КАК ЗАЩИТИТЬ WEB-ПОРТАЛ ОТ ИНФОРМАЦИОННЫХ АТАК

Зиннатуллина Лилия Рафилевна

студент, Казанский национальный исследовательский технологический университет, РФ, Республика Татарстан, г. Казань

Ситдикова Алия Раилевна

студент, Казанский национальный исследовательский технологический университет, РФ, Республика Татарстан, г. Казань

Мифтахова Лина Хатыповна

научный руководитель, канд. техн. наук, старший преподаватель кафедры информационная безопасность, Казанский национальный исследовательский технологический университет, РФ, Республика Татарстан, г. Казань

В настоящее время в России, как и во всём мире, имеет место тенденция роста практического использования государственными и коммерческими организациями публичных Web-порталов, подключённых к сети Интернет. Порталы этого типа могут применяться для решения самых разнообразных задач, таких, например, как реклама в сети Интернет характера деятельности компании, организация Интернет-торговли или же обеспечение работы системы «Клиент-Банк». Этому способствует тот факт, что на сегодняшний день на отечественном рынке информационных технологий представлено несколько готовых промышленных решений, на основе которых возможно построение полнофункциональных Web-порталов. К таким решениям относится семейство продуктов «Internet Information Services» компании Microsoft, “Sun ONE “ компании Sun Microsystems и “WebSphere” компании IBM.

Типовая архитектура Web-портала, как правило, включает в себя следующие основные компоненты:

· публичные Web-серверы, которые обеспечивают доступ пользователей сети Интернет к информационным ресурсам портала;

· кэш-серверы, обеспечивающие временное хранение копии ресурсов, к которым получали доступ Интернет-пользователи. При обращении к ресурсам Web-портала первоначально производится попытка извлечения ресурса из памяти кэша-серверов, и только если ресурс там отсутствует, то тогда запрос передаётся публичным Web-серверам. Использование кэш-серверов позволяет снизить нагрузку на основные публичные серверы, а также уменьшить время доступа пользователей к кэшированным ресурсам;

· DNS-серверы, обеспечивающие возможность преобразования символьных имён серверов Web-портала в соответствующие им IP-адреса;

· серверы приложений, на которых установлено специализированное программное обеспечение, предназначенное для управления информационным содержимым Web-портала;

· серверы баз данных, которые обеспечивают централизованное хранение информационных ресурсов Web-портала;

· коммуникационное оборудование, обеспечивающее взаимодействие между различными

серверами Web-портала.

Как правило, серверы Web-порталов размещаются на территории Интернет-провайдеров, которые имеют возможность обеспечить необходимую полосу пропускания каналов, по которым серверы портала подключаются к сети Интернет. Управление Web-порталом в этом случае осуществляется удалённо через Интернет с автоматизированных рабочих мест (АРМ) администраторов. Обобщённая архитектура Web-портала изображена на рис. 1.

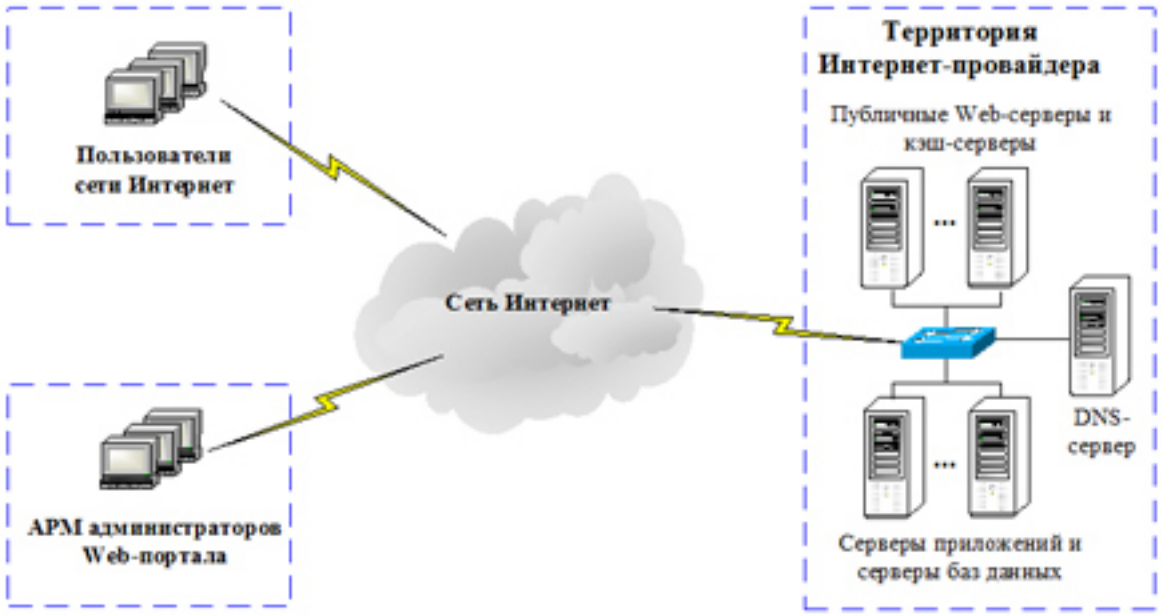

Рисунок 1. Типовая архитектура Web-портала

Учитывая тот факт, что ресурсы публичного Web-портала по определению открыты любому пользователю сети Интернет, они становятся потенциальной мишенью для атак нарушителей. Необходимо отметить, что за последние несколько лет наблюдается значительный рост информационных атак, основная часть которых направлена именно на общедоступные ресурсы, к которым относятся и Web-порталы. Атаки нарушителей могут быть направлены на нарушение конфиденциальности, целостности или доступности информационных ресурсов, хранящихся на серверах Web-портала.

Для защиты Web-портала наиболее целесообразно применять комплексный подход, сочетающий организационные и технические средства защиты. Организационные средства защиты связаны с разработкой и внедрением нормативно-правовых документов, таких как политика и концепция обеспечения информационной безопасности Web-портала, должностные инструкции по работе персонала с автоматизированной системой портала и т.д. Технические же средства защиты реализуются при помощи соответствующих программных, аппаратных или программно-аппаратных средств, которые обеспечивают выполнение целей и задач, определённых в соответствующих нормативно-правовых документах. Использование комплексного подхода предполагает объединение технических средств защиты Web-портала в интегрированный комплекс, включающий в себя подсистемы антивирусной защиты, контроля целостности, разграничения доступа, обнаружения вторжений, анализа защищённости, криптографической защиты информации, а также подсистему управления. Ниже приведено описание основных функциональных возможностей этих подсистем, а также особенностей их применения для защиты Web-портала.

Подсистема разграничения доступа

Подсистема разграничения доступа является основным элементом комплекса безопасности

Web-портала и предназначена для защиты информационных ресурсов портала от несанкционированного доступа. При помощи средств защиты, входящих в эту подсистему, Web-портал подразделяется на четыре функциональных сегмента (рис. 2):

· сегмент демилитаризованной зоны, в котором размещаются серверы портала, доступ к которым могут получить любые пользователи сети Интернет. К таким серверам относятся кэш-серверы, публичные Web-серверы и DNS-серверы;

· сегмент служебных серверов, доступ к ресурсам которых могут получить только администраторы или служебные сервисы Web-портала;

· сегмент управления, в котором размещаются средства, необходимые для управления комплексом безопасности Web-портала;

· коммуникационный сегмент, включающий в себя маршрутизаторы и коммутаторы, обеспечивающие взаимодействие между другими сегментами портала.

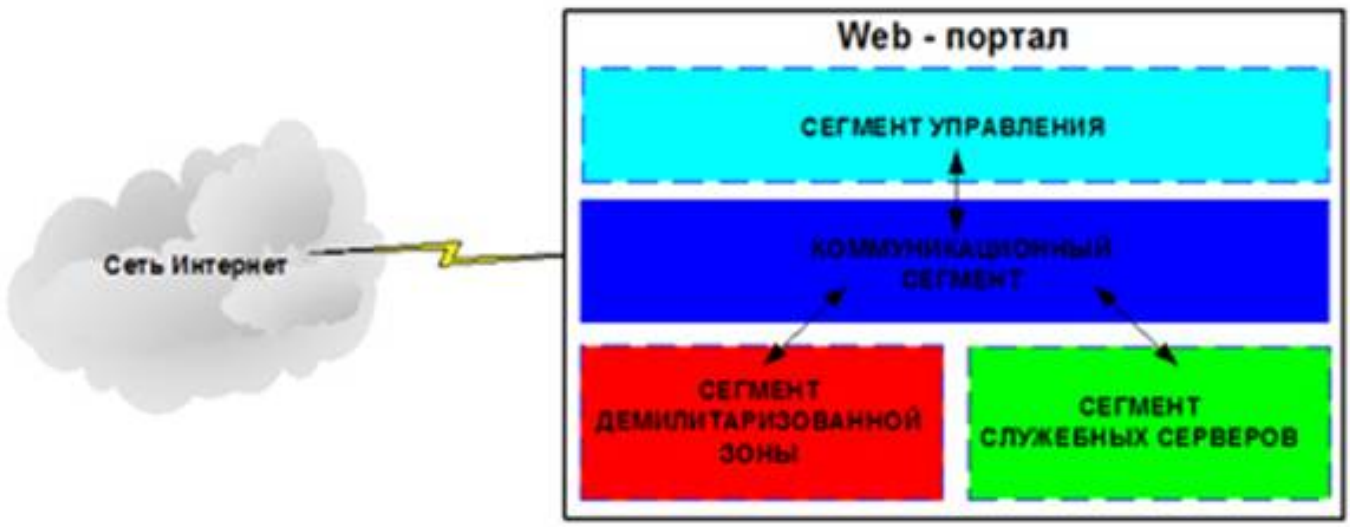

Рисунок 2. Структура защищённого Web-портала

Разделение на отдельные сегменты позволяет изолировать различные ресурсы Web-портала друг от друга. В этом случае при компрометации сервера одного из сегментов портала нарушитель не сможет получит доступ к информационным ресурсам, расположенным в других сегментах.

Разграничение доступа реализуется подсистемой на трёх уровнях стека TCP/IP – канальном, сетевом и прикладном. На канальном уровне разграничение доступа осуществляется на основе виртуальных локальных сетей VLAN (Virtual Local Area Network), на которые разделяется Web-портал. Деление на такие виртуальные сети производится при помощи настроек коммутаторов, в которых каждый физический порт включается в определённую виртуальную сеть. Хосты могут свободно обмениваться данными друг с другом в рамках одной виртуальной сети, а управление взаимодействием между различными виртуальными сетями осуществляется посредством списков контроля доступа ACL (Access Control List). В этих списках определяются правила, в соответствии с которыми разрешается или запрещается информационный обмен между разными сетями VLAN. Так, например, если для работы Web-портала два публичных Web-сервера не должны обмениваться между собой информацией, то они разделяются на разные виртуальные сети, между которыми запрещается взаимодействие. В случае, если нарушитель «взломает» один из публичных серверов Web-портала ему не удастся получить доступ к тем ресурсам, которые хранятся на других серверах, включённых в другие виртуальные сети.

На сетевом уровне разграничение доступа проводится при помощи двух межсетевых экранов (МЭ), обеспечивающие фильтрацию пакетов данных в соответствии с заданными критериями. Примеры критериев фильтрации, определённых на различных уровнях стека протоколов TCP/IP, приведены в табл. 1.

Таблица 1.

Примеры критериев фильтрования пакетов данных на различных уровнях стека TCP/IP

Уровень стека протоколов	**Примеры критериев фильтрации**
Сетевой уровень	• IP-адреса получателя и отправителя IP-дейтаграммы; • тип протокола, при помощи которого сформирован блок данных, размещённый в поле данных IP-дейтаграммы; • длина IP- дейтаграммы; • тип пакета данных ICMP и др.
Транспортный уровень	• номера TCP- и UDP-портов отправителя и получателя TCP-сегмента или UDP-дейтаграммы; • значение флагового поля передачи TCP-сегментов; • длина TCP-сегмента; • порядковые номера TCP-сегментов и др.
Уровень приложения	• длина заголовка блока данных прикладного уровня; • тип команды, содержащейся в блоке данных прикладного уровня; • адрес ресурса, которому предназначена команда, содержащаяся в блоке данных прикладного уровня и др.

Первый межсетевой экран устанавливается в точке сопряжения Web-портала с сетью Интернет и выполняет фильтрацию пакетов данных, поступающих из сети Интернет в сегмент демилитаризованной зоны. Фильтрация осуществляется на основе критерий сетевого, транспортного и прикладного уровня стека TCP/IP. Второй МЕЖСЕТЕВОЙ ЭКРАН устанавливается таким образом, чтобы через него проходили все пакеты, которыми обмениваются серверы сегмента демилитаризованной зоны и сегмента служебных серверов. Этот межсетевой экран выполняет фильтрацию только на сетевом и транспортном уровнях. Схематично установка межсетевого экрана в коммуникационном сегменте Web-портала показана на рис. 3.

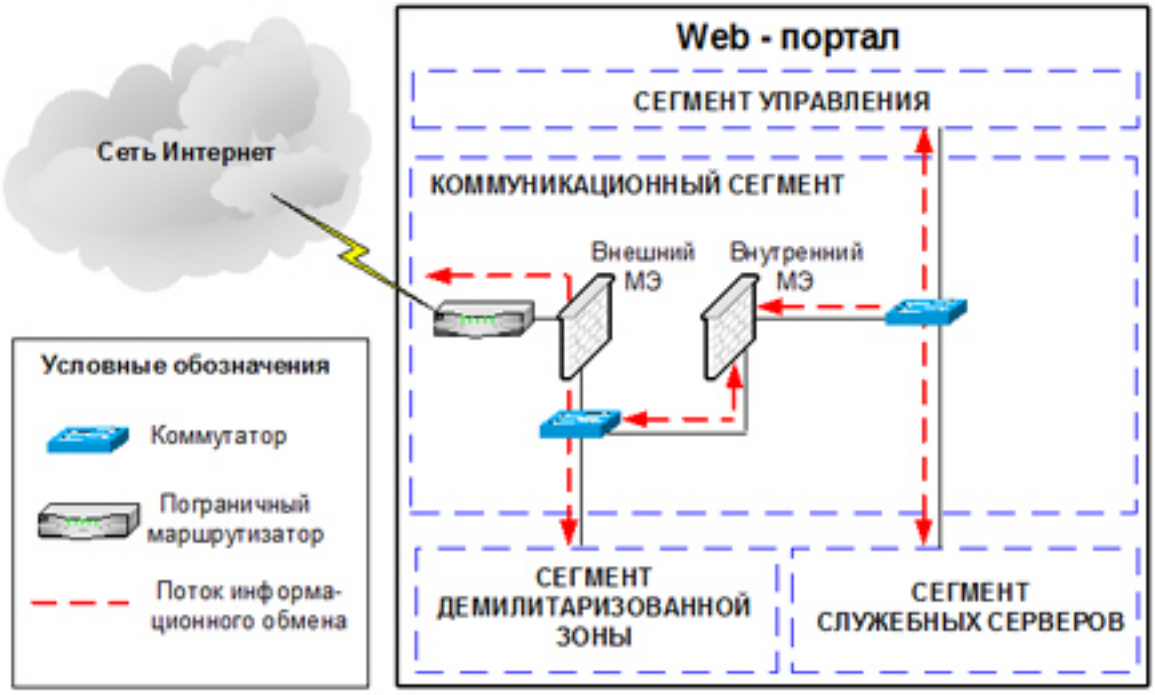

Рисунок 3. Схема установки межсетевых экранов в Web-портале

Второй межсетевой экран дублирует функции защиты на тот случай, если нарушитель сможет взломать внешний экран. Надо сказать, что потенциальная уязвимость атакам внешнего межсетевого экрана обусловлена тем, что он выполняет сложную фильтрацию пакетов данных на прикладном уровне при помощи программных модулей, которые могут содержать ошибки. Примером здесь могут служить ошибки, недавно выявленные в модулях межсетевого экрана “CheckPoint АЦ-1” содержащих уязвимость типа «переполнение буфера» (http://www.us-cert.gov/cas/techalerts/TA04-036A.html). Используя эту уязвимость нарушители могли получить полный контроль над межсетевым экраном и использовать его для развития атаки на сервера Web-портала. Однако с учётом того, что внутренний межсетевой экран выполняет лишь базовую фильтрацию на сетевом и транспортном уровне, он не может быть уязвим в отношении тех атак, которые используют уязвимости модулей, занятых обработкой пакетов данных на прикладном уровне.

Внешний межсетевой экран также выполняет защиту от атак типа «отказ в обслуживании» (denial of service), которые реализуются путём формирования большого числа запросов на установление сетевых соединений с публичными Web-серверами. В результате проведения атаки Web-сервера не справляются с обработкой всех запросов, что приводит к выходу из строя всего Web-портала. Защита от такого рода атак обеспечивается путём ограничения максимального количества входящих TCP-соединений, которые могут быть установлены с одного IP-адреса. В этом случае межсетевой экран будет блокировать все попытки установить сетевые соединения, количество которых превышает заданное ограничение, обеспечивая тем самым защиту Web-серверов от перегрузки их вычислительных ресурсов.

Разграничение доступа на прикладном уровне реализуется средствами прикладного программного обеспечения, установленного на серверах Web-портала. Это ПО должно обеспечивать идентификацию и аутентификацию администратора и некоторых пользователей портала и назначать им соответствующие права доступа к файловым ресурсам. Аутентификация может обеспечиваться на основе паролей или цифровых сертификатов.

Подсистема антивирусной защиты

Подсистема антивирусной защиты должна обеспечивать выявление и удаление информационных вирусов, которые могут присутствовать в ресурсах Web-портала.

Подсистема состоит из двух компонентов – модулей-датчиков, предназначенных для обнаружения вирусов и модуля управления антивирусными датчиками. Сами датчики устанавливаются на все серверы Web-портала, а также на АРМ администратора портала. При такой схеме установки датчиков создаются условия для проведения периодической проверки файлов портала на предмет наличия вирусов или программ типа «Троянский конь». Для того, чтобы подсистема антивирусной защиты могла эффективно выявлять и новые типы вирусов необходимо регулярно обновлять базу данных сигнатур подсистемы.

Подсистема контроля целостности

Подсистема контроля целостности должна обеспечивать выявление несанкционированного искажения содержимого Web-портала. Датчики этой подсистемы, как правило, устанавливаются на серверах портала для того, чтобы с заданной периодичностью проверять целостность файловых ресурсов портала на основе контрольных сумм или хэшей. При этом должен обеспечиваться контроль целостности файлов не только прикладного, но и общесистемного ПО. Алгоритм работы этой подсистемы выглядит следующим образом. Для заданного множества файлов подсистема вычисляет эталонные контрольные суммы. По истечению определённого временного интервала подсистема заново вычисляет контрольные суммы файлов и сравнивает их с ранее сохранёнными эталонными значения. При выявлении несоответствия между эталонным и полученным значением фиксируется факт искажения файлового ресурса, о чём немедленно оповещается администратор безопасности.

Подсистема контроля целостности не является превентивным средством защиты, поскольку позволяет выявить лишь последствия информационного вторжения. Однако наличие такой подсистемы по существу жизненно необходимо, поскольку если все имеющиеся средства защиты пропустили информационную атаку, то подсистема контроля целостности позволяет выявить её последствия.

Подсистема обнаружения вторжений

Подсистема обнаружения вторжений предназначена для выявления сетевых атак, направленных на информационные ресурсы портала. Подсистема включает в себя следующие компоненты:

· модули-датчики, предназначенные для сбора информации о пакетах данных, циркулирующих в Web-портале;

· модуль выявления атак, выполняющий обработку данных, собранных датчиками, с целью обнаружения информационных атак нарушителя;

· модуль реагирования на обнаруженные атаки;

· модуль хранения данных, в котором хранится вся конфигурационная информация, а также результаты работы подсистемы обнаружения вторжений. Таким модулем, как правило, является стандартная СУБД, например MS SQL Server, Oracle или IBM DB2;

· модуль управления компонентами средств обнаружения атак.

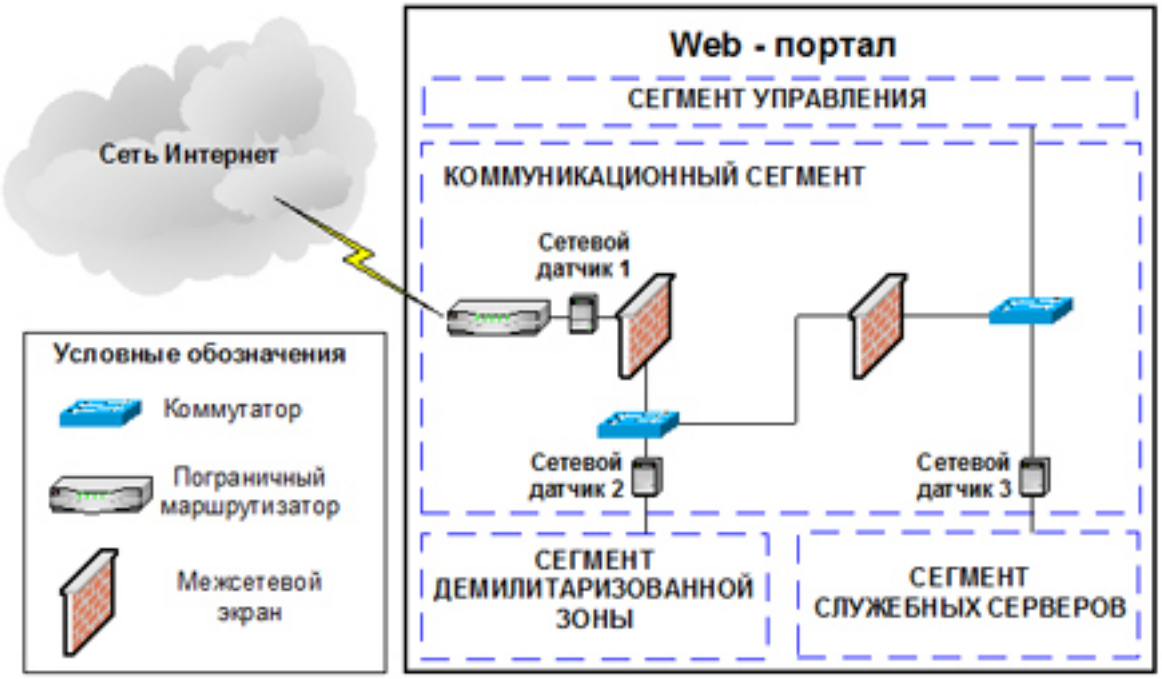

Рисунок 4. Схема установки сетевых датчиков подсистемы обнаружения вторжений в Web-портале

Первый сетевой датчик подсистемы обнаружения вторжений (рис. 4) устанавливается до внешнего межсетевого экрана и предназначен для выявления всех внешних атак на серверы портала, а также на межсетевой экран. Второй сетевой датчик устанавливается таким образом, чтобы он имел возможность перехватывать весь сетевой трафик, поступающий в сегмент демилитаризованной зоны. Таким образом, второй датчик имеет возможность выявлять атаки на публичные и кэш-серверы, которые были пропущены внешним межсетевым экраном. Анализ результатов работы первого и второго сетевого датчика позволяет контролировать работу внешнего межсетевого экрана и при необходимости изменять его правила фильтрации. Третий датчик предназначается для мониторинга сетевой активности в сегменте служебных серверов Web-портала.

Хостовые датчики подсистемы обнаружения вторжений устанавливаются на всех серверах сегмента демилитаризованной зоны и сегмента служебных серверов.Датчики этого типа должны быть реализованы в виде активных фильтров, функционирующих на уровне прикладного программного обеспечения Web-портала. Это необходимо для того, чтобы датчики не снижали производительности работы серверов портала, а также имели возможность обрабатывать трафик, передаваемый по криптозащищённым каналам связи.

Информация, собранная сетевыми и хостовыми датчиками, анализируется модулем выявления атак с целью обнаружения возможных вторжений нарушителей. Анализ данных может проводиться при помощи двух основных групп методов – сигнатурных и поведенческих. Сигнатурные методы описывают каждую атаку в виде специальной модели или сигнатуры. В качестве сигнатуры атаки могут выступать: строка символов, семантическое выражение на специальном языке, формальная математическая модель др. Алгоритм работы сигнатурного метода заключается в поиске сигнатур атак в исходных данных, собранных сетевыми и хостовыми датчиками. В случае обнаружения искомой сигнатуры, фиксируется факт информационной атаки, которая соответствует найденной сигнатуре. База данных сигнатур атак подсистемы обнаружения вторжений должна обновляться на регулярной основе.

Поведенческие методы, в отличие от сигнатурных, базируются не на моделях информационных атак, а на моделях штатного процесса функционирования Web-портала. Принцип работы поведенческих методов заключается в обнаружении несоответствия между текущим режимом функционирования АС и моделью штатного режима работы, заложенной в

параметрах метода. Любое такое несоответствие рассматривается как информационная атака. Как правило, модуль выявления атак интегрируется вместе с сетевыми и хостовыми датчиками подсистемы обнаружения вторжений.

Подсистема анализа защищённости

Подсистема анализа защищённости предназначена для выявления уязвимостей в программно-аппаратном обеспечении Web-портала. Примерами таких уязвимостей могут являться неправильная конфигурация сетевых служб портала, наличие программного обеспечения без установленных модулей обновления (service packs, patches, hotfixes), использование неустойчивых к угадыванию паролей и др. По результатам работы подсистемы анализа защищённости формируется отчёт, содержащий информацию о выявленных уязвимостях и рекомендации по их устранению. Своевременное устранение уязвимостей, выявленных при помощи этой подсистемы позволяет предотвратить возможные информационные атаки, основанные на этих уязвимостях. Сканирование Web-портала должно осуществляться по регламенту с заданной периодичностью. При этом должна регулярно обновляться база данных проверок уязвимостей. Подсистема анализа защищённости устанавливается на АРМ администратора безопасности в сегменте управления Web-портала.

Подсистема криптографической защиты

Подсистема криптографической защиты предназначена для обеспечения защищённого удалённого взаимодействия с Web-порталом. Подсистема базируется на технологии виртуальных частных сетей VPN (Virtual Private Network), которая позволяет создавать защищённые сетевые соединения, в рамках которых проводится аутентификация пользователей, а также обеспечивается конфиденциальность и контроль целостности передаваемых данных. Установка, управление и закрытие таких соединений осуществляется при помощи специализированных криптоpотоколов. Для организации VPN-сети могут использоваться разные типы криптопротоколов, функционирующие на различных уровнях стека TCP/IP (табл.2).

Таблица 2.

Криптопротоколы различных уровней стека TCP/IP

Наименование уровня стека TCP/IP	**Наименование криптопротокола**
Прикладной уровень	• SSL (Secure Sockets Layer) / TLS (Transport Layer Security) • Secure HTTP
Сетевой уровень	• IPSec (Internet Protocol Security) • SKIP (Secure Key Interchange Protocol)
Канальный уровень	• PPTP (Point-to-Point Tunneling Protocol) • L2F (Layer 2 Forwarding Protocol) • L2TP (Layer 2 Tunneling Protocol)

В состав подсистемы криптографической защиты информации входит VPN-шлюз, который устанавливается в Web-портале и VPN-клиенты, устанавливаемые на рабочие станции администраторов Web-портала, а также на станции тех пользователей, для которых необходимо обеспечить защищённое взаимодействие с серверами портала. VPN-шлюз устанавливается в коммуникационном сегменте портала между внешним и внутренним межсетевым экраном. Такая схема установки позволят использовать внутренний экран для фильтрации пакетов данных уже после того, как они будут расшифрованы VPN-шлюзом. В случае, если для организации VPN-сети используется протокол SSL, то на стороне пользователей Web-портала можно не устанавливать дополнительного ПО и использовать стандартные Интернет-браузеры, в которые интегрированы функции SSL-клиента.

Подсистема управления средствами защиты Web-портала

Подсистема управления средствами защиты размещается в одноимённом сегменте Web-портала. Подсистема включает в себя АРМ администратора безопасности, с которого осуществляется управление, а также служебные серверы, необходимые для функционирования соответствующих средств защиты. Подсистема также дополнительно может включать в себя модуль корреляции событий, зарегистрированных различными подсистемами защиты портала. Наличие такого модуля позволяет автоматизировать обработку большого объёма информации, регистрируемой в Web-портале, и в соответствии с заданным набором правил выделить наиболее критические события, которые требуют немедленного реагирования.

Архитектура защищённого Web-портала, в котором установлены все рассмотренные выше подсистемы защиты, изображена на рис. 5.

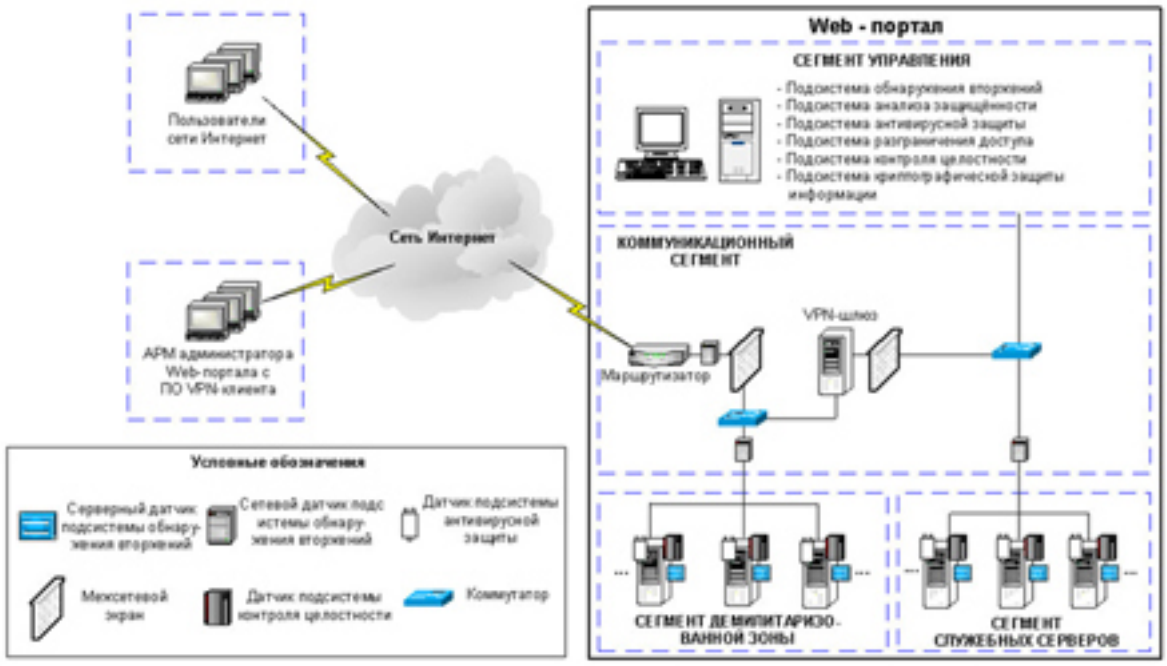

Рисунок 5. Архитектура защищённого Web-портала

Для повышения надёжности работы портала наиболее критические элементы комплекса средств безопасности, такие как межсетевой экран и VPN-шлюз должны резервироваться путём создания отказоустойчивых кластеров. В этом случае их сбой или отказ не приведёт к нарушению работоспособности всего Web-портала.

Поскольку комплекс средств защиты Web-портала сам может выступать в качестве цели возможной атаки, то все его подсистемы должны быть оснащены механизмами собственной безопасности, которые бы позволяли выполнять следующие функции:

• обеспечение конфиденциальности и контроля целостности информации, передаваемой между компонентами подсистем по каналам связи;

• обеспечения взаимной аутентификации компонентов подсистем перед обменом информацией;

• обеспечения контроля целостности собственного программного обеспечения подсистем на основе контрольных сумм;

• аутентификации администратора безопасности при доступе к консоли управления подсистем на основе пароля. При этом должна регистрироваться информация обо всех

успешных и неуспешных попытках аутентификации администратора.

Заключение

В настоящее время нормальное функционирование Web-портала, подключённого к сети Интернет, практически невозможно если не уделять должное внимание проблеме обеспечения его информационной безопасности. Наиболее эффективно эта проблема может быть решена путём применения комплексного подхода к защите ресурсов портала от возможных информационных атак. Для этого в состав комплекса средств защиты портала должны входить подсистемы антивирусной защиты, обнаружения вторжений, контроля целостности, криптографической защиты, разграничения доступа, а также подсистема управления. При этом каждая из подсистем должна быть оснащена элементами собственной безопасности.

Список литературы:

1. Лукацкий А. Обнаружение атак. – СПб.: БХВ-Петербург, 2001.

2. Рыбин Алексей. Корпоративный сайт. Эффективный инструмент бизнеса или нереализованные возможности. Бюллетень JetInfo № 4 (119), 2003.

3. Сердюк В.А. Ахиллесова пята информационных систем //BYTE/Россия. 2004. №4 (68). С. 19–22.

4. Pierre-Alain Fayolle, Vincent Glaume, A buffer overflow Study. Attacks and Defenses , ENSEIRM, 2002.