МОДЕЛИРОВАНИЕ СИСТЕМ

УДК 37.016

ОСОБЕННОСТИ АРХИТЕКТУРЫ ЗАЩИЩЕННОГО КОРПОРАТИВНОГО ПОРТАЛА

© 2016 Т. В. Глотова, В. Н. Кострова

Воронежский институт высоких технологий
Воронежский государственный технический университет

В статье рассматриваются предложения по построению корпоративного портала. Отмечены его функциональные возможности. Описана система защиты портала. Перечислены задачи, которые можно решать с помощью портала. Для защиты атак из внешней сети описаны соответствующие функции.

Ключевые слова: портал, связь, защита, пользователь, архитектура, сеть.

В качестве интеграционного решения нами была выбрана intranet-технология как единственный реальный способ объединить все системы, построенные на различных платформах, использующих разные операционные среды, базы данных и приложения. Система обеспечения безопасности информации (СОБИ) корпоративного портала должна включать следующие основные элементы:

- сервер доступа;
- брокер услуг на основе proxy-сервера;
- агенты идентификации пользователей, использующие смарт-карту.

На сетевом уровне безопасность передаваемой информации обеспечивается за счет VPN-агентов, устанавливаемых на всех серверах портала и рабочих станциях пользователей. Для аутентификации субъекта доступа используется агент идентификации, устанавливаемый на рабочей станции пользователя. Агент опрашивает смарт-карту, определяет, установлен ли VPN-агент, загружает сертификат и ключ пользователя в VPN-агент и от имени пользователя запрашивает на сервере доступа конкретный информационный ресурс портала. В процессе запроса сервер доступа формирует уникальный билет доступа к данному ресурсу в форме пакета с косвенной идентификационной информацией. Билет доступа действует только для данного клиента и только для выбранного ресурса, причем время его действия ограничено. По билету пользователя запускается процедура предоставления выбранного ресурса портала. Каждый выданный билет регистрируется в системе и доступен для мониторинга. Принцип выдачи билетов реализует механизм распараллеливания и балансировки нагрузки в системе предоставления доступа.

Сервер доступа обеспечивает мажоритарную модель разграничения прав доступа к конфиденциальным ресурсам портала и поддерживает такие понятия, как пользователь, группа пользователей, ресурс, тип ресурса, атрибуты ресурса, привилегии пользователя на атрибуты ресурса, уровень доступа к ресурсу. Права и привилегии могут наследоваться по пользователям, группам и услугам с возможностью добавления и исключения. Поддерживаются установка и контроль времени жизни назначаемых прав.

В функциональном плане портал поддерживает:

- проведение классификации ресурсов портала (общую и пользовательскую);
- предоставление информации в соответствии с ролями пользователей;
- гарантированную доставку информации;
- подписку пользователей на информационные ресурсы;
- уведомление пользователей;
- проведение аудиты работы пользователей с информационным ресурсом.

Глотова Татьяна Витальевна – Воронежский институт высоких технологий, студент, e-mail: BlohTat@yandex.ru.
Кострова Вера Николаевна – Воронежский государственный технический университет, д. т. н., профессор, e-mail: kafeckostrb@yandex.ru.

Прежде всего, необходимо понять, что именно мы защищаем, то есть, выделить объект защиты. Понятно, что защищается информация, это касается не только конфиденциальной информации, в портальных решениях необходимо защищать и открытую информацию. Можно вспомнить распространенную цель в хакерских атаках, связанную с искажением или заменой главных страниц на популярных порталах и Web-сайтах. Это значит, что в таких случаях нам необходимо принять контрмеры, противостоящие нарушениям целостности информации.

В системе защиты порталов необходимо обеспечить свойства конфиденциальности, целостности и доступности информации. На ее основе должны устраняться либо компенсироваться угрозы (говорят об обобщающем понятии «парирование угроз»). Если говорить о полном перечне угроз информации на портале, который сгруппирован по трем основным характеристикам безопасности информации (речь идет о конфиденциальности, целостности, доступности), то это можно представить таким образом:

Конфиденциальность:

- осуществление хищения информации;
- проведение незаконного копирования и распространения;
- происходят процессы утраты информации.

Целостность:

- осуществление модификации информации;
- проведение отрицания подлинности;
- проведение навязывания ложной информации.

Доступность:

- осуществление уничтожения информации;
- проведение блокирования доступа.

Множество угроз могут быть нейтрализованы на основе организационно правовых методов. Например, угрозы, связанные с незаконным копированием и распространением, то есть, нарушением авторских прав мы можем эффективным образом убрать лишь на основе применения правовых методов. Если мы будем вводить и практически реализовать более жесткие правовые нормы, связанные с тем, что нарушается конфиденциальность, целостность, доступность информации, то это может привести к снижению числа внедрений на сайты и порталы.

Какие проблемы при учете оставшихся (после использования соответствующих организационно-правовых способов) угроз необходимо решать в системе собственной безопасности? Мы можем сформировать такой список:

- проведение защиты от несанкционированного доступа к ресурсам, расположенным на портале (это относится к пользователям, не имеющим соответствующих полномочий, а также к посторонним лицам);
- осуществление контроля степени подлинности и целостности по ресурсам в портале;
- проведение централизованного управления средствами СОБИ в рамках политик безопасности портала;
- осуществление оперативного аудита по тому, чтобы была безопасность на портале, обеспечивалась полная подконтрольность по всем совершаемым порталом операций;
- проведение организации того, чтобы было безопасное подключение портала к Интернету;
- осуществление обнаружения внедрений и применение антивирусной защиты.

Важную роль при решении возникающих задач имеют сетевые и прикладные уровни обеспечения безопасности порталов, следует отметить, что прикладной уровень имеют, большей частью, программные продукты, а сетевой – программно-технические.

На прикладном уровне обеспечивается безопасность для информации на портале для более высокого иерархического уровня. Для прикладного уровня требуется использовать функции безопасности, которые недостижимы для более низких уровней, это такие:

- проведение идентификации пользователей;
- проведение однократной (SSO) аутентификации пользователей;
- осуществление ролевого (RBAC) управления доступом к информационным ресурсам на портале;
- проведение контроля подлинности и целостности по некоторым ресурсам портала на основе применения технологий ЭЦП;
- мониторинг и аудит.

На сетевом уровне защиты портала можно отметить более насыщенный функционал, возможно, в связи с тем, что любую внешнюю атаку, как правило, начинают на сетевом уровне. Стоит добавить еще вирусы и злонамеренный код, который проникает, большей частью, сквозь периметр корпоративных сетей. Для того, чтобы противодействовать возникающим угрозам для сетевого

уровня необходимо проводить организацию защиты от атак, как по внешним, так и внутренним сетям.

Для осуществления защит от атак из внешней сети требуется использовать такие функции безопасности:

- формирование рубежей защиты для сетевого периметра;
- проведение организации защищенных обменов информацией для внешних источников;
- проведение обнаружения и блокирования вторжений;
- проведение обнаружения, блокирования распространения, уничтожения вредоносных программ.

С целью проведения защит от атак из внутренних областей требуется проведение решение следующих задач:

- осуществление устранения / уменьшения угроз, которые связаны с тем, что есть неправомочные действия со стороны кадров, контрагентов, кадров внешних обслуживающих предприятий и других людей;
- осуществление выявления уязвимостей и слабостей по программно-техническим средствам портала;
- проведение сегментирования сети относительно уровней конфиденциальности, по территориальным и функциональным признакам.

Реализация функций защиты большей частью может быть реализована на основе того, что внедряются технологии VPN, межсетевые экраны и IDS, обеспечивающие защиты по сетевому периметру, формирование и управление по защищенным виртуальным сетям, проведение сегментирования сетей для уровней безопасности, и еще проведение интеграции систем антивирусной защиты, проведение обнаружения по вторжениям и поиске уязвимостей.

Для формирования архитектур систем обеспечения безопасности нами предлагается такие подсистемы:

- для осуществления управления безопасностью;
- для того, чтобы идентифицировать и аутентифицировать;
- для того, чтобы управлять доступом к информации;
- для осуществления процедур, связанных с контролем целостности информации;
- для проведения регистрации и аудита;
- при управлении ключами и сертификатами.

Для данных подсистем отношение имеют прикладной уровень и сетевой.

Архитектурные решения СОБИ должны реализоваться так, чтобы такие подсистемы интегрировались в единое целое. Проблему можно формулировать таким образом: проведение интеграции управления для подсистем безопасности в сетевом и прикладном уровнях на основе разработанной политики безопасности, которая состоит из множества формализованных правил, связанных с доступом к сегментам сетей, хосту, порту, сервису, приложениям, есть еще правила, позволяющие аутентифицировать субъекты доступа, мониторинга того, какова характеристика безопасности порталов. Проведение формализации и решение указанной проблемы может определить улучшение математических моделей и методов.

В сервере управления безопасностью формируется общая политика безопасности как множество правил по тому, чтобы был сетевой доступ к сегментам, хосту, порту, сервису и правилам proxy-доступа к сервисам, портлетам приложениям и статическим информационным ресурсам. Происходит трансляция указанной политики в соответствующие локальные политики FW/VPN агентов и proxy-систем, потом происходит доставка и исполнение на них.

То, что нет выходного proxy-сервера в анализируемой архитектуре портала, можно объяснить тем, что в системах мы не стремились к тому, чтобы защищать доступ к ресурсам среды Интернет, так как подобный доступ из внутренней сети является запрещенным.

Если подвести итоги, то можно сформулировать три базовых преимущества анализируемой архитектуры СОБИ в портале.

• Применять решения можно различного вида портальных систем и платформ.

• Нет необходимости в переработке кодов портальных приложений.

• Применение типовых протоколов сетевого уровня (IP/IPSec) и прикладного уровня (HTTP/HTTPS) дают улучшение интегрируемости средств защиты и реализацию функций, относящихся к безопасности.

Основным является то, что указанное решение может рассматриваться как типовое для разных портальных систем и что оно является «разъемным», то есть при осуществлении интеграции с действующим порталом его можно встроить без того, чтобы перерабатывать код в портальных приложениях.

Отметим базовые преимущества в рассматриваемой архитектуре системы безопасности корпоративных порталов:

- Решение можно применять для большого круга портальных систем и платформ.

- Нет необходимости в переработке кодов портальных приложений.

- За счет типовых протоколов сетевого уровня (IP/IPSec) и прикладного уровня (HTTP/HTTPS) улучшается интегрируемость по средствам защиты и реализуемости функций безопасности.

ЛИТЕРАТУРА

1. Землянухина Н. С. О применении информационных технологий в менеджменте / Н. С. Землянухина // Успехи современного естествознания. – 2012. – № 6. – С. 106-107.

2. Преображенский Ю. П. Формулировка и классификация задач оптимального управления производственными объектами / Ю. П. Преображенский, Р. Ю. Паневин // Вестник Воронежского государственного технического университета. – 2010. – Т. 6. – № 5. – С. 99-102.

3. Завьялов Д. В. О применении информационных технологий / Д. В. Завьялов / Современные наукоемкие технологии. – 2013. – № 8-1. – С. 71-72.

4. Москальчук Ю. И. Проблемы оптимизации инновационных процессов в организациях / Ю. И. Москальчук, Е. Г. Наумова, Е. В. Киселева // Моделирование, оптимизация и информационные технологии. – 2013. – № 2. – С. 10.

5. Филипова В. Н. О применении информационных технологий в туристической сфере / В. Н. Филипова // Успехи современного естествознания. – 2012. – № 6. – С. 112-113.

6. Кудрина О. С. О проблемах медиаобразования / О. С. Кудрина // Современные наукоемкие технологии. – 2013. – № 8-1. – С. 72-73.

7. Ряжских А. М. Построение стохастических моделей оптимизации бизнес-процессов / А. М. Ряжских, Ю. П. Преображенский // Вестник Воронежского института высоких технологий. – 2008. – № 3. – С. 079-081.

8. Зяблов Е. Л. Построение объектно-семантической модели системы управления / Е. Л. Зяблов, Ю. П. Преображенский // Вестник Воронежского института высоких технологий. – 2008. – № 3. – С. 029-030.

9. Лисицкий Д. С. Построение имитационной модели социально-экономической системы / Д. С. Лисицкий, Ю. П. Преображенский // Вестник Воронежского института высоких технологий. – 2008. – № 3. – С. 135-136.

10. Преображенский Ю. П. Некоторые аспекты информатизации образовательных учреждений и развития медиакомпетентности преподавателей и руководителей / Ю. П. Преображенский, Н. С. Преображенская, И. Я. Львович // Вестник Воронежского государственного технического университета. – 2013. – Т. 9. – № 5-2. – С. 134-136.

11. Исакова М. В. Об особенностях систем управления персоналом / М. В. Исакова, О. Н. Горбенко // Вестник Воронежского института высоких технологий. – 2014. – № 12. – С. 168-171.

12. Фомина Ю. А. Принципы индексации информации в поисковых системах / Ю. А. Фомина, Ю. П. Преображенский // Вестник Воронежского института высоких технологий. – 2010. – № 7. – С. 98-100.

THE ARCHITECTURE IS PROTECTED ENTERPRISE PORTAL

© 2016 T. V. Glotova, V. N. Kostrova

Voronezh Institute of high technologies
Voronezh state technical University

The paper discusses suggestions for building a corporate portal. Marked by its functionality. Described the protection system of portal. Lists the tasks that can be solved using the portal. To protect attacks from the external network described respective functions.

Keywords: portal, communications, security, user, architecture, network.