ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ ИНТЕРНЕТ-ПОРТАЛОВ

В.И. Шилин
А.А. Круглов

В соответствии с современными принципами построения информационной инфраструктуры организации взаимодействие государственного учреждения или коммерческой структуры с гражданами (клиентами), другими организациями, включая органы управления, целесообразно обеспечить с помощью создаваемого в сети Интернет информационного портала, представляющего собой единую точку доступа ко всем потребителям, ресурсам либо, как вариант, к набору информационных сервисов.

Основной задачей создания общедоступных Интернет-порталов является повышение уровня информационного обеспечения населения России, других потребителей о деятельности федеральных и региональных органов исполнительной власти, социально-экономическом развитии страны, законотворческой деятельности и т.д. Примерами таких Интернет-порталов являются Правительственный портал, порталы государственной статистики России, Центральной избирательной комиссии России и др.

В рамках ряда Интернет-порталов, создаваемых органами государственной власти или коммерческими структурами, должны быть реализованы задачи обеспечения свободного доступа всех пользователей сети Интернет к общедоступным ресурсам, а также организации работы авторизованных пользователей портала с теми или иными сервисами (приложениями). К таким задачам, решаемым с помощью портальных технологий, можно отнести реализацию систем электронной торговли (СЭТ), обеспечение защищенного доступа удаленных пользователей к корпоративным ресурсам и т.д. Например, в связи с тем, что в регионах РФ реализация типового решения СЭТ (системы электронных госзакупок для региональных и муниципальных нужд) проводится в рамках развертывания региональных Интернет-порталов, целесообразно решать вопросы обеспечения безопасности информационных систем (ИС), реализуемых с использованием портальных технологий, на основе единого подхода.

В соответствии с Доктриной информационной безопасности Российской Федерации одна из важнейших задач в информационной сфере — обеспечить «защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России». В полной мере такая проблема стоит при создании в сети Интернет общедоступных и корпоративных порталов.

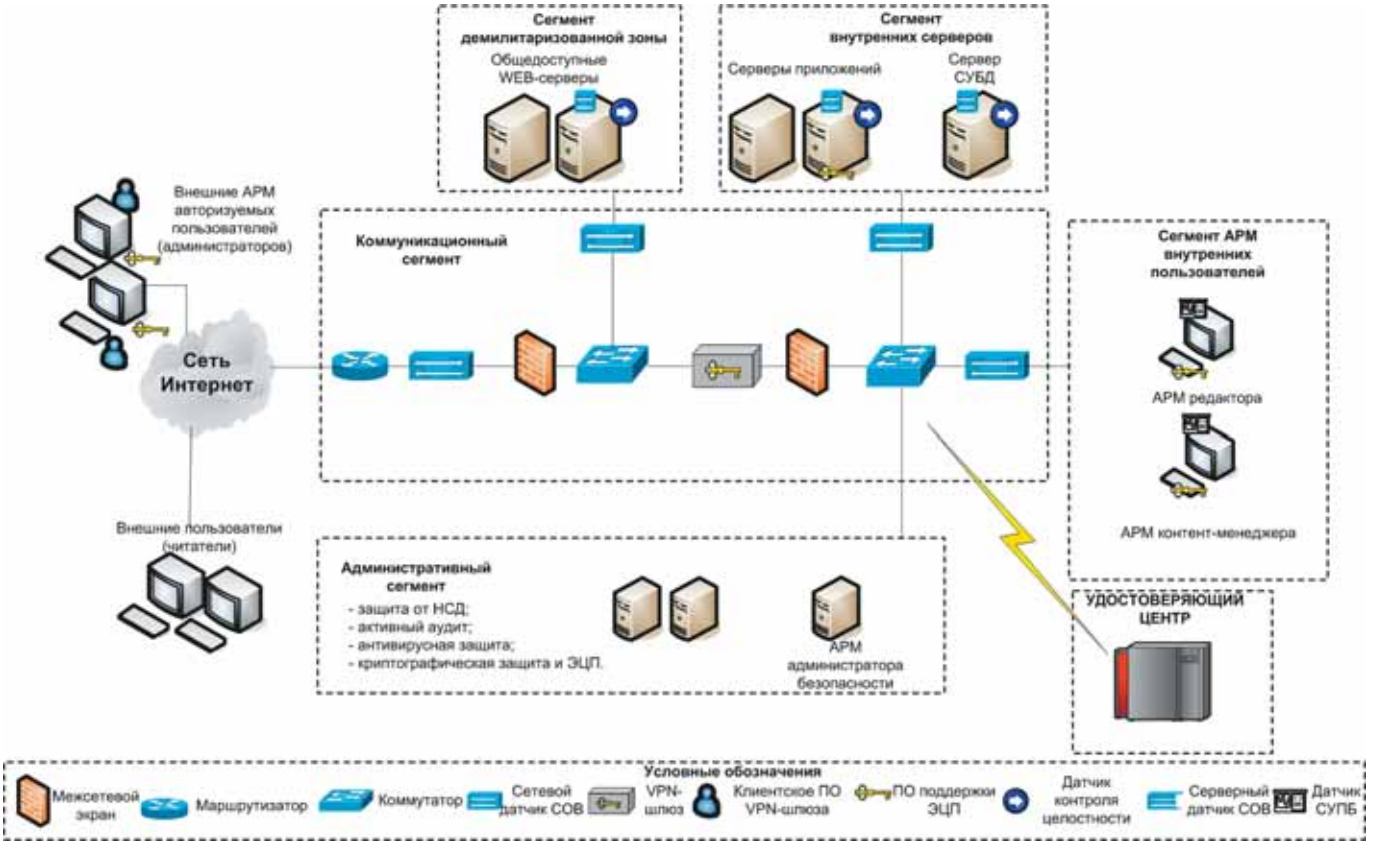
В настоящее время проблема защиты информационных ресурсов подобных распределенных ИС, использующих открытые каналы связи (Интернет), может быть решена на основе комплексного интегрированного подхода к обеспечению информационной безопасности Интернет-порталов. Это достигается путем создания в рамках единого процесса проектирования ИС подсистемы (системы) защиты информационных ресурсов (ПОЗИР) портала.

Под ПОЗИР будем понимать комплекс мер и средств, направленных на выявление, отражение и ликвидацию характерных угроз безопасности Интернет-портала.

Современная концепция защиты объектов информатизации, включая Интернет-порталы, предполагает реализацию следующей последовательности действий:

— проведение анализа функционирования объектов информатизации и выделение ресурсов (элементов), требующих обеспечения безопасности информации (определение объектов защиты);
— определение возможных угроз, их ранжирование по значимости и формирование перечня требований по обеспечению безопасности информации защищаемых ресурсов;
— разработка адекватных угрозам безопасности информации мер, выбор средств и технологий защиты;
— согласование выбора информационных технологий (программно-аппаратных и сетевых средств) с точки зрения применимости средств защиты информации и реализация на базе ПОЗИР комплексного подхода к защите информационных ресурсов Интернет-портала.

Необходимо учитывать, что ПОЗИР является поддерживающей системой по отношению к порталу. Она должна включать адекватные средства защиты во все информационные технологии (ИТ), защищать критически важные ресурсы и информацию, не ухудшая потребительских качеств программных и ап-



паратных средств ИС. При этом применяемые меры и средства защиты ИТ должны реализовывать требования Доктрины информационной безопасности Российской Федерации, Федерального закона «Об информации, информатизации и защите информации», ГОСТов, руководящих документов ФСТЭК (Гостехкомиссии) России, других действующих в России нормативно-правовых документов в области обеспечения информационной безопасности.

Это обеспечивается путем использования ряда взаимосвязанных защитных организационно-технических механизмов, позволяющих существенно уменьшить вероятность реализации основных угроз и создать платформу как для совершенствования всей системы управления защитой информационных ресурсов, так и для безопасного наращивания функций Интернет-портала.

Информация, предоставляемая пользователям (читателям) общедоступных Интернет-порталов, является открытой. Поэтому основной задачей в части реализации безопасности порталов является обеспечение целостности и доступности их информационных ресурсов. В этой связи от ПОЗИР требуется, в первую очередь, обеспечить целостность циркулирующей в Интернет-портале информации, а также ее защиту от несанкционированного доступа (НСД) из сети Интернет. Кроме того, в соответствии с требованиями Указа Президента РФ от 12.05.2004 г. № 611 информация, размещаемая на портале, должна быть достоверной.

Таким образом, наиболее актуальными являются задачи:

— обеспечения целостности и доступности информации, реализуемые в рамках портальных решений СЭТ;
— организации защищенного доступа удаленных пользователей к информационным ресурсам портала;
— обеспечения конфиденциальности информации управления порталом, передаваемой по сетям общего пользования (Интернет);
— реализации процедур строгой аутентификации авторизованных пользователей на портале при доступе к корпоративным ресурсам и др.

В частности, ключевой проблемой при обеспечении безопасности информации СЭТ является обеспечение целостности и достоверности циркулирующих в системе электронных документов. Наличие такого требования, а также упомянутых выше требований Указа № 611 подразумевает включение в ПОЗИР портала программно-технических средств, гарантирующих:

— доказуемость авторства внесенных, измененных и удаленных записей, образующих электронные документы, в том числе при размещении на портале информационного контента;
— санкционированное внесение, изменение и удаление администраторами портала записей в базах данных и т.д.

Более подробно эти требования будут описаны ниже.

Структура типового защищенного Интернет-портала должна быть построена таким образом, чтобы технологии защиты, реализуемые в рамках ПОЗИР, были задействованы во всех решаемых порталом информационных задачах (администрирования портала; управления как общедоступным, так и внутренним, предназначенным для авторизуемых пользователей информационным контентом; подключения портала с помощью телекоммуникационных средств к сети Интернет и др.).

Структурная схема построения ПОЗИР типового защищенного Интернет-портала приведена на рисунке.

Реализуется принцип сегментирования локальной вычислительной сети (ЛВС) Интернет с учетом наличия разных требований к уровням защищенности конкретных сегментов.

Выделены сегменты:

— внутренних серверов — содержит серверы приложений (рабочие серверы), серверы баз данных и др.;
— демилитаризованной зоны (ДМЗ) — включает серверы, реализующие потенциально опасные сетевые службы и сервисы. К этому разряду следует отнести публичные общедоступные Интернет-серверы, обеспечивающие прием запросов, их обработку, включая кэширование, а также передачу информации конечным пользователям;
— коммуникационный — содержит активное и пассивное коммуникационное оборудование, обеспечивающее сегментирование ЛВС и подключение Интернет-портала к сетям общего пользования;
— административный — включает серверы, обеспечивающие функциональность развернутых средств защиты, а также автоматизированные рабочие места (АРМ) администраторов Интернет-портала (администраторов сети, администратора безопасности и т.д.);
— внутренних пользователей — состоит из АРМ внутренних пользователей (администраторов) — редакторов и контент-менеджеров, обеспечивающих наполнение информационного контента на портале;
— внешних пользователей — содержит (АРМ) авторизуемых внешних пользователей (администраторов). В состав этого сегмента условно можно включить и всех пользователей сети Интернет — «читателей» информации, размещаемой на портале.

Функциональная схема построения ПОЗИР типового защищенного Интернет-портала

В целях обеспечения комплексной защиты информационных ресурсов типового Интернет-портала его ПОЗИР должна реализовывать следующие основные функции и включать в себя соответствующие подсистемы:

— защиты от НСД;
— активного аудита;
— антивирусной защиты;
— криптографической защиты и поддержки электронной цифровой подписи (ЭЦП).

Функция защиты от НСД реализуется средствами:

— защиты ресурсов портала от НСД со стороны сети Интернет и на уровне защищаемых сегментов ЛВС, в том числе штатными средствами защиты использованных в портале операционных систем (ОС) и систем управления базами данных (СУБД). Сюда же относится использование сертифицированных по требованиям безопасности информации ОС и СУБД;
— администрирования средств защиты от НСД;
— регистрации системных событий и попыток НСД к защищаемым ресурсам, оперативного оповещения администраторов безопасности о попытках НСД и т.д.

Эта подсистема обычно содержит межсетевые экраны, средства контроля целостности серверов Интернет-портала, средства доверенной загрузки АРМ и серверов и т.д. (см. рисунок).

Функции активного аудита реализуются средствами (системами) обнаружения вторжений, анализа защищенности, мониторинга и управления политикой безопасности на АРМ администраторов (пользователей) Интернет-портала.

Система обнаружения вторжений (СОВ) обеспечивает контроль поступающих из сети Интернет информационных потоков, обнаружение и отражение потенциально содержащихся в них компьютерных атак на сигнатурном и поведенческом уровнях. СОВ содержит сервер с консолью, сетевые и серверные датчики (см. рисунок).

Система анализа (контроля) защищенности (САЗ) обеспечивает проведение анализа защищенности сетевых узлов Интернет-портала путем моделирования информационных атак нарушителя.

Система мониторинга и управления политикой безопасности предназначена для проведения в режиме реального времени сбора и анализа информации о процессах, происходящих на рабочих станциях пользователей, а также для оперативного управления АРМ пользователей в соответствии с требованиями заданной политики безопасности. Система содержит сервер с консолью и датчики (агенты) на АРМ пользователей (администраторов) (см. рисунок).

Функции антивирусной защиты в Интернет-портале реализуются с помощью соответствующего ПО, устанавливаемого на всех основных аппаратно-программных средствах портала: серверах, шлюзах сети, АРМ администраторов и контент-менеджеров и др.

С помощью средств подсистемы криптографической защиты и поддержки ЭЦП производится обеспечение идентификации и аутентификации удаленных пользователей и ресурсов портала на основе использования криптографических методов защиты информации управления Интернет-порталом от несанкционированного изменения, уничтожения, ознакомления и копирования. Кроме того, входящие в подсистему средства установки и проверки ЭЦП под электронными документами и файлами в соответствии с требованиями Указа № 611 реализуют целостность и достоверность размещаемой на портале информации, подтверждение авторства внесенных тем или иным администратором (редактором) изменений в информационном контенте. Эти же средства (механизмы) могут быть задействованы для обеспечения сохранения гарантии достоверности полученной пользователем портала информации, прошедшей по сети Интернет.

В Системе электронных госзакупок для региональных и муниципальных нужд (вариант реализации СЭТ), разработанной в рамках Федеральной целевой программы «Электронная Россия», подсистема с использованием сертифицированного криптоядра позволила обеспечить следующие функции:

— формирование и проверку ЭЦП под электронным документом, созданным Web-сервером СЭТ и передаваемым пользователю по общедоступным каналам связи;
— формирование и проверку ЭЦП под электронным документом, сформированным на рабочем месте пользователя и передаваемым Web-серверу СЭТ по общедоступным каналам связи.

В итоге в СЭТ обеспечивается подлинность субъектов, подписавших данные документы, а также целостность циркулирующих в системе электронных документов.

Требованиями Указа № 611 обусловлено использование в ПОЗИР общедоступных Интернет-порталов только сертифицированных средств защиты информации (межсетевых экранов, СОВ, САЗ и др.).

В системе комплексной защиты информационных ресурсов Интернет-портала существенным моментом является применение организационных и организационно-технических мер. В частности, при вводе Интернет-портала в действие (подключении к сети Интернет) необходимо разработать всю организационную и нормативно-техническую документацию, в том числе в части обеспечения безопасности информации. Необходимо назначить и подготовить администратора безопасности, провести обучение остального персонала (контент-менеджеров и редакторов) основным правилам обеспечения безопасности информации. Также для повышения доступности информационных ресурсов Интернет-портала необходимо в полной мере использовать технологии и средства резервирования и дублирования (например, за счет применения кластерных решений), максимально задействовать средства резервного копирования и восстановления данных, другие меры.

ЗАКЛЮЧЕНИЕ

Предлагаемые для реализации комплексные организационно-технические решения позволяют обеспечить защиту информационных ресурсов разрабатываемых и уже развернутых общедоступных и корпоративных Интернет-порталов. При обеспечении необходимого уровня безопасности информации путем предотвращения и блокирования характерных угроз достигается устойчивое функционирование программно-аппаратного комплекса ПОЗИР и Интернет-портала в целом.

Предложенные решения по построению защищенных Интернет-порталов реализованы компанией ЗАО «РНТ» в рамках работ по созданию, вводу в действие и сопровождению ПОЗИР ряда Интернет-порталов, в первую очередь, ключевых органов государственной власти России.

Компания «РНТ»
Россия, 127434, г. Москва,
Дмитровское ш., д.17, к.2, а/я 78
тел.: (095) 777–7577
факс (095) 777–75–76.
e-mail: rnt@rnt.ru
http://www.rnt.ru