Nf – количество документов, найденных по запросу (из них Nrf документов релевантны запросу).

Полнота и точность, полученные по отдельным запросам, усреднены и сведены в приведенную ниже таблицу:

	Исходный поиск	Ассоциативный поиск
Полнота	0,74	1,0
Точность	0,96	0,89

Отметим, что за счет ассоциативных отношений заметно выросла полнота поиска при относительно небольшом падении точности. Отсюда можно сделать вывод о целесообразности использования автоматически построенных ассоциативных отношений в системах с нечетким поиском.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Сэлтон Г.* Автоматическая обработка, хранение и поиск информации. – М.: Советское радио, 1973. – 560 с.
2. *Маркусова В.А.*, *Реброва М.П.*, *Страшко В.П.* Особенности интерактивного поиска проблемно-ориентированной информации в базе данных SCI-SEARCH. НТИ. Сер. 2, № 3, 1988. С. 26–30.
3. *Ашманов И.*, *Григорьев С.*, *Гусев В.*, *Харин Н.*, *Шабанов В.* Применение статистических методов для интеллектуальной компьютерной обработки текстов / Труды Международного семинара Диалог'97 по компьютерной лингвистике и ее приложениям. Ясная Поляна, 10–15 июня 1997 г. С. 33–37.
4. *Солтон Дж.* Динамические библиотечно-информационные системы. – М.: Мир, 1979.
5. *Ашманов И.*, *Харин Н.* Интеллектуальные технологии обработки текстов. Электронный офис, май-июнь 1997, С. 24–25.
6. *Y. Qui*, *H.P. Frei*. Concept based query expansion. ACM SIGIR, 1993.

Е.А Ломако

О НЕКОТОРЫХ АСПЕКТАХ БЕЗОПАСНОСТИ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Современные информационные системы (ИС) *представляют собой комплексные программно-аппаратные решения*, базирующиеся на различных технологиях и способах их реализации. Так, для большинства ИС будет верно распределение составляющих их элементов по следующим ролям:

- хранение и обработка данных;
- представление данных;
- доступ к данным.

Роль хранения и обработки данных обычно выполняют различные базы данных. Применение той или иной системы хранения обусловлено различными факторами, в том числе: объёмом данных, сложностью их обработки, требуемой скоростью обработки и обмена данными, совместимостью с другими подсистемами и т. д. Наиболее значимые на рынке продукты представлены компаниями Oracle, Microsoft, IBM.

Системы представления данных обычно реализованы по клиент-серверной технологии и обеспечивают работу с хранимыми данными. В последнее время наиболее популярной реализацией системы представления данных является информационный портал, работа которого основана на множестве различных технологий, активно применяемых в сети Интернет. На стороне сервера приложений используются технологии Java, ASP, PHP. На стороне клиента – XHTML, XML, JavaScript, Flash. В последнее время все активнее используется технология AJAX, позволяющая производить динамическое обновление данных на стороне клиента без полной перезагрузки отображаемой страницы.

Связующим звеном между клиентами и порталами, между составными частями портала, а также между различными порталами служит сеть передачи данных. Элементы телекоммуникационной инфраструктуры обеспечивают доступ пользователей и элементов информационных систем к хранимым данным. По зонам доступа разделяют три основных сегмента сети:

- Интернет (глобальный доступ к данным подавляющего большинства пользователей мировой сети);
- экстранет (доступ к данным ограниченного числа пользователей, например, сотрудников одной компании, по публичным каналам связи);
- интранет (доступ пользователей, размещенных в пределах локальной сети).

В каждой из указанных зон применяются различные технологии организации связи и, как следствие, – оборудование различных производителей, среди которых наиболее популярны Cisco Systems, HP, Bay Networks, ZyXEL, Nortel.

Действующие отраслевые, международные и национальные стандарты способствуют интеграции технологических решений от различных производителей. В то же время сложность современных информационных систем требует рассматривать их как ненадежную совокупность надежных элементов.

Как правило, жизненный цикл автоматизированной системы связан с наращиванием ее функциональности. При этом данный процесс затрагивает, фактически, все подсистемы: с ростом объёма данных модернизируется подсистема хранения данных, изменение и расширение функций приложения реализуются на уровнях представления и хранения, подключение новых групп пользователей выполняется путём изменений уровня доступа. *Потребности бизнеса превращают жизненный цикл автоматизированных систем в постоянный процесс обновления состава и реализаций используемых технологий.* Оборотной стороной такого процесса является *снижение эффективности систем вследствие деградации их надежности и общего уровня информационной безопасности*. Таким образом, модернизация ИС должна рассматриваться в виде комплексной задачи, учитывающей все факторы, влияющие на эффективность ее функционирования.

Анализ современной проблематики в области информационной безопасности показывает, что к основным факторам, влияющим на безопасность развивающихся ИС, следует отнести:

- наличие ошибок в новых реализациях программ и устройств;
- свободная трактовка производителями принятых стандартов;
- рост числа используемых в ИС технологий;
- рост числа элементов ИС;
- рост числа пользователей;
- изменение профилей и регламентов безопасности в связи с изменившимися возможностями и потребностями элементов ИС.

Зачастую в конкурентной борьбе решающим фактором является срок появления того или иного продукта. Производители, заинтересованные в росте продаж своих продуктов, стремятся выйти на рынок раньше своих конкурентов, в результате цикл окончательного тестирования зачастую совпадает с началом эксплуатации. Это дает возможность злоумышленникам воспользоваться несовершенством продуктов для достижения своих целей. Принимая во внимание ограниченную ответственность производителей, данный фактор необходимо учитывать в политике безопасности ИС.

Отраслевые стандарты определяют границы ответственности тех или иных подсистем, протоколов и технологий, накладывают ограничения на их реализацию и использование. В результате совокупность стандартов гарантирует непротиворечивость и полноту системы, построенной с их соблюдением. Однако для производителей такие границы и ограничения не всегда являются приемлемыми как в отношении стоимости их реализации, так и с учётом маркетинговой политики. Производители заинтересованы в расширении рынка. Точное соблюдение стандартов лишает их конкурентных преимуществ перед сторонними производителями смежных продуктов. В итоге, отдельные реализации, формально соответствующие стандартам, приобретают полноценность и достаточность только при использовании комплексного решения от одного производителя.

Добавление новых технологий в реализацию ИС ведет к ее усложнению, что повышает вероятность наличия технологических несовместимостей.

Рост числа элементов ИС экстенсивно влияет на трудозатраты по их эксплуатации и, тем самым, повышает влияние человеческого фактора на безопасность систем.

Рост числа пользователей статистически повышает риск деструктивных действий с их стороны.

Любые изменения в структуре ИС требуют пересмотра правил и политик, выполнение которых при эксплуатации требуется для обеспечения безопасности. Эффективность такого пересмотра должна в обязательном порядке подлежать экспертной оценке, в противном случае безопасность системы должна быть признана недостаточной. Кроме того, в реализации новых правил и политик всегда присутствует человеческий фактор: администраторы должны правильно настроить отдельные элементы ИС, а пользователи соблюдать правила в части, касающейся их. Следовательно, на этапе внедрения и начальной эксплуатации риск несоблюдения требований безопасности довольно высок, что также снижает безопасность систем в целом.

Таким образом, все *перечисленные выше факторы объективно обоснованы и могут использоваться в качестве базиса для оценки безопасности ИС*.

Принимая сложившиеся правила существования и развития рынка, IT-сообщество, в состав которого входят стратеги, производители, интеграторы и пользователи, *выработало несколько универсальных подходов к созданию эффективных информационных систем*.

Безопасность информационных систем рассматривается как *разделенная на уровни подсистема*. Каждый из уровней безопасности соотнесен с одной или несколькими ролями и, соответственно, элементами ИС. При этом отдельный уровень безопасности попадает в зону ответственности отдельного производителя, что положительно влияет на качество его реализации. Такой подход создаёт благоприятные условия для эффективной оценки подсистемы безопасности, однако не решает остальных проблем.

Следующим шагом на пути повышения эффективности ИС является *применение стандартных решений*, предоставляемых системными интеграторами. В

этом случае опытные эксперты создают высокоэффективные схемы взаимодействия элементов ИС, а многократное их применение позволяет накопить достаточный опыт эксплуатации и подготовить исчерпывающую консультационную и регламентную базы. Применение стандартных решений приемлемо для большинства компаний малого и среднего бизнеса, но не эффективно для крупных компаний.

Автоматизация бизнеса корпоративных заказчиков, как правило, является эксклюзивной задачей, требующей применения самых современных и производительных решений с обязательной оценкой эффективности их совокупной безопасности. Обеспечить надлежащее соответствие продуктов предъявляемым к ним требованиям могут только производители. С учётом их заинтересованности в удержании крупных клиентов, большинство мировых лидеров IT-рынка стремятся предоставить *комплексные решения*, учитывающие, в том числе, и вопросы информационной безопасности. В таких решениях трактовка стандартов безопасности не является препятствием для создания полноценного продукта, поскольку производитель имеет возможность формировать большинство элементов ИС и заинтересован в ее успешном внедрении. Предложенная комбинация технологий обычно является достаточной для реализации требуемого функционала, однако при прочих равных условиях предпочтение будет отдаваться решениям, построенным на наиболее распространенных технологиях без их излишнего многообразия. Аналогично будет оцениваться и число элементов ИС – чем их меньше и чем более они универсальны, тем эффективнее предложенное комплексное решение. С учётом высокой стоимости комплексных решений, они изначально подразумевают работу с большими объёмами данных и большим количеством пользователей. Как следствие, они предусматривают автоматизацию процесса применения и контроля исполнения политик безопасности и, тем самым, минимизируют влияние соответствующих отрицательных факторов.

Примером качественного комплексного решения является *продукт Microsoft SharePoint*. Лидирующее положение Microsoft на рынке операционных систем для персональных компьютеров и серверов приложений, а также серверных и сетевых приложений, позволяет компании определять направления развития рынка в данной области. Продукты Microsoft полностью реализуют роли хранения и обработки данных, представления данных. В части организации доступа Microsoft предлагает широко распространенное решение по построению сетевых каталогов информационных ресурсов (Active Directory) и интегрированные с ним средства сетевой безопасности, основу которых составляет Microsoft ISA Server. Стек фирменных протоколов является технологической основой для построения интегральных решений от Microsoft, а особенности их реализации практически исключают использование в них продуктов сторонних производителей без согласия разработчика. Для эффективной работы систем безопасности на уровне доступа Microsoft активно сотрудничает с ведущими производителями коммуникационного оборудования, прежде всего с Cisco Systems. В результате комплексные решения по организации информационных порталов от Microsoft и Cisco Systems являются полноценными и охватывают все основные функции по обеспечению информационной безопасности.

Проведенный анализ продукта Microsoft SharePoint по факторам, влияющим на информационную безопасность, позволяет выделить следующие «конструктивные» преимущества данного решения.

Ошибки в реализации. Решение SharePoint имеет многоуровневую структуру, надстраиваемую над службами безопасности таких базовых продуктов и тех-

нологий, как ASP.NET, IIS (Internet Information Services), SQL Server 2000, Windows Server 2003 и зависящую от этих служб. Компания Microsoft предоставляет пользователям и партнерам сервис бесплатного обновления программного обеспечения для исправления ошибок и модернизации в целях повышения безопасности своих продуктов. Каждый из перечисленных элементов решения постоянно дорабатывается, что позволяет избежать пагубных последствий недоработок до их массового использования хакерами. Вместе с тем, целенаправленная профессиональная атака на существующие уязвимости возможна, а с учётом масштаба корпоративного пользователя весьма вероятна. В этом случае защита решения будет обеспечиваться эшелонированной системой безопасности, поскольку совокупная вероятность наличия ошибок в реализации всех уровней чрезвычайно мала.

Соответствие стандартам. Большинство протоколов, реализованных компанией Microsoft, имеют специфические особенности, расширяющие возможности соответствующих стандартов. В условиях замкнутой среды комплексного решения такие допущения не снижают уровень безопасности и являются преимуществом, поскольку способствуют росту уровня функциональности системы. Наиболее распространенные протоколы выполнены полностью совместимыми с другими отраслевыми реализациями. К таким протоколам относятся в числе прочих X.509 и LDAP.

Используемые технологии. В SharePoint используется ряд технологий по обеспечению безопасности, в том числе следующие.

1. **Проверка подлинности (сеансовый уровень OSI)**: опирается на концепцию участников безопасности Windows, что позволяет использовать методы строгой проверки, политики паролей, политики блокировки учетных записей и шифрование. Для выполнения необходимой проверки привлекается служба IIS. Для клиентов сети интранет используется аутентификация Kerberos или NTLM. Клиенты сетей Интернет и экстранет используют возможности протокола HTTP 1.1 с обязательным шифрованием трафика аутентификации по протоколу Secure Sockets Layer (SSL). В качестве дополнительной или альтернативной проверки подлинности возможно использование сертификатов X.509, что позволяет унифицировать процесс аутентификации пользователей за счет использования публичных центров выдачи сертификатов. Пользователь, получивший сертификат в таком центре, будет иметь возможность получать доступ к данным на всех информационных порталах, доверяющих данному центру выдачи сертификатов. Еще одной технологией, повышающей комфортность использования решений от Microsoft, является служба Single Sign-On (SSOSrv). Данная служба обеспечивает хранение и сопоставление учетных данных (имен учетных записей и паролей) с тем, чтобы приложения портала могли извлекать необходимую информацию из сторонних приложений и внутренних систем. Пользователи избавляются от необходимости повторной проверки подлинности, когда приложению портала потребуется информация из других бизнес-приложений и систем.

2. **Авторизация**: основана на модели разрешений и обеспечивает высокую степень детализации контроля доступа к содержимому узла. Доступ пользователей к ресурсам осуществляется в соответствии с полномочиями участников безопасности Windows, в качестве которых могут выступать учетные записи отдельных пользователей и учетные записи групп безопасности.

3. **Разграничение доступа кода (уровень приложения OSI)**: технология .NET Framework управляет доступом программного кода информационного портала к защищенным ресурсам и операциям, позволяет эффективно бороться с несанкционированными вредоносными действиями без сокращения возможностей

для пользователей и разработчиков. Разрешения для исполняемого кода наследуются от вызывающих его пользователей. Существует механизм получения кодом информации об имеющихся разрешениях, что позволяет разрабатывать более гибкие приложения. Пользователям могут быть предоставлены разрешения на исполнение того или иного кода.

4. **Протоколы безопасности (транспортный и сеансовый уровни OSI)**, такие как SSL и IPSec, обеспечивают защиту данных, передаваемых внутри и вне зоны действия межсетевого экрана. SSL является сеансовым протоколом, использующим алгоритм открытых ключей для шифрования на основании аутентификационных данных клиента. Протокол IPSec действует на транспортном уровне и прозрачно шифрует трафик протокола IP между двумя операционными системами Microsoft, соответствующий установленным фильтрам. Таким образом, можно шифровать только необходимую часть трафика, например, трафик обмена с другими серверами портального комплекса.

5. **Безопасное хранение данных (уровень приложения OSI)** реализовано в серверных операционных системах Microsoft как шифрование на файловом уровне, а в базах данных – как шифрование хранилищ и индексов.

При кажущемся разнообразии применяемых технологий, они распределены по разным эшелонам системы безопасности и в большинстве случаев лишь дополняют друг друга. В рамках комплексного решения такое разнообразие не приводит к нарушению границ ответственности и не снижает безопасности системы. Вместе с тем, реализованный в Active Directory механизм политик позволяет создавать шаблоны параметров безопасности всех перечисленных протоколов и применять их для различных групп пользователей и серверов. Роли администраторов при этом могут быть разделены таким образом, чтобы исключить возможность несанкционированных изменений настроек безопасности либо подтвердить факт сговора администраторов.

Количество элементов системы. Уникальность решений Microsoft заключается в их чрезвычайной масштабируемости. Все перечисленные выше технологии, реализованные в конкретных продуктах, могут размещаться на одном сервере. Впоследствии по мере роста нагрузки, в соответствии с рекомендациями производителя, отдельные сервисы могут быть перемещены на другие сервера без остановки функционирования системы. При этом увеличение числа серверов с точки зрения управляемости системой в целом не является существенным фактором снижения безопасности, поскольку структура сетевого каталога Active Directory легко распространяет необходимые настройки на любое количество серверов.

Работа с пользователями и политики безопасности.

Все серверные продукты Microsoft поставляются с готовыми шаблонами политик безопасности. Это позволяет оперативно приступить к эксплуатации системы и постепенно настраивать необходимый уровень информационной безопасности. Распределение пользователей и серверов по организационным модулям (Organization Units, OU), присвоение данным модулям отдельных политик безопасности, а также механизм наследования данных политик представляют собой мощный инструмент управления безопасностью комплексного решения от Microsoft. Для удобства наборы разрешений могут объединяться в роли, в том числе стандартные, поставляемые вместе с соответствующими продуктами. Все перечисленные возможности в совокупности с развитой системой журналирования событий делают систему безопасности Microsoft адекватной большому числу пользователей и элементов системы, упрощают процесс изменения настроек и позволяют контролировать полученные результаты.

Таким образом, комплексное решение Microsoft SharePoint представляет собой гибкую и сбалансированную среду для реализации информационных порталов. Подсистема безопасности данного решения соответствует отраслевым стандартам, спроектирована с достаточным запасом надежности, ее поведение прогнозируемо, а управление соответствует решаемым задачам. К недостаткам решения следует отнести ограниченные возможности интеграции с аналогичными решениями сторонних производителей, а в части обеспечения безопасности – отсутствие собственных функций антивирусной проверки.

Тесная взаимосвязь между эффективностью решений по построению информационных систем и их безопасностью определяет поведение участников IT-рынка и заставляет производителей уделять серьёзное внимание данной тематике. Производители вынуждены вкладывать средства в разработку технологий и продуктов, обеспечивающих информационную безопасность, совместно с интеграторами решать вопросы эффективности стандартных решений, а для крупных клиентов выстраивать стратегию развития своих продуктов в направлении формирования полноценных комплексных решений. Наличие таких решений в ближайшие годы будет определять политику потребителей IT-систем и, следовательно, будет формировать практику их эксплуатации. При разработке методик анализа эффективности решений в области информационной безопасности целесообразно учитывать сложившиеся тенденции IT-рынка.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Архитектура безопасности в продуктах и технологиях SharePoint http://www.microsoft.com/rus/security/articles/sharepoint/default.mspx
2. Обзор функций узла SharePoint http://office.microsoft.com/ru-ru/help/HA011425981049.aspx
3. Обеспечение безопасности интернет-транзакций в финансовой корпорации «НИКойл» http://www.microsoft.com/Rus/Government/newsletters/issue17/10.mspx
4. Темы из области безопасности https://www.microsoft.com/rus/technet/security/topics/default.mspx

М.В. Курмаз, Л.С. Берштейн

НАХОЖДЕНИЕ КРИТИЧЕСКОГО ПУТИ В СЕТЕВОМ ПЛАНИРОВАНИИ В УСЛОВИЯХ ЛИНГВИСТИЧЕСКОГО ЗАДАНИЯ ВРЕМЕНИ

Задача сетевого планирования состоит в том, чтобы графически, наглядно и системно отобразить и оптимизировать последовательность и взаимозависимость работ, действий или мероприятий, обеспечивающих своевременное и планомерное достижение конечных целей. Для отображения и алгоритмизации тех или иных действий или ситуаций используются экономико-математические модели, которые называются сетевыми моделями, а простейшие из них – сетевыми графиками.

Сетевое планирование применяется для оптимизации планирования и управления сложными разветвленными комплексами работ, требующими участия большого числа исполнителей и затрат ограниченных ресурсов.

Основными образующими элементами сетевой модели являются *события* и *работы*.