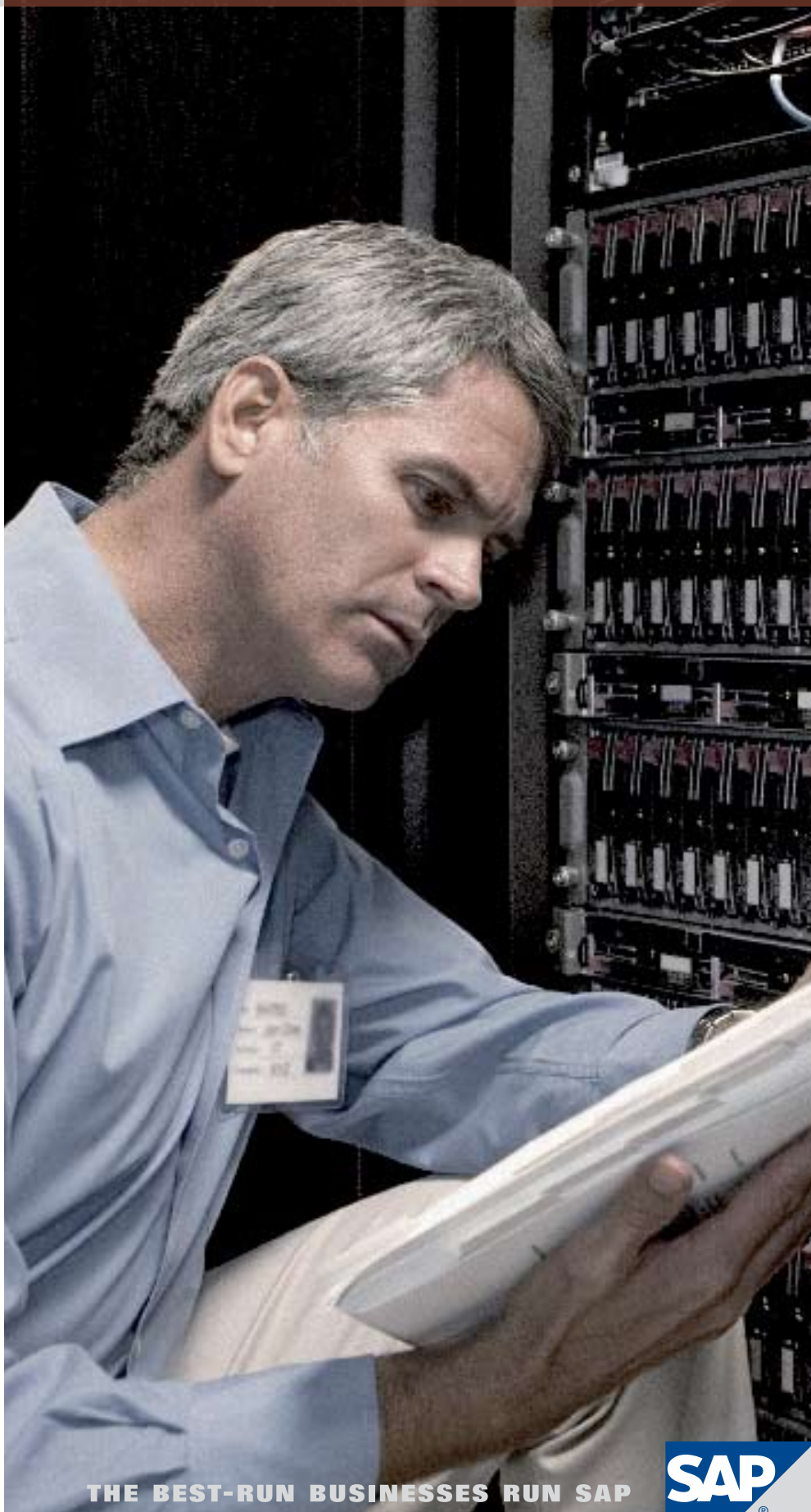


ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РЕШЕНИЯХ SAP

- 2 Открытость для бизнеса и надежная защита
- 2 Средства обеспечения безопасности в решениях SAP
- 8 Реализация российских криптографических алгоритмов в решениях SAP
- 9 Сертификация решений SAP ГК России и Министерством обороны Российской Федерации
- 10 Портрет компании



ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РЕШЕНИЯХ SAP

Открытость для бизнеса и надежная защита

Сегодня растущий бизнес стремится к максимальному использованию новых технологий управления, основанных на методах совместной деятельности, деловыми партнерами, взаимодействии компаний в рамках единой логистической сети, прозрачности финансовой отчетности для существующих и потенциальных инвесторов.

Открытый доступ к совместно используемым данным несет дополнительные риски, связанные с недостаточным уровнем контроля безопасности, для каждой из компаний-участников взаимодействия. Обеспечить возможность для повышения эффективности управления процессами как внутри предприятия, так и вне его, при этом не снижая требований к уровню контроля сохранения коммерческой (а в случае необходимости – государственной) тайны, – такая общая задача стоит перед службами информационных технологий и безопасности компаний.

Политика информационной безопасности компании должна охватывать все уровни правил обращения с объектами и носителями информации – от защиты от возможных физических угроз для носителей информации до аудита действий пользователей в информационных системах.

С помощью этого документа мы демонстрируем, на каких принципах построена концепция безопасности решений SAP и как использование решений SAP поможет предприятию

в построении безопасной ИТ-инфраструктуры.

Компания SAP – многолетний поставщик решений для коммерческих фирм, государственных и военных организаций. Наш опыт говорит о том, что основные аспекты информационной безопасности должны быть учтены непосредственно поставщиком решения на этапе проектирования и разработки – как это было сделано при разработке комплекса решений SAP «Управление современным предприятием» (SAP Business Suite). Только в этом случае можно организовать эффективную систему администрирования и защиты от несанкционированного доступа, необходимую для сохранения информации, содержащей коммерческую и государственную тайны.

Средства обеспечения безопасности в решениях SAP

Для обеспечения эффективной защиты информации в решениях SAP предусмотрен контроль на трех основных уровнях:

- контроль доступа к информации со стороны пользователей информационной системы;
- контроль физической сохранности баз данных и их непротиворечивости;
- контроль конфиденциальности передаваемых по сетям данных и работоспособности сетевой инфраструктуры.

Ниже подробнее рассмотрены технологии, с помощью которых реализуются требования к обеспечению конфиденциальности информации в решениях SAP.

Безопасность на уровне бизнес-приложений

Аутентификация пользователей, авторизация при попытке доступа к бизнес-транзакциям и документам, подтверждение и протоколирование действий пользователей – вот три основные группы процедур, обеспечивающие защиту коммерческой информации в решениях SAP от несанкционированного доступа и изменения средствами SAP.

Аутентификация пользователей

Первой задачей при построении системы безопасности является задача аутентификации – необходимо знать, кто пользователи, работающие в системе, известны и не могут выдавать себя за кого-то другого. В решениях компании SAP предлагаются механизмы защиты учетных записей пользователей от неправомерного использования.

- Правила составления и проверки паролей. Обычная практика предполагает аутентификацию (распознавание) пользователей с помощью паролей. В решениях компании SAP есть ряд встроенных и настраиваемых правил составления паролей, которые можно расширить с учетом потребностей предприятия. В частности, средствами SAP можно установить системное требование регулярной смены паролей пользователей, запрета использования определенных слов или сочетаний символов. Система также блокирует пользователей и сеансы после нескольких неудачных попыток входа, чтобы исключить возможность получения несанкционированного доступа к системе. Средства контроля количества регистраций пользователей,

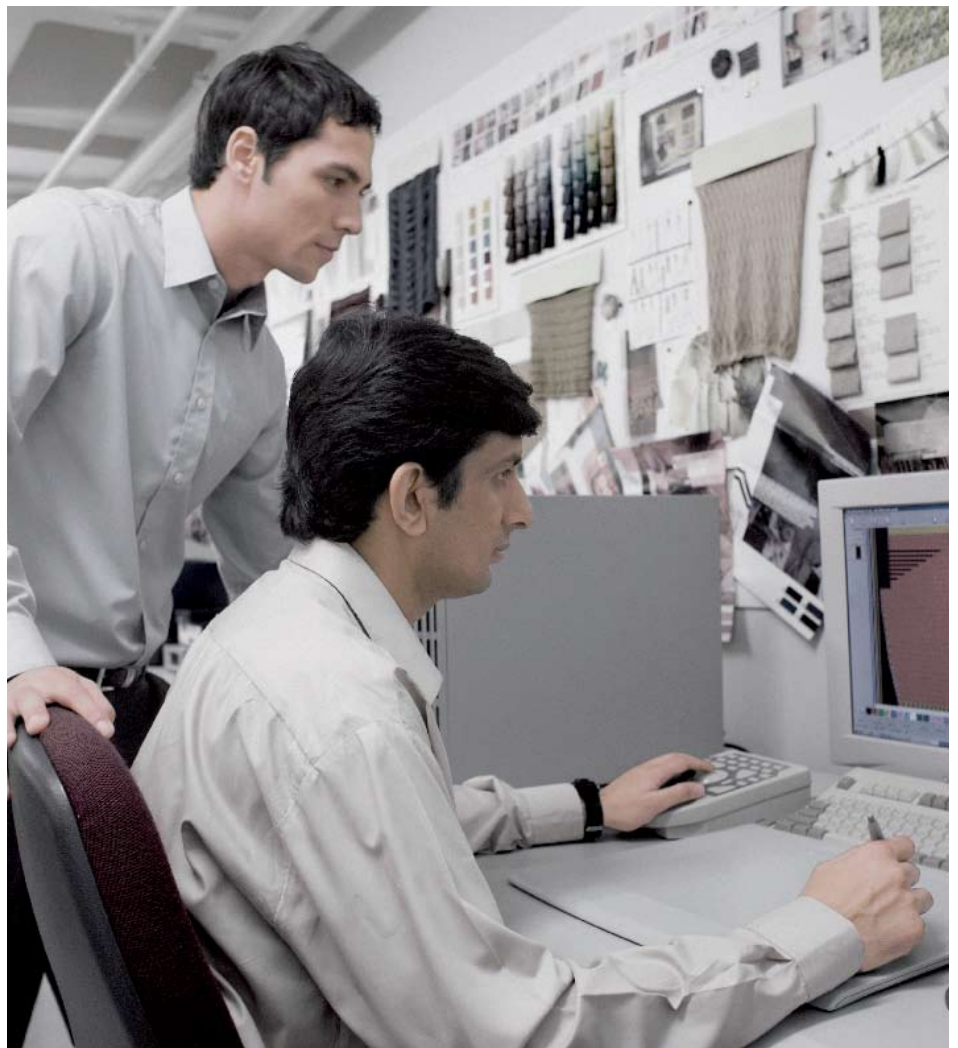
удаления неактивных пользователей и протоколирования адресов подключения при регистрации пользователя являются надежным инструментом администрирования, реализующим все необходимые функции контроля процедур аутентификации.

- **Дополнительные средства аутентификации.** Помимо использования паролей, для организации системы аутентификации могут быть применены интерфейсы Secure Network Communications (SNC). В этом случае совместно с SNC-интерфейсом необходимо использовать внешнее средство криптографии, сертифицированное SAP. При этом для аутентификации будет использоваться технология пар ключей (открытый/приватный). Возможно также использование Single Sign-On (SSO) технологии. В этом случае пользователи проходят процедуру аутентификации только один раз, даже если они работают с несколькими системами. Пользователи регистрируются во внешнем средстве обеспечения безопасности, а это средство создает «учетные данные» для пользователей, которые затем передаются в другие системы, например, в приложения SAP. Для хранения аутентификационной информации пользователей Вы можете воспользоваться чип-картами (для этого потребуется внешнее средство обеспечения безопасности, способное работать с чип-картами). При использовании чип-карт сведения об аутентификации пользователя сохраняются на личной карточке пользователя. Такие

карточки также защищены PIN-кодом (личным идентификационным номером). Поскольку пользователь владеет карточкой и знает PIN-код, вероятность несанкционированного копирования информации или доступа к ней значительно снижается. Необходимо отметить, что интерфейс Secure Network Communications при аутентифика-

ции не требует передачи по сети информации о пароле – направляется подтверждение, которое и идентифицирует пользователя.

Авторизация доступа к данным
Логика решений SAP построена на ролевой модели разграничения доступа, т.е. все работники предприятия, выступая в той или иной роли,



ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РЕШЕНИЯХ SAP

выполняют определенный на системном уровне круг задач. Доступ к информации и процессам закрыт для тех сотрудников, чья роль в организации не требует такого доступа. Например, работнику отдела кадров необходим доступ к процессам расчета зарплаты и данным о сотрудниках. Эта информация не доступна для работников других отделов, таких, как отделы производства и продаж.

- Проверка полномочий при доступе к бизнес-объектам. Проверка полномочий пользователя в решениях SAP выполняется при каждой попытке выполнения бизнес-транзакции, а также при попытке доступа к просмотру или изменению бизнес-документа. Например, для конкретного бухгалтера на предприятии в соответствии с его ролью может быть открыта возможность доступа к выполнению проводки бухгалтерского документа, но только на уровне своей бизнес-единицы, по конкретной группе счетов или по операциям отдельных деловых партнеров. Если у пользователя нет необходимых полномочий, система отказывает в получении доступа к соответствующим транзакциям или документам.
- Администрирование ролей пользователей. Для того, чтобы упростить ведение детальных данных полномочий каждого пользователя, в решениях SAP предусмотрен специальный инструмент – генератор профилей полномочий. Основная идея заключается в использовании стандартных ролей бизнес-пользователей в соответствии с их должностными ролями. Вы можете,

например, присвоить отдельному сотруднику одну или несколько стандартных ролей, и этим полностью определить профиль его полномочий. При необходимости Вы можете отредактировать перечень функций, добавив или удалив один объект полномочий или целую группу функций. Существует также возможность настройки собственных ролей, используемых затем на предприятии для целей стандартизации и масштабирования.

Подтверждение и протоколирование действий пользователей

Ограничения полномочий пользователя не являются гарантией корректности данных бизнес-документов. В случае, если все действия пользователя документируются и существует формальное подтверждение автора изменений, Вы можете контролировать источник данных и, как следствие, управлять ответственностью за конкретные действия пользователей.

- Механизмы протоколирования действий. Необходимо вести учет событий и деятельности для последующего использования в справочных целях. Протоколирование действий пользователя, также как и проверка полномочий, ведется на двух уровнях. На уровне администрирования пользователей ведется история выполнения пользователем отдельных бизнес-транзакций, программ и процессов, даты и времени регистрации в системе, изменения личных данных и другой информации системного характера. Для отдельного документа, бухгалтерской проводки или другого бизнес-объекта системой

сохраняется история изменения документа – с данными автора изменений, даты и времени изменения, состава внесенных изменений. Таким образом, сохраняется полная версия при управлении бизнес-документами и обеспечивается персональная ответственность за все внесенные изменения.

- Механизмы ведения оригиналов документов. В ряде случаев системной информации об авторе документа недостаточно – необходимо подписание формы документа и сохранение оригинала документа в отсканированном виде. Используемые в составе решения SAP «Управление ресурсами предприятия» (SAP ERP) механизмы электронной подписи, а также средства управления документами Document Management System (SAP DMS), позволяют сохранять формальные подтверждения подлинности бизнес-документов. Использование электронной подписи, в разрешенных для этого случаях, позволяет значительно сократить время обработки документов и общую производительность труда персонала.

Безопасность на уровне баз данных

Многолетний опыт компании SAP позволил определить методологию и стандартные регламенты как процедур обеспечения физического сохранения данных (в первую очередь – операций копирования и резервного сохранения данных), так и процедур контроля непротиворечивости на уровне базы данных.

- Семантическая целостность данных. Средства семантических проверок, реализованных в алгоритмах

прикладных программ решений SAP, обеспечивают непротиворечивость данных на уровне базы данных. Программы приложений SAP представляют собой многошаговые процессы, на каждом из шагов которых производятся семантические проверки.

- Защита одновременного доступа к изменению данных. Решения SAP обеспечивают защиту одновременного доступа к объектам

многопользовательской обработки с помощью механизмов блокировки. Эти механизмы предотвращают одновременный доступ нескольких пользователей к одному и тому же объекту через транзакцию изменения, сохраняя, как правило, возможность просмотра объекта.

- Физическая целостность данных. Сохранность данных, накопленных в процессе деятельности компании, обеспечивается средствами

копирования и восстановления информационной базы. С помощью механизмов планирования и выполнения фоновых заданий могут управляться автоматические операции создания резервных копий, а средства мониторинга параметров базы данных обеспечивают постоянный контроль технических аспектов эксплуатации решений SAP.

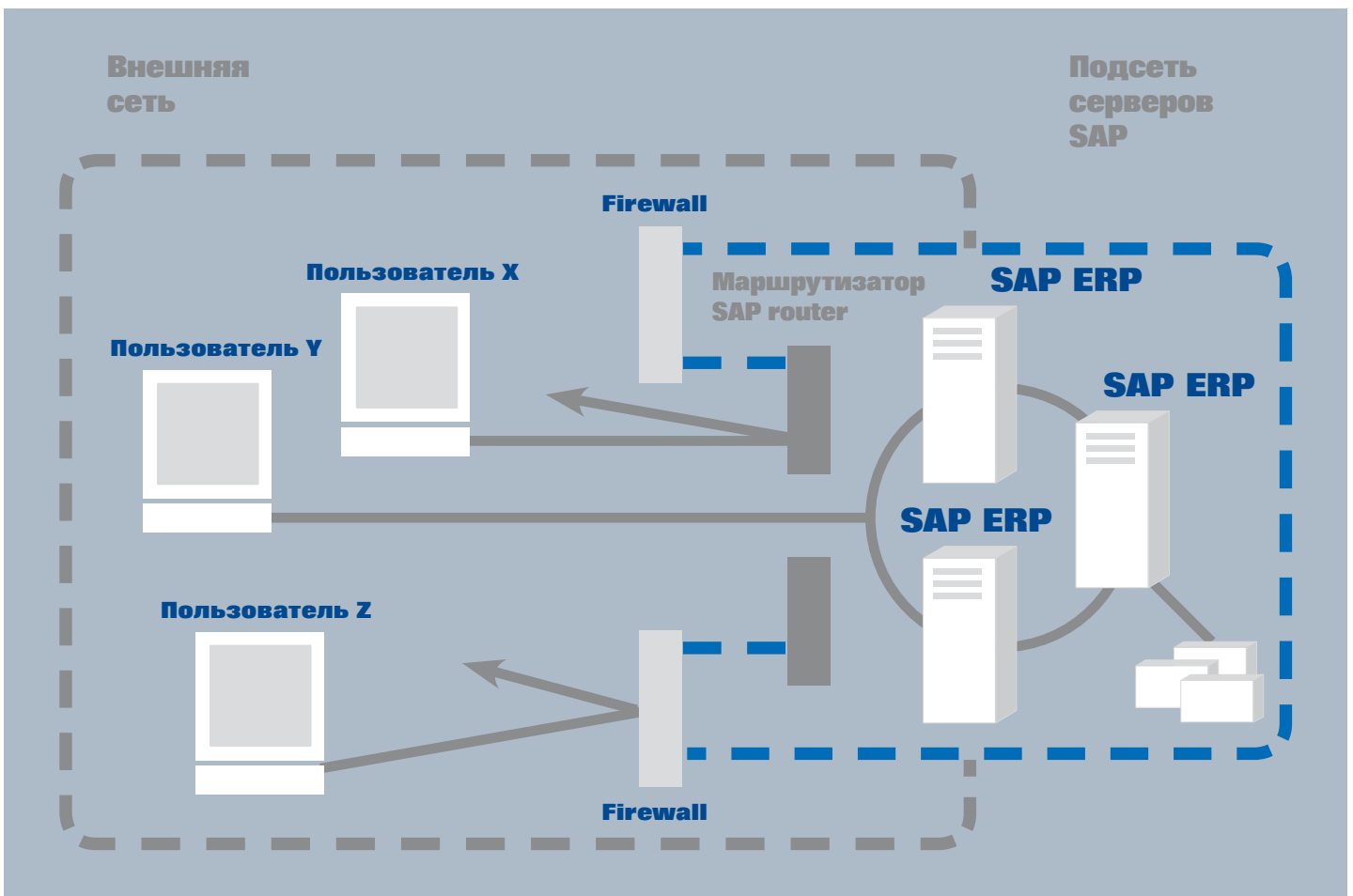


Рисунок 1. Защита локальной сети с помощью SAP router и межсетевого экрана Firewall.

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РЕШЕНИЯХ SAP

Безопасность на уровне сетевых коммуникаций

Сетевая инфраструктура чрезвычайно важна для обеспечения безопасности системы. Если при проектировании топологии сети безопасности уделяется серьезное внимание, можно значительно сократить число вероятных угроз.

Защита доступа к локальной сети

Инструменты SAP router и Secure Network Communications (SNC) — это основные службы безопасности SAP, обеспечивающие сетевую безопасность.

SAP router — это прокси-сервер уровня приложений, который используется

вместе с межсетевым экраном для эффективной защиты сети от несанкционированного доступа. Межсетевой экран защищает от нежелательного доступа к Вашей внутренней сети. Для тех информационных запросов, которые Вы хотите обрабатывать в сети, необходимо открыть соответствующие «ворота» в межсетевом экране.

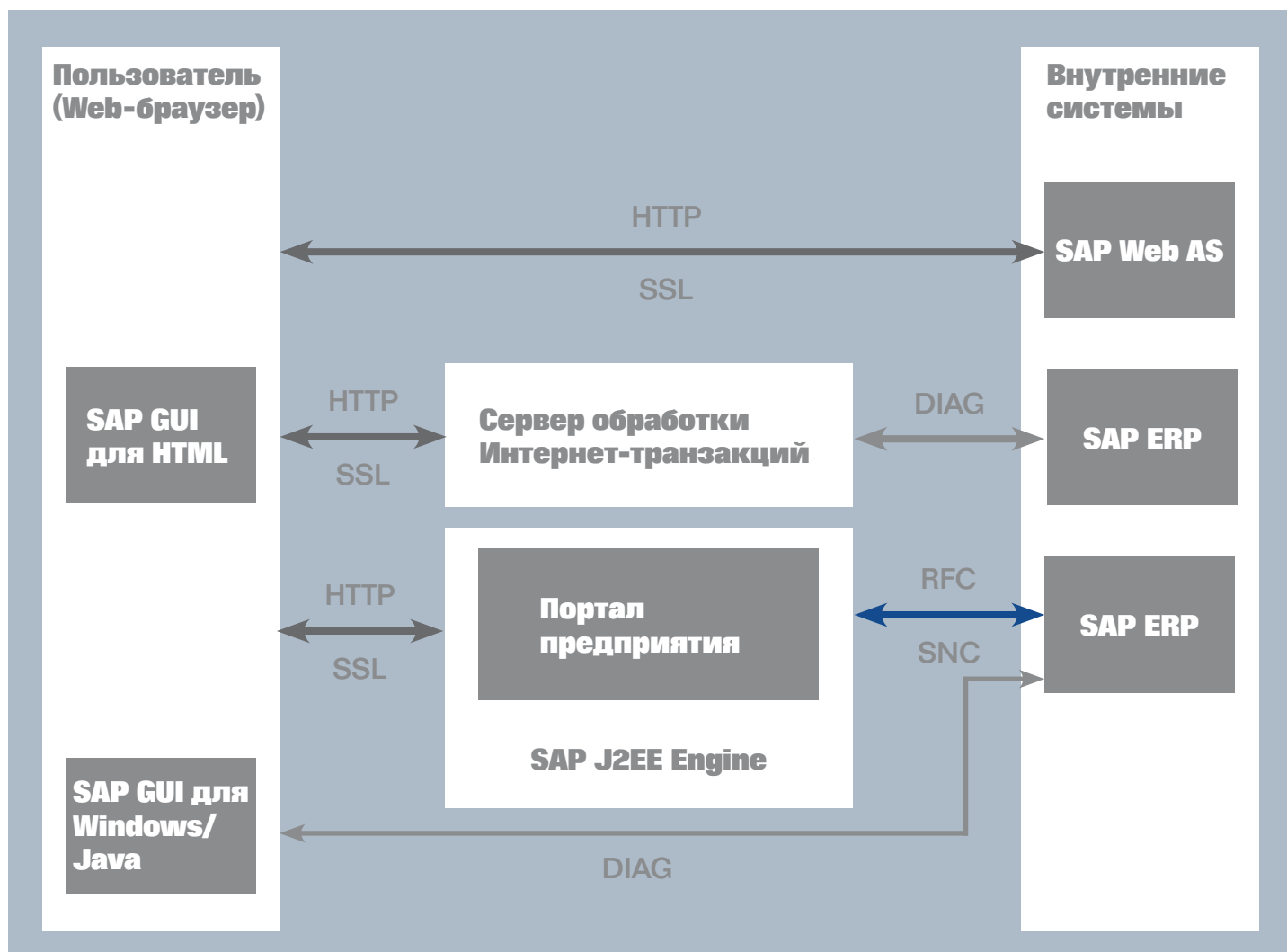


Рисунок 2. Возможности по организации доступа к средствам SAP через Web-интерфейс.

Далее, для дополнительного контроля доступа внутри сети, используется SAP router.

SAP router также проверяет действительность запроса, но на более детальном уровне, принимая или отклоняя запросы, исходящие от определенного пользователя или компьютера, или направляя запросы только определенному компьютеру. SAP router вместе с межсетевым экраном обеспечивают эффективную защиту локальной сети установленных решений SAP от несанкционированного доступа.

Прокси-сервер SAP router используется для повышения сетевой безопасности за счет:

- защиты соединений и данных от несанкционированного внешнего доступа с паролем;
- разрешения доступа только через конкретные программы SAP router;
- разрешения только зашифрованных соединений с известным партнером (при использовании SNC).

Защита взаимодействия в сети Интернет

Географическая распределенность филиалов и производственных площадок предприятий, а также развитие взаимосвязей с партнерами, требует, помимо необходимости контролировать доступ к информации внутри корпоративной сети, организации нескольких уровней защиты при проектировании архитектуры Интернет-приложений.

Средства решений SAP позволяют организовать доступ к компонентам решений непосредственно через WEB-браузер, используя Сер-

вер обработки Интернет-транзакций (SAP Internet Transaction Server) или инструменты Портала Предприятия (SAP Enterprise Portal).

Уровень защиты информации Интернет-приложений зависит от настроек сетевой архитектуры и размещения компонентов. Для повышения уровня безопасности SAP рекомендует развертывание дополнительных межсетевых экранов между различными частями сети и использование фильтров пакетов. Портал предприятия, как средство доступа к информации, содержащей коммерческую тайну, обеспечен всеми необходимыми механизмами проверки аутентификации и авторизации действий. При использовании Сервера обработки Интернет-транзакций желательно развертывание его элементов AGATE и WGATE (отвечающих за связь с WEB-сервером и приложениями SAP из внутренней подсети соответственно) на различных хостах.

Шифрование данных – электронные подписи и цифровые конверты
Электронные подписи и цифровые конверты основаны на технологии открытых ключей. У пользователя, создающего электронные подписи или цифровые конверты, имеется пара ключей – открытый и закрытый. Эти два ключа обладают следующими характеристиками: ключи составляют пару и функционируют вместе, невозможно рассчитать один из ключей, используя другой. Открытый ключ необходим для того, чтобы «подписать» документ. После того, как документ подписан, для его прочтения пользователь-получатель должен обладать за-

крытым ключом, необходимым для доступа к зашифрованной информации.

Цифровые конверты также используются для защиты передаваемой информации от несанкционированного доступа. Чтобы создать цифровой конверт, используется закрытый ключ сообщения для «упаковки» документа в «конверт». Получатель сообщения должен знать этот ключ, чтобы расшифровать документ. Поэтому ключ сообщения зашифровывается с использованием открытого ключа получателя и отправляется вместе с документом.

Функции SSF могут применяться в различных сценариях для защиты данных и документов. К типичным сценариям в решениях SAP относятся следующие:

1. Приложение, использующее механизмы SSF, преобразует незашифрованные данные из SAPgui в защищенный формат и сохраняет их в базе данных используемого решения SAP. При последующих обращениях приложения к этим данным они извлекаются из базы данных и дешифруются с использованием функций SSF. Если данные подписаны электронной подписью, приложение может также проверить электронную подпись.
2. Приложение считывает данные из базы данных SAP и подготавливает их для внешней передачи или сохранения. Для этого данные сначала преобразуются в соответствующий внешний формат, затем защищаются с использованием функций SSF. После преобразования данных в защищенный формат

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РЕШЕНИЯХ SAP

приложение может безопасно сохранять их на носителе данных (например, на диске или в архиве данных) или передавать их по (возможно) незащищенным каналам связи (таким, как Интернет). Санкционированным получателем может быть другое приложение SAP или другая система, поддерживающая используемый защищенный формат.

3. Приложение получает защищенные данные или данные, подписанные электронной подписью, из внешнего источника и импортирует их в приложения SAP. Если данные защищены с использованием формата, совместимого с SSF, то приложение может использовать функции SSF для расшифровки данных или проверки подписи.

Реализация российских криптографических алгоритмов в решениях SAP

При использовании механизмов электронной подписи или цифровых конвертов в Российской Федерации должны быть применены российские криптографические механизмы. Для реализации средств криптографической защиты компанией SAP привлекаются российские партнеры. В настоящий момент наибольшим опытом в разработке и внедрении средств обеспечения безопасности обладают компании «ЛИССИ» и НПО «МЕКОМП», представляющие решения по шифрованию данных и обеспечению средств Single Sign-on. За информацией об альтернативных решениях партнеров компании SAP по безопасности обращайтесь в офисы SAP в странах СНГ.

Решения «LISSI-SNC» и «LISSI-SSF» Российским партнером SAP в области защиты информации – компанией «ЛИССИ» – разработаны программные решения «LISSI-SNC» и «LISSI-SSF», которые обеспечивают криптографическую защиту передаваемых по сети данных и электронных документов с использованием российских криптографических алгоритмов. В решении «LISSI-SNC» для аутентификации пользователей используется алгоритм ГОСТ Р 34.10-2001. Весь объем передаваемых данных шифруется по алгоритму ГОСТ 28147-89, целостность передаваемых данных контролируется с помощью создания и проверки имитовставок. Ключ для шифрования уникален для каждого пакета с данными и создается на основе разделяемого секрета, полученного на этапе аутентификации пользователя.

Решение «LISSI-SNC» обеспечивает:

- Надежную криптографическую защиту данных.
- Использование российских (сертифицированных соответствующими службами) криптографических алгоритмов ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001.
- Поддержку всех основных платформ SAP – IBM AIX, SUN Solaris, Microsoft Windows, HP-UX.
- Надежную программно-аппаратную аутентификацию пользователей при помощи электронной цифровой подписи и электронного ключа ruToken.
- Использование цифровых сертификатов и стандартов Инфраструктуры Открытых Ключей (Public Key Infrastructure).
- Единый вход в систему (Single Sign On).

Решение «LISSI-SSF» обеспечивает:

- Подпись электронных документов пользователями с использованием сертификатов ЭЦП.
- Проверку подписи электронных документов пользователями с использованием сертификатов ЭЦП.
- Хранение зашифрованных электронных документов в цифровых конвертах, доступ к которым определяется ответственным лицом.
- Использование российских (сертифицированных соответствующими службами) криптографических алгоритмов ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001.
- Поддержку всех основных платформ SAP – IBM AIX, SUN Solaris, Microsoft Windows, HP-UX.

Решения «MSNC-адаптер» и «MSSF-адаптер»

Российским партнером SAP – компанией НПО «МЕКОМП» – совместно с ФГУП ГИВЦмет «Центринформ» разработано программное обеспечение «MSNC-адаптер» и «MSSF-адаптер», обеспечивающее защиту информации в среде продуктов SAP.

Данные решения обеспечивают:

- Криптографическую аутентификацию, целостность и конфиденциальность передаваемых данных при взаимодействии между программными компонентами SAP-систем.
- Использование сценариев единой регистрации пользователей (Single Sign On) и смарт-карт.
- Формирование и обработку электронной цифровой подписи для импорта, экспорта и хранения данных на серверах приложений SAP и клиентских местах SAP GUI.

- Использование инфраструктуры открытых ключей.
- Использование российских криптографических алгоритмов: хеширование (преобразование) данных в соответствии с ГОСТ Р 34.11-94, шифрование данных в соответствии с ГОСТ 28147-89, алгоритмы формирования и проверки электронной цифровой подписи ГОСТ Р 34.10-94 и ГОСТ Р 34.10-2001.

**Сертификация решений SAP
Государственной технической
комиссией при Президенте
Российской Федерации
и Министерством обороны
Российской Федерации**

Открытость программных кодов решений SAP позволяет оценивать степень защиты данных средствами SAP и разработок российских партнеров. Компания SAP одной из первых в России прошла сертификационные испытания в Государственной технической комиссии при Президенте Российской Федерации. В результате проведенных испытаний Государственная техническая комиссия выдала компании SAP сертификаты, удостоверяющие, что решения и компоненты ПО SAP предоставляют необходимые средства обеспечения защиты информации и соответствуют требованиям руководящего документа Государственной технической комиссии при Президенте Российской Федерации «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» по 4-му классу защищенности и могут быть использованы для разработки прикладного програм-



ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РЕШЕНИЯХ SAP

много обеспечения автоматизированных систем до класса защищенности 1 В включительно.

В 2008 году компания SAP первой в России получила сертификат по линии Министерства обороны Российской Федерации. Высокий уровень безопасности систем SAP был по достоинству оценен экспертами испытательных лабораторий и 27-го Центрального НИИ Министерства обороны Российской Федерации. Полученный сертификат удостоверяет соответствие ПО SAP требованиям приказа Министерства обороны Российской Федерации 1996 года № 058:

- по 4-му классу защищенности информации от несанкционированного доступа согласно руководящему документу «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992 г.);
- по 3-му уровню контроля отсутствия недекларированных возможностей согласно руководящему документу «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (Гостехкомиссия России, 1992 г.);
- по соответствию реальных и декларируемых в документации функциональных возможностей.

Сертификация по указанным уровням означает, что ПО SAP официально одобрено Министерством обороны Российской Федерации для использования в автоматизированных системах, обрабатывающих информацию, составляющую государственную тайну, под грифом Секретно.

Портрет компании

Компания SAP является ведущим в мире поставщиком программных решений для управления бизнесом. Комплексное предложение SAP включает решения, отвечающие требованиям организаций любого масштаба – от компаний сегмента малого и среднего бизнеса до глобальных корпораций. Решения SAP для управления бизнесом помогают предприятиям во всем мире повышать эффективность деятельности всех функциональных подразделений и компании в целом, совершенствовать взаимоотношения с клиентами и расширять сотрудничество с партнерами. В настоящее время более 40 000 компаний, расположенных в более чем 120 странах мира, используют в своей работе программное обеспечение SAP.

Все решения SAP базируются на платформе SAP NetWeaver – технологической платформе нового поколения для управления бизнес-процессами, которая обеспечивает возможность перехода к сервисно-ориентированной архитектуре ИТ-ландшафта и поддерживает быструю реализацию инноваций и гибкую адаптацию бизнеса к изменениям рыночной среды.

Отраслевые решения SAP эффективно поддерживают уникальные бизнес-процессы более чем 28 отраслей, в число которых наряду с флагманами экономики – нефтегазовой отраслью, металлургией, энергетикой – входят развивающиеся быстрыми темпами сфера розничной торговли и производства товаров народного потребления, индустрия машиностроения, сектор финансовых институтов и многие другие отрасли. Решения SAP успешно используются также для эффективного управления государственным сектором экономики разных стран.

Компания SAP имеет представительство в более чем 50 странах мира, представлена на нескольких биржах, включая Франкфуртскую фондовую биржу и Нью-Йоркскую фондовую биржу.

Дополнительная информация:

<http://www.sap.com>

В 1992 году открылось представительство SAP AG в Москве. За прошедшие годы открылись представительства в Санкт-Петербурге, Алматы и Киеве, а численность сотрудников превысила 600 человек. У клиентов SAP в странах СНГ работают в промышленной эксплуатации более 900 информационных систем на базе решений SAP. Всего в странах СНГ с решениями SAP работают более 90 000 человек.

Дополнительная информация:

<http://www.sap.ru>



Информация к действию

Мы готовы ответить на Ваши вопросы и продемонстрировать, как решения SAP помогут Вашей компании оптимизировать все сферы деятельности и создать долгосрочные конкурентные преимущества.

Позвоните нам прямо сегодня, чтобы завтра быть впереди конкурентов!

Телефон для контактов (звонок по России бесплатный): **8 800 200 9777**

Подробную информацию на русском языке о компании SAP, наших решениях и услугах можно найти на нашем Интернет-сайте по адресу: www.sap.ru, где Вы также можете задать интересующие Вас вопросы. Будем рады ответить на них!

Подпишитесь на рассылку новостей по адресу www.sap.ru/company/digest/, и Вы будете в курсе последних новостей SAP для стран СНГ.

Адреса офисов

ООО «САП СНГ»

РФ, 115054, Москва,
Космодамианская
набережная, д. 52/2.
Т.: +7 (495) 755-9800.
Ф.: +7 (495) 755-9801.

E-mail: info.cis@sap.com
www.sap.ru

ООО «САП СНГ»

РФ, 190000, Санкт-Петербург,
ул. Малая Морская, д. 23.
Т.: +7 (812) 448-4103.
Ф.: +7 (812) 448-4102.

E-mail: info.cis@sap.com
www.sap.ru

ООО «САП Украина»

Украина, 03150, Киев,
ул. Димитрова, д. 5.
Т.: +38 (044) 490-3391, 490-3393.
Ф.: +38 (044) 490-3394.

E-mail: info.Ukraine@sap.com
www.sap.ua

ТОО «САП Казахстан»

Казахстан, 050059, Алматы,
ул. Фурманова 240Г.
Телефон: +7 (727) 250-8400,
факс: +7 (727) 250-8401.

E-mail: info.kazakhstan@sap.com
www.sap.ru

Авторское право © 2008 SAP AG. Все права защищены.
SAP, SAP Business Suite, xApps, xApp, SAP NetWeaver
и другие упомянутые здесь продукты и услуги SAP, а также
соответствующие им логотипы являются торговыми марками
SAP AG или торговыми марками SAP AG, зарегистрирован-
ными в Германии и в ряде других стран. Названия других про-
дуктов или услуг, встречающиеся в этом документе, являются
торговыми марками соответствующих компаний.