С. С. Велигодский, Н. Г. Милославская
Московский инженерно-физический институт (государственный университет)

БЕЗОПАСНОСТЬ КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ ПОРТАЛОВ

1. Введение в Порталы

Очередным этапом в эволюции локальных вычислительных сетей (ЛВС) является Интранет, построенный на базе современных веб-технологий, нашедших широкое применение в Интернете. Данные сети [1] как корпоративные унифицированные информационные сети были задуманы для интеграции людей, процессов и информации внутри организаций. Портал в рамках Интранета представляет собой единую точку доступа к ее ресурсам и обеспечивает персонализированный доступ к приложениям, контенту, людям и процессам через единый веб-интерфейс. При этом зачастую порталы не требуют установки на рабочие места (АРМы) пользователей какого-либо дополнительного программного обеспечения (ПО) за исключением стандартного интернет-обозревателя.

Порталы делят на несколько классов в зависимости от их технических особенностей и целевой аудитории. Термин «интранет-портал», или «корпоративный информационный портал» (КИП), стал широко известен примерно в 1998 г. Данный тип портала использовался для организации централизованной точки доступа к информации и сервисам для клиентов, сотрудников и деловых партнеров. КИП использовались для хранения, обработки, анализа и контроля доступа к структурированным и неструктурированным данным, которые использовались во внутренних и внешних бизнес-процессах. Они аккумулировали данные из различных внутренних и внешних источников, при этом предоставляя доступ к этим данным в форматах, затребованных пользователям. Одновременно с этим КИП обеспечивали вспомогательные сервисы: поиск, совместную работу, документооборот и безопасность, а также доступность их сервисов.

КИП позволили решить множество проблем, стоящих перед службами IT-подразделений: масштабируемость и переносимость корпоративных приложений, применение принципов унифицированной точки администрирования и сопровождения, поддержка принципа единой регистрации в сети (Single Sign-On, SSO), уменьшение ресурсов, необходимых для сопровождения корпоративной инфраструктуры, и пр.

В соответствии с точкой зрения Шайлакса и Тилмана, аналитиков компании Merrill Lynch [2], КИП — это «приложения, позволяющие компаниям раскрывать информацию, хранящуюся внутри и вне организации, и предоставлять пользователям единый шлюз доступа к персонализированной информации, необходимой для принятия бизнес-решений». Они являются «...совокупностью программных приложений, которые консолидируют, управляют, анализируют и распространяют информацию по всему предприятию и за его пределами».

В портальных решениях сочетаются приложения различного класса: системы принятия решений (Business Intelligence), управления контентом (Content Management), хранения и обработки данных (Data Ware House & Data Mart) и т. п. Системы управления контентом обрабатывают, фильтруют и преобразуют неструктурированные данные и информацию (при этом зачастую выполняя функции структуризации) и сохраняют их в корпоративном централизованном/распределенном хранилище. Системы поддержки принятия решений обеспечивают доступ к информации с возможностью создания отчетов и аналитической обработки информации в режиме реального времени. Системы обработки и анализа информации предоставляют пользователям значимую для них информацию в удобочитаемом виде. Хранилища данных являются интегрированными, долговременными массивами данных, поддерживающими системы поддержки принятия решений (DSS). Системы управления данными выполняют извлечение, преобразование и загрузку «чистых данных, администрирование и управление метаданными для хранилищ данных и витрин данных» [2]. Как правило, КИП обладает открытой

архитектурой, позволяющей расширять их функциональность за счет добавления сторонних приложений или дополнительных компонентов.

Как видно, для поддержки функциональности порталов используются практически все современные информационные и сетевые технологии. Наличие известных, но неисправленных или неизвестных уязвимостей в них может быть использовано злоумышленниками и повлиять в целом на информационную безопасность (ИБ) любой реализации портальной технологии или на любой элемент информационной инфраструктуры организации.

2. Уязвимости и угрозы ИБ КИП

Условия ведения современного бизнеса требуют от организаций применять в своих бизнес-процессах сложные и интегрированные информационные решения и решения, обеспечивающие возможность совместной работы, которые, взаимодействуя, должны удовлетворять текущим потребностям пользователей. При этом одним из основных вопросов является разработка надежной инфраструктуры безопасности, представляющей собой компромисс между защищенным доступом к информации и удобством использования систем. Зачастую решения по самообслуживанию пользователей используют единую точку доступа к бизнес-процессам через веб ориентированный интранет-портал. При этом пользователи должны быть уверены в том, что информация, обрабатываемая на портале, и функции, которые он предоставляет, являются безопасными. Так, необходимо дать гарантии того, что меры контроля, реализованные на портале, соответствуют текущим угрозам (информационные потоки между пользователями и компонентами портала идентифицированы, протоколированы и проконтролированы, пользователи, выполняя процедуру входа на портал, получают персонализированный доступ только к той информации, к которой им предоставлен доступ в рамках имеющихся у них полномочий и пр.).

В то же время КИП существенно упростили жизнь злоумышленникам. Например, если раньше доступ к бизнес-системам можно было ограничить на сетевом уровне, а для регистрации в системах необходимо было использовать различные учетные записи, то после внедрения портальных технологий доступ организуется через единый общедоступный шлюз, контролируемый на прикладном уровне. Таким образом, с точки зрения ИБ КИП становится подобием «информационного сердца организации», нарушение работоспособности и/или безопасности которого ведет к угрозам ИБ для всей инфраструктуры. Массовый доступ пользователей, большое количество как известных, так и неизвестных уязвимостей в технологиях, используемых при построении портальных решений, ошибки в конфигурации систем и выборе портальной архитектуры, а также многие другие аспекты жизненного цикла КИП существенно увеличивают угрозы нарушения конфиденциальности, целостности и доступности портальных ресурсов.

КИП могут быть реализованы с использованием различных технологий и архитектур, при этом проблемы безопасности в том или ином виде остаются актуальными для каждого из них. В общем случае КИП является классическим веб-приложением с набором стандартных проблем безопасности, характерных для них. Современные веб-приложения предоставляют возможность с помощью стандартных интернет-обозревателей (Microsoft Internet Explorer, Mozilla FireFox и пр.) получать доступ к централизованным ресурсам, таким как веб-сервер, за которым расположены остальные компоненты приложения: сервер приложений и СУБД. Фактически каждый из указанных элементов в клиент-серверной веб-архитектуре имеет большое количество старых, хорошо изученных, и новых уязвимостей, которые делят на десять основных классов:

1) непроверяемые входные данные;

2) уязвимость вследствие некорректной реализации механизмов контроля доступа;

3) уязвимость вследствие некорректной реализации подсистем аутентификации и управления сессиями;

4) уязвимости класса «межсайтовый скриптинг»;

5) уязвимость вследствие неправильного управления памятью (атаки типа переполнения буфера);

6) некорректная обработка управляющих команд в параметрах запросов;

7) некорректная реализация подсистемы обработки ошибок;

8) уязвимость вследствие неправильного хранения прикладных и конфигурационных данных;

9) уязвимость вследствие неправильной работы с ресурсами (атаки типа «отказ в обслуживании»);

10) уязвимость вследствие незащищенной подсистемы администрирования (некорректное разделение полномочий администратора и обыкновенного пользователя, возможность получения прав администратора и т. п.) [7].

Одной из не решенных на настоящий момент проблем является сохранение и передача идентификаторов пользовательских сессий (так называемых Session ID), которые используются в механизмах аутентификации веб-приложений. Наиболее известной и широко применяемой атакой на идентификатор сессии является атака типа «межсайтовый скриптинг» (cross-site scripting), основанная на краже идентификатора у авторизованных пользователей. Не решена также проблема «фишинговых» атак (phishing), основанных на доверии пользователя злонамеренным веб-сайтам, замаскированным злоумышленником под доверенные интернет-ресурсы.

С другой стороны, технологии, используемые при построении портальных решений (такие как общий доступ к документам, виртуальные распределенные рабочие группы, различные коммуникационные инструменты и протоколы, хранилища данных, системы публикаций и пр.), нуждаются в защите от специфичных для них угроз, приводящих к локальным и удаленным атакам. Например, многие портальные решения имеют в своем составе инструменты для публикации информации (форумы, чаты, рабочие группы, доски объявлений), которые существенно повышают риски распространения деструктивного ПО (вирусы, троянские программы и пр.). Кроме того, существует проблема построения защищенной подсистемы аутентификации и авторизации при интеграции различных гетерогенных систем в составе портала.

В рамках одной статьи невозможно рассмотреть все аспекты безопасности КИП. Однако необходимо отметить, что портал, как в принципе и любая автоматизированная система, подвержен атакам всех современных классов. Проведенный нами анализ позволил выявить ряд проблем, стоящих перед разработчиками (и, без сомнения, перед владельцами) портальных решений при позиционирования их в качестве доверенного инструмента ведения бизнеса.

Таким образом, портальные решения в соответствии с текущим уровнем угроз ИБ должны включать надежную подсистему безопасности. Это означает усиление акцентов на безопасности портальных ресурсов, включая такие важные элементы, как конфиденциальность, целостность контента, неотказуемость от операций, доступность и т. д. Поскольку большинству пользователей требуются еще и гарантии безопасности, разумно выбрать соответствующие требования безопасности портального решения с учетом имеющихся угроз ИБ и реализовать соответствующие меры по обеспечению ИБ с использованием комплексного подхода (разработка политики безопасности, выбор безопасной архитектуры и технологий, усиленная идентификация и аутентификация пользователей, мониторинг и аудит ИБ, применение средств выявления уязвимостей и обнаружения вторжений и т. д.).

3. Политика ИБ КИП

Защищенный КИП должен обладать тремя основными характеристиками: конфиденциальностью, целостностью и доступностью (хотя в настоящее время к этим классическим еще принято добавлять неотказуемость/причастность, аутентичность/авторство, учетность и функциональность/адекватность).

Технологии и компьютеры не могут сами по себе обеспечить защищенность обрабатываемой, хранимой или передаваемой информации. Защита ресурсов портала и информации о его пользователях должна осуществляться в соответствии с рисками нарушения ИБ, связанными с особенностями эксплуатации портальных сервисов.

КИП предоставляет два основных типа организации веб-доступа: внутренний портал для сотрудников (внутренний портал) и общедоступный портал для клиентов и партнеров (внешний портал). Соответственно, существуют различные требования безопасности для каждого из данных типов для

защиты от двух классов злоумышленников: «инсайдеров» (в лице внутренних сотрудников) и «аутсайдеров» (партнеры, удаленные пользователи и т. д.). При этом внутренний портал должен предоставлять больше информации и сервисов для пользователей, в то время как внешний портал должен обладать существенно более строгими ограничениями и политикой верификации пользователей.

Однако в обоих случаях должным образом разработанная и внедренная политика ИБ ресурсов и компонентов КИП является ключевым и первостепенным этапом его защиты. Без политики безопасности корпоративного портала (ПБКП) невозможно создать фундаментальную базу корпоративной безопасности. Первоначально защита должна быть обеспечена ресурсам Интранета, а затем КИП как средства доступа к данным ресурсам. ПБКП должна обеспечивать координацию системы безопасности КИП для пользователей и сотрудников организации при обработке, хранении и передаче данных и определять разрешения и ограничения. ПБКП состоит из общей политики для всего КИП (в ней должна быть представлена стратегия и тактика его использования с учетом целей, задачи и требований ИБ и т. п.) и частных политик использования учетных записей, парольных политик, удаленного доступа, правил доступа к ресурсам и других аспектов [3, 4]. ПБКП должна быть краткой, понятной, а главное, выполнимой. ПБКП необходимо регулярно обновлять для отражения в ней существенных изменений, которые неизбежно происходят в организациях. Кроме того, ПБКП должна быть сбалансирована для избежания ее негативного влияния на бизнес-процессы. ПБКП также должна содержать положения, объясняющие, почему данная политика важна для организации; описывать область применения; определять категории информации/доступа; определять правила и ответственность для внешних организаций; описывать правила обработки нарушений ИБ. Обучение ПБКП должно быть частью процедуры повышения квалификации персонала в отношении КИП и осуществляться на регулярной основе.

Хотя в настоящее время существует множество определений механизмов безопасности, для простоты ключевые технологии безопасности КИП можно представить следующим образом: идентификация и аутентификация, шифрование, централизованный и локальный мониторинг и аудит ИБ и контроль доступа [5], системы обнаружения/предотвращения вторжений, межсетевые экраны и сканеры защищенности.

Аутентификация — процедура проверки предъявленного идентификатора (например, имени учетной записи). Она подтверждает, что пользователь является тем, за кого он себя выдает. Например, пользователь должен предоставить имя учтенной записи и пароль и/или биометрический признак, который проверяется доверенным участником (например, базой данных или контроллером домена). Авторизация — процесс разрешения/запрета доступа к ресурсам. Он представляет собой разрешения, которые пользователь/группа имеет к конкретному ресурсу(ам) КИП (портлетам или html-страницам). Аутентификация и авторизация должны контролироваться централизованным компонентом безопасности (менеджером безопасности). Применяемые парольные политики должны обеспечивать соблюдение общего формата имен учетных записей и требования к стойкости паролей, их попыток неправильного ввода и правил обновления.

В обоих типах КИП (внутренних и внешних) существует множество разнообразных потоков информации. Использование протоколов шифрования и VPN-туннелей внутри и снаружи Интранета организации гарантирует, что передача информации является конфиденциальной и при передаче/получении информации обеспечена ее целостность.

Итак, защищенный КИП — это приложение, в котором управление доступом осуществляется централизованно при постоянном мониторинге событий ИБ и адекватной реакции на них. При большом количестве объектов и ресурсов (портал масштаба среднего предприятия) представляется затруднительным децентрализованное управление подсистемой авторизации, также это может привести к перегрузке канала запросов к подсистеме авторизации. В этом случае ресурсы общего доступа или подобные им корпоративные ресурсы размещают под централизованным управлением в Интранете, а более детальный контроль доступа к защищаемым ресурсам реализуется средствами КИП. Порталу предоставляется неограниченный доступ ко всем ресурсам, размещенным на нем, и на него возлагаются

функции по контролю доступа пользователей. В рамках данной модели контроль доступа осуществляется средствами самого портала. Однако при этом высокие привилегии, предоставленные порталу, создают угрозу компрометации всех его ресурсов при компрометации всего лишь одного (поскольку уязвимость самого слабого звена означает уязвимость всей системы).

Правильно спланированный КИП должен обладать механизмами инвентаризации и организации источников информации, определения пользователей данной информации и установления правил организации и контроля доступа к ней. При этом решение по управлению доступом должно в первую очередь:

- быть унифицированным;
- предоставлять гибкие модели администрирования для эффективного управления и легкой интеграции с веб ориентированными корпоративными приложениями и различными источниками информации;
- иметь открытые интерфейсы и поддержку технологий, построенных на базе стандартов, что позволяет быстро разрабатывать и внедрять новые сервисы;
- предусматривать возможность мониторинга инфраструктуры в режиме реального времени;
- быть масштабируемым для удовлетворения требований постоянно растущего бизнеса;
- иметь надежную и универсальную подсистему безопасности.

Кроме того, первым этапом разработки и внедрения портального решения должны являться определение и разработка требований безопасности. Отметим, что приведенные в данной статье требования безопасности, разделенные на шесть основных групп, являются базовыми. Данный список не претендует на полноту и может дополняться в зависимости от специфики эксплуатации и дальнейшего развития портальных технологий.

3.1. Общие требования безопасности

· Доступ к защищенным ресурсам портала предоставляется только после успешной процедуры идентификации и авторизации. Выбор протоколов аутентификации осуществляется исходя из категории информации.

· Все действия пользователей портала должны быть запротоколированы. Уровень детализации журнала регистрации должен быть четко определен.

· Должна быть обеспечена защита периметра КИП путем применения дополнительного ПО или встроенных подсистем безопасности (например, межсетевые экраны, системы обнаружения и предотвращения вторжений и пр.).

· Пользователям в рамках портального интерфейса не должны быть доступны интерфейсные объекты (ссылки, кнопки, блоки данных и пр.), выполняющие действия, не разрешенные данному пользователю. Пользователю могут быть предоставлены только справочные элементы, описывающие действия, которые могут быть выполнены с его привилегиями, а также функции поиска, возвращающие результаты поисковых запросов только по той информации, доступ к которой предоставлен пользователю.

· Разработчики порталов должны определить типы сетевого трафика, необходимого для администрирования и работы портала. Остальной трафик должен быть заблокирован.

· Взаимодействие субъектов доступа (пользователи, процессы) с объектами доступа (html-страницы, портлеты и пр.) определяется операциями (создание, модификация, удаление), при этом любое взаимодействие должно осуществляться в рамках принятой модели безопасности.

3.2. Требования к модели контроля доступа

· Информация подсистемы контроля доступа КИП должна храниться централизованно в единой структуре с контролем целостности и протоколирования совершенных в ней изменений.

· Пользователи должны иметь возможность отправить заявку на регистрацию учетной записи. При этом только авторизованные пользователи (администраторы) могут создавать/удалять учетные записи после подтверждения поданной заявки.

· Портал должен включать функциональность для логической консолидации пользователей в группы/роли для распределения привилегий по ним.

· Разрешение на использование любой функции портала должно предоставляться путем наделения соответствующими привилегиями учетных записей или групп, в которые входят данные учетные записи. Пользователь, входящий в группу, получает все привилегии данной группы. Группы входят в состав ролей. Роли определяют функциональную позицию сотрудника в организации.

· Должны быть определены списки всех привилегий с описанием всех возможных действий, которые можно выполнить через портальный интерфейс с имеющимися привилегиями.

· Каждый запрос к КИП должен проходить через процедуры аутентификации и авторизации.

· Зарегистрированные пользователи могут отправлять в КИП данные в различных форматах. Данная информация должна попадать в хранилище портала только после процедуры верификации (проверки антивирусным ПО, контроля корректности форматов и пр.), модерации, контекстного анализа.

· Доступ к функциям по управлению компонентами КИП должен быть возможен только в рамках выполнения административных операций пользователям, обладающим соответствующими полномочиями.

· После установленного администратором периода неактивности учетная запись пользователя должна быть заблокирована.

3.3. Требования к механизмам проверки пользовательских данных

· Все данные, переданные пользователем портала через веб-интерфейс, должны проходить проверки на их корректность (отсутствие управляющих символов, правильная кодировка и пр.)

3.4. Требования к портальному решению

· Портальное решение должно быть установлено и настроено с применением принципа минимальных привилегий.

· Любое ПО, в котором отсутствует необходимость при работе портала, должно быть удалено.

· Должен быть проведен анализ конфигурационных параметров и их значений, установленных «по умолчанию» для используемого ПО (включая ОС, сервера приложений, веб-сервера и пр.), для выявления настроек, потенциально приводящих к уязвимостям решения.

· Необходимо проведение регулярного анализа ресурсов портала специализированными сканерами защищенности с целью выявления уязвимых компонентов и ликвидации возможных угроз ИБ.

3.5. Требования к подсистеме обработки ошибок

· Любая страница, содержащая информацию об ошибках, должна отображать общее описание ошибки без детализации информации о ней. Любая информация, раскрывающая работу внутренних механизмов или процессов, а также информация о текущем состоянии портала должна быть исключена.

3.6. Требования к процессу разработки

· Все данные, связанные с разработкой КИП (исходные тексты, конфигурационные данные, тестовые учетные записи и пр.), должны передаваться по публичным сетям (Интернет) в зашифрованном виде.

· В процессе разработки или тестирования до установки новых версий ПО все существующие версии должны быть удалены штатным образом.

· Разработка или тестирование на работающем портальном сервере должны быть запрещены.

· В случае перевода аппаратных средств, использовавшихся при разработке, в промышленную эксплуатацию установленное ПО должно быть полностью удалено и выполнена процедура очистки содержимого жестких дисков.

4. Модель защищенного КИП

Сегодня многие портальные серверы приложений поддерживают встроенные механизмы аутентификации, авторизации и аудита. Для портальных решений, обрабатывающих некритичную информацию, риски нарушения конфиденциальности, целостности и доступности которой невелики, данных механизмов может оказаться вполне достаточно.

При необходимости повышения защищенности КИП применение концепции так называемого внешнего менеджера безопасности (ВМБ) предоставит гораздо более гибкие возможности для построения защиты. Кроме того, ВМБ позволяет централизовать управление безопасностью всех приложений, входящих в состав портального решения. Существует два возможных варианта его реализации.

1. *«Надстроенная» подсистема информационной безопасности (ПИБ)*. Этот подход применим, если необходимо обеспечить безопасность портала, уже находящегося в эксплуатации. Однако он обладает рядом существенных недостатков. Надстроенную ПИБ для существующего КИП сложней разработать, так как изменение портальной архитектуры в случае, если разработчики портала при его реализации не планировали использовать внешние компоненты безопасности, может оказаться трудоемким или невозможным (из-за несовместимости, например). При этом поиск уязвимостей в ПИБ в данном случае будет более сложен, чем разработка комплексной стратегии обеспечения ИБ КИП с начального этапа. К тому же нарушается принцип непрерывности защиты, подразумевающий проведение оценки уровня безопасности на всех жизненных циклах портального решения.

2. *ПИБ, построенная на основе ВМБ*. Более правильным является изначальная разработка портального решения одновременно со встроенной (интегрированной) ПИБ. Данный подход позволяет учесть все необходимые требования безопасности на самом раннем этапе проектирования и гарантирует эффективную, целостную защиту КИП.

В то же время, разрабатывая ПИБ, необходимо предоставить бизнесу не только гарантии надежной защиты портальных ресурсов, но и возможность адекватного управления данной системой, что может быть обеспечено единым, централизованным на уровне всей Интранет Менеджером безопасности, который взаимодействует с соответствующими сервисами безопасности.

Основные подсистемы защищенного портального решения приведены на рис. 1.

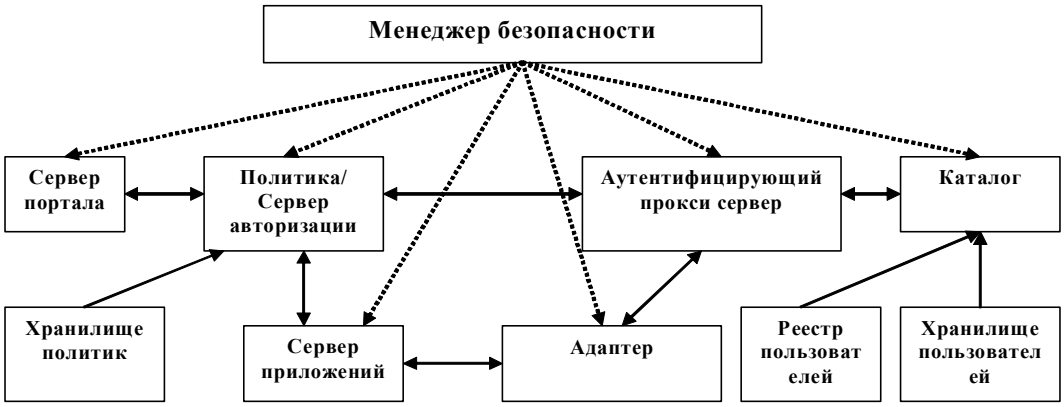

Рис. 1. Архитектура защищенного портала

1. *Сервер портала (СП)*. Один из основных компонентов портала, с которым непосредственно взаимодействуют пользователи, выполняющий функции отображения контента приложений и основные операции.

2. *Реестр пользователей (РП)*. БД, содержащая информацию об учетных записях пользователей, обычно это ID пользователя и пароль. Используется в современных системах единой регистрации Single Sign-On.

3. *Хранилище пользователей (ХП)*. БД, содержащая информацию о профилях учетных записей, например: имя или адрес. Возможно разнесение РП и ХП на два независимых хранилища.

4. *Каталог (К)*. Данная подсистема обеспечивает подсистему аутентификации соответствующей информацией из РП и информацией, хранимой в профиле пользователя в ХП. Доступ к каталогу может быть предоставлен по протоколам Lightweight Directory Access Protocol (LDAP). РП может

использовать сервис каталога или собственное хранилище. В случае использования внешнего ВМБ более предпочтительным является использование сервиса каталога. В случае автономного решения защищенного портала любой из вариантов может быть использован. Однако LDAP в дальнейшем позволит осуществить более простую интеграцию с ВМБ.

5. *Сервер приложений (СПр)*. Компонент, отвечающий за все базовые портальные сервисы (например, доступ к документу, групповую работу, механизмы индексации, прикладные шлюзы и пр.), одним из которых является сервис безопасности.

6. *Аутентифицирующий прокси-сервер (АП)*. Все запросы и ответы перенаправляются через АП. Он использует каталог для доступа к РП для получения информации об ID пользователя и его пароле. Реверсивный прокси-сервер — компонент, используемый в основном для осуществления URL-отображений и управления сессиями пользователей для защиты структуры портала от внешних атак, также может использоваться для аутентификации. Данный компонент обычно размещается в ДМЗ-сегменте (демилитаризованной зоне — специализированном сетевом сегменте внешней сети, определяющем строгие ограничения на обмен потоками информации) в качестве фронтальной части портала.

7. *Политики/сервер авторизации (ПАС)*. Компонент, ответственный за управление безопасностью. ПАС поддерживает основное хранилище политик с данными подсистемы авторизации и контроля доступа.

8. *Хранилище политик (ХП)*. ХП является хранилищем списков контроля доступа (ACL-листов), используемых ПАС для контроля доступа к ресурсам.

9. *Адаптер*. Компонент, отвечающий за взаимодействие между СПр и ПАС. Он проверяет запрос и предоставляет ID пользователя СПр, получая его от ПАС.

10. *Менеджер безопасности (МБ)*. Координирует все механизмы безопасности, управляя ими централизованно.

Процесс аутентификации и авторизации пользователей портала представлен в табл. 1.

Таблица 1. Процесс аутентификации и авторизации

Аутентификация пользователя портала	**Авторизация: доступ к защищенному ресурсу**
1. Запрос принимается АП. 2. АП определяет, что запрошенный ресурс является защищенным, после чего переадресует пользователя на страницу аутентификации (например, HTTP-аутентификация или аутентификация на основе html-форм). 3. Пользователь вводит и передает свой ID и пароль. 4. АП проверяет предъявленный ID и пароль на соответствие хранимым в РП. После успешной аутентификации создается ID сессии для дальнейшей идентификации запросов пользователя, который сохраняется в cookie-файлах. 5. АП сохраняет информацию о сессии пользователя в HTTP-заголовках и переадресует запрос СПр. 6. СПр получает запрос и вызывает адаптер для получения информации о полномочиях пользователя. 7. СПр выполняет поиск пользователя в РП. В случае успеха СПр создает токен, идентифицирующий пользователя. 8. Запрос поступает на ПС и результат возвращается через АП пользователю	Предположим, что пользователь предварительно прошел процедуру аутентификации. 1. Запрос поступает на АП. 2. АП перенаправляет полномочия пользователя к СПр. 3. Поскольку пользователь уже прошел процедуру аутентификации, его запрос перенаправляется СПр к ХП. 4. ХП проверяет необходимые права доступа для запрошенного ресурса. 5. ХП запрашивает ПАС на предмет наличия пользователей/групп для ролей запрошенного ресурса. 6. Определяется уровень соответствия предъявленных и необходимых полномочий и возвращается результат проверки полномочий

Итак, основными методами защиты КИП в приведенной выше модели являются следующие:
- строгая аутентификация субъектов и объектов доступа;
- централизованный и детализированный контроль доступа к портальным ресурсам;
- выбор правильной архитектуры портала;
- мониторинг и аудит событий ИБ (включая использование, учет и анализ использования ресурсов и результаты проверки переданных пользователями данных);
- защита системных компонент портала.

5. Возможная реализация защищенного корпоративного портала

Существует два способа реализации защищенного КИП.

Первый — приобрести хорошо известное на рынке промышленное портальное решение (IBM WebSphere Portal, Microsoft SharePoint, Oracle Application Server Portal, SAP Enterprise Portal и пр.), полагаясь на мнение экспертов по безопасности. В настоящее время крупные игроки на рынке портального ПО осознали необходимость поддержки в своих решениях технологий безопасности корпоративных ресурсов и предлагают уже готовые решения [6].

Второй вариант — разработка собственного решения со всеми необходимыми сервисами безопасности и с учетом специфики бизнес-процессов и информационной инфраструктуры организации. Тогда построение защищенного портала требует использования большинства стандартных технологий безопасности (например, протоколов SSL/TLS). Поддержка промышленных стандартов (таких как LDAP, NTLM, NIS и пр.) дает организациям возможность интеграции построенного решения со всей информационной инфраструктурой, а также гибкой адаптации его настроек безопасности с учетом возможного изменения требований безопасности. Также должны применяться средства мониторинга и аудита ИБ (встроенный аудит, системы обнаружения/предотвращения вторжений и пр.) за всеми информационными потоками для выявления событий информационного обмена, потенциально указывающих на возможные проявления угроз ИБ.

Одновременно с этим разработка портального решения должна осуществляться с применением проверенной и наиболее надежной с точки зрения ИБ среды разработки.

СПИСОК ЛИТЕРАТУРЫ

1. *Horgan T.* Developing Your Intranet Strategy and Plan. http://www.cio.com.
2. *Christopher C.* Shilakes and Julie Tylman. Enterprise Information Portals. Merrill Lynch, Inc., New York, NY, November 16, 1998.
3. http://www.sans.org/resources/policies.
4. http://www.eff.org/Censorship/Academic_edu/CAF/policies.
5. IBM redbook. http://www.redbooks.ibm.com.
6. *David K. Black*. Portal Security: Managing Identities and Relationships in a Competitive Economy. http://www.accenture.com/xdoc/en/services/secsol/insights/portal.pdf.