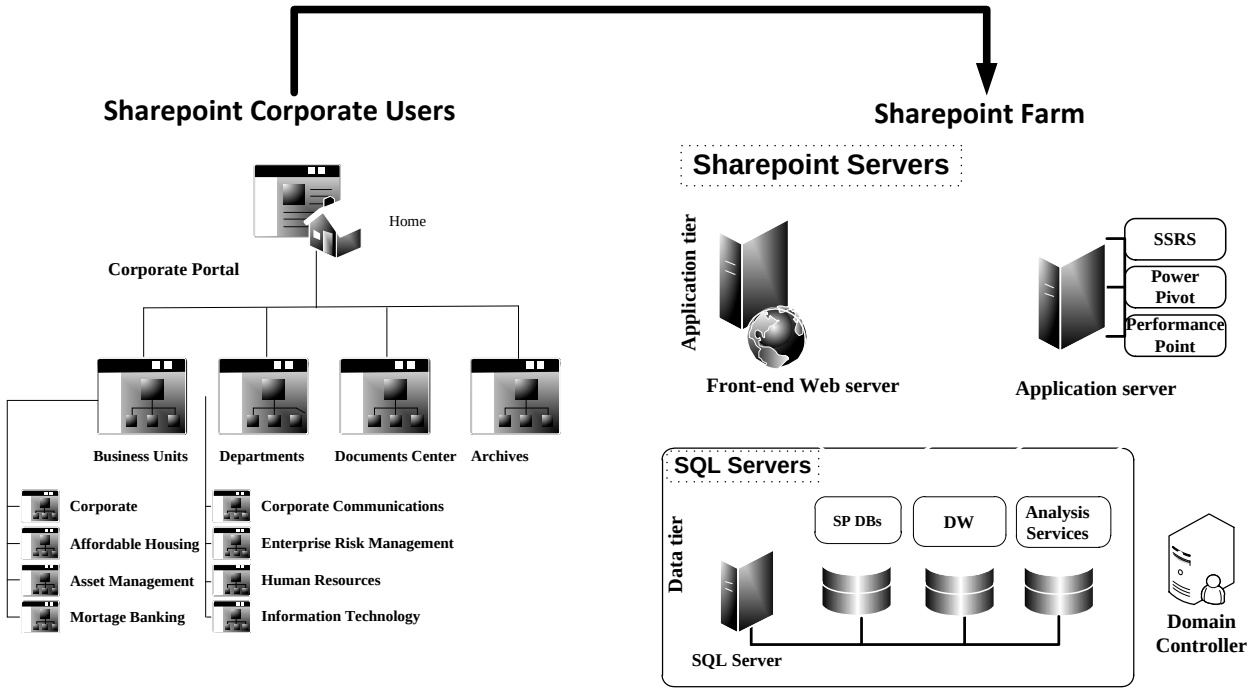

Рис. 1. Функциональная схема взаимодействия и обработки задач клиентов предложенной конфигурации на базе универсальной топологии Share Point Farm

В результате практической реализации, предложенной на рис. 1, конфигурации развернут тестовый портал, который может успешно масштабироваться и обрабатывать задачи пользователей корпораций среднего и большого бизнеса. Позволяет гибкую настройку рабочих областей для каждой рабочей группы и разделяемых ресурсов.

Анализ многоуровневой защиты предложенной системы

Рассматривая вопросы безопасности облачных систем, к которым относится данная разработка, необходимо проанализировать методы и принципы, которые предоставят пользователям системы максимальный уровень защиты для их персональных данных. Представленная система корпоративного облачного портала, согласно НД ТЗІ 2.5-005 -99, относится к АС класса 3 с повышенными требованиями к обеспечению конфиденциальности, целостности и доступности обрабатываемой информации [4]. Принципы защиты подобных систем определяются мощностью средств контроля и зависят от конфиденциальности ресурса. Одной из главных особенностей систем данного вида является то, что большинство ресурсов могут быть виртуализированы.

Таким образом, клиенты, пользующиеся службами, размещенными в облаке, могут иметь ресурсы, которые невозможно связать с физическим объектом – данные могут храниться виртуально и распределяться по нескольким местоположениям.

При внедрении системы было выяснено, что данный факт приводит к изменениям анализа рисков и применения элементов контроля безопасности к традиционным уровням многоуровневой защиты: оборудование, сеть, доступ к удостоверениям, авторизация доступа и аутентификация, хостинг.

Принцип многоуровневой защиты является базовым элементом в предоставлении защищенной облачной инфраструктуры. Применение средств контроля на нескольких уровнях подразумевает задействование механизмов защиты, разработку стратегий по снижению риска и способность реагировать на атаки в случае их возникновения. Использование комплекса мер обеспечения безопасности различной силы (в зависимости от конфиденциальности защищаемого ресурса) приводит к повышению эффективности предотвращения проникновения в систему и снижению негативного влияния инцидента безопасности.

Разумеется, при этом по-прежнему необходимо предпринимать меры обеспечения физической и сетевой безопасности. Однако важнейший момент управления рисками смещается в сторону уровня объекта и элементов, используемых в облачной среде: контейнеров хранилищ статических или динамических данных, объектов виртуальных машин, сред выполнения, в которых производятся вычисления.

Корпорация Microsoft обеспечивает определение внешнего и внутреннего периметров и усиление средств защиты на каждом слое периметра [5, 6]. На рис. 2 отображены продукты Microsoft, которые способны предоставить безопасность для центров обработки данных, сетевого оборудования и средств связи представленной на рис. 2 системы в следующем:

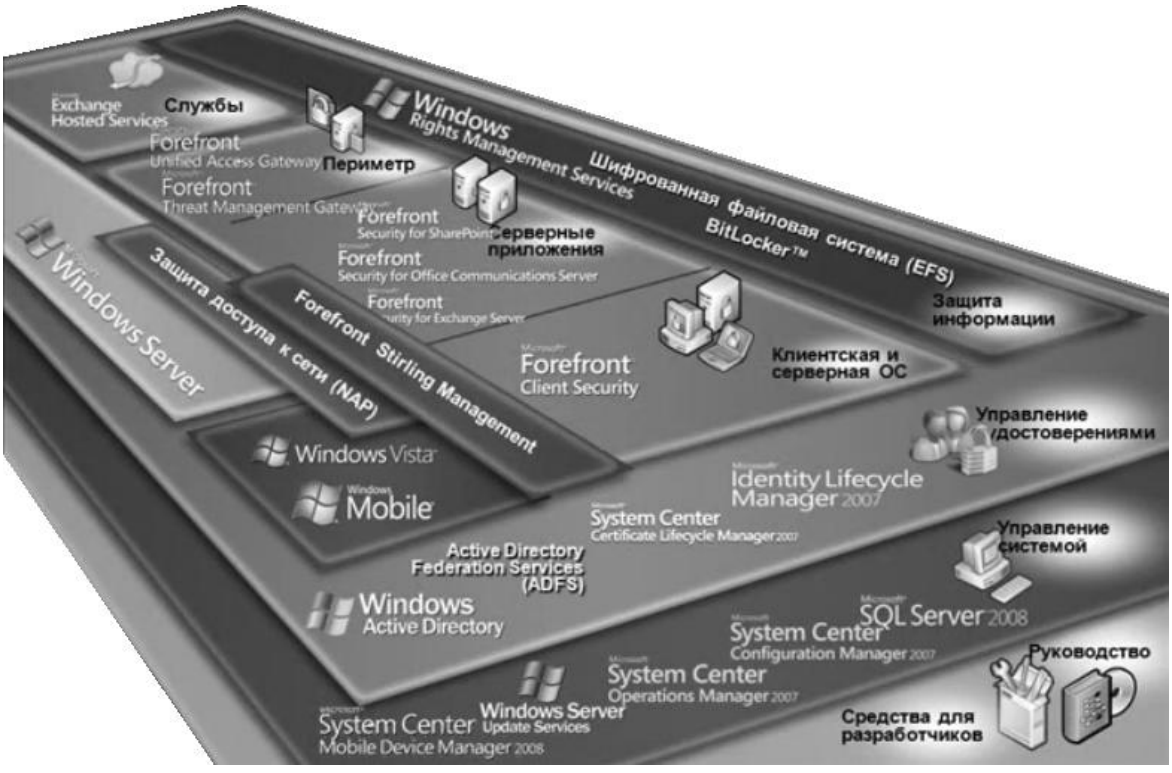

Рис. 2. Программные продукты для обеспечения многоуровневой защиты

- защита клиентской и серверной операционных систем;
- управление удостоверениями;
- управление системой;
- защита доступа к сети передачи данных;
- контроль работы служб и серверных приложений.

В представленной разработке было применено несколько уровней безопасности для устройств центров обработки данных и сетевых подключений. Например, элементы контроля безопасности используются как для контроля, так и для управления. Имеется специализированное оборудование (например, балансировку нагрузки выполняет, параллельно своим основным задачам, Web-Frontend) для управления потоками данных.

Заключение

Упомянутые принципы обеспечения безопасности для сред облачных вычислений, а именно координированное и стратегическое их использование для процессов и технологий позволяет облачной инфраструктуре адаптироваться к стремительным изменениям в сфере IT-технологий в рамках построения защищенных информационных систем.

Посредством этих программных продуктов возможно создать комплексную инфраструктуру обеспечения и контроля безопасности, обеспечивающих необходимый уровень надежности, ожидаемый заказчиками, и соответствие действующему международному стандарту ISO/IEC 27001:2005 [7] с повышенными требованиями к обеспечению конфиденциальности, целостности и доступности обрабатываемой информации.

Список литературы: 1. *Стратегия* построения защищенных информационных систем (Trustworthy Computing) корпорации Microsoft: http://www.microsoft.com/twc. 2. *Уведомление* корпорации Microsoft о конфиденциальности в сети: http://www.microsoft.com/privacy. 3. *Сертификат* ISO 27001: 2005 группы Microsoft Global Foundation Services: http://www.bsiglobal. com/en/Assessment-and-certification-cervices/Client-directory/CertificateClient-Directory-Search-Results/?pg=1&licencennumber= lS+533913& searchkey=companyXegXmicrosoft. 4. *Microsoft* Clobal Foundation Services:http://www.globalfoundation services.com. 5. *Процесс* Microsoft Security Development Lifecycle (SDL): http://www.microsoft.com/en us/library/cc307748.aspx. 6. *Центр* Microsoft Security Response Center: http://www.microsoft. com/security/msrc. 7. *Службы* Microsoft Online: http://www.microsoft.com/online

Черкасский государственный
технологический университет

Поступила в редколлегию 15.09.2012