А. В. Архангельская, А. А. Шернюкова

РАЗРАБОТКА МОДЕЛИ ОДНОНАПРАВЛЕННОГО ШЛЮЗА[1]

Для соединения открытых сетей с внутренней сетью, в которой обрабатывается информация с ограниченным доступом, необходимо использовать технологию, способную обеспечить гарантированную однонаправленную передачу данных из открытой сети во внутреннюю сеть. В случае обработки сведений, составляющих государственную тайну, либо при работе с информацией, обладателями которой являются государственные органы и которая содержит служебную тайну, должны применяться только сертифицированные средства защиты информации [1]. В настоящее время представлено относительно небольшое количество решений, удовлетворяющих данным требованиям, одним из которых является однонаправленный шлюз, который мог бы обеспечить изолированность защищаемой информации от доступа извне. Подобные устройства существуют [2–11] и достаточно широко применяются, но анализ показал, что ни в одном из них не предусмотрена гарантированная передача данных, что существенно затрудняет их применение при решении практических задач. Разработка модели однонаправленного шлюза, позволяющего осуществлять передачу данных с подтверждением и способного пройти процесс сертификации, поможет решить одну из важных задач в области информационной безопасности — обеспечить защиту информации от доступа извне.

Рассмотрим однонаправленный шлюз, который, как правило, состоит из двух логических компонентов – компьютеров, размещенных в одном корпусе (Рис. 1). Внешний компонент (А) обеспечивает полноценное соединение с внешней сетью, а внутренний (В) — с внутренней сетью, причем между компонентами А и В существует строго однонаправленная связь и данные с компонента В не могут быть переданы на компонент А.

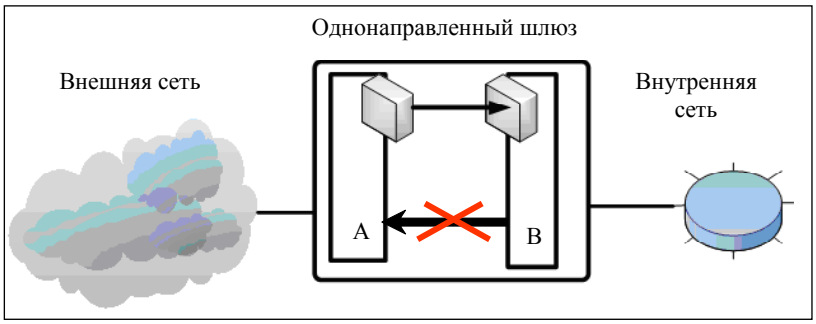

Рис. 1. Общая схема однонаправленного шлюза

[1] Статья написана в рамках НИР «Обеспечение безопасности информации в открытых распределенных вычислительных системах», заданной Государственным контрактом № П2397 в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 годы.

При применении однонаправленных шлюзов были выявлены следующие каналы утечки информации:

· утечка информации через технический канал;

· сетевые атаки;

· изменение программной схемы шлюза;

· занесение вирусов во внутреннюю сеть, вызывающее нарушение целостности/доступности информации;

· утечка информации через стеганографический канал передачи данных;

· доступ к информации, хранящейся на шлюзе, лица, не имеющего допуска к информации данного уровня секретности, или в случае, когда работа с данной информацией не является необходимой для исполнения его должностных обязанностей;

· человеческий фактор.

С использованием обнаруженных каналов утечки информации, действующей нормативной базы [12–15] и с учетом проведенного анализа существующих устройств однонаправленной передачи данных был составлен перечень требований, предъявляемых к однонаправленным шлюзам. В однонаправленном шлюзе необходимо наличие:

· функций аудита безопасности;

· контроля целостности программной схемы устройства;

· криптографических функций;

· безопасного импорта данных из внешней сети;

· обеспечение целостности хранимых данных;

· идентификация и аутентификация пользователей;

· функции, обеспечивающие приватность.

Аудит безопасности включает в себя распознавание, запись, хранение и анализ информации, связанной с действиями, относящимися к безопасности. Записи, получаемые в результате аудита, должны быть проанализированы для определения, какие действия, относящиеся к безопасности, происходили и кто из пользователей несет за них ответственность. Из этого класса функций необходимо реализовать следующие:

· реакция на обнаружение событий, указывающих на возможное нарушение безопасности;

· анализ аудита безопасности, использующегося для обнаружения атак и автоматической реакции на ожидаемое нарушение безопасности;

· просмотр аудита, предоставляемого администратору сети;

· создание журнала аудита безопасности с защитой от несанкционированного доступа, от потери данных при переполнении журнала, обеспечивающего гарантированную доступность данных.

Для корректной работы однонаправленного шлюза необходим контроль целостности программной схемы устройства, который может быть реализован как программно, так и аппаратно. Поскольку в работе предлагается построение однонаправленного шлюза с помощью программируемых логических интегральных схем (ПЛИС), необходим контроль физического доступа к устройству и обязательно использование специальных защитных знаков.

Для защиты обрабатываемой информации необходим набор функций, обеспечивающих безопасность данных пользователя, а именно:

· безопасный импорт данных из внешней сети;

· обеспечение целостности хранимых данных.

Функции, обеспечивающие анонимность пользователей в системе (например, невозможность узнать о действиях, выполняемых другими пользователями), псевдонимность (например, возможность использования сервиса или услуги без раскрытия своего идентификатора с

сохранением ответственности за выполненные действия), скрытность (например, невозможность для других пользователей определить, кто использовал какой-либо сервис или услугу), образуют класс, именуемый «приватность».

С учетом обнаруженных каналов утечки информации и рассмотренных способов их устранения предложена аппаратная реализация однонаправленного шлюза (Рис. 2). Для обеспечения гарантированной однонаправленной передачи данных предлагается выделение общей памяти ограниченного размера, доступ к которой должны иметь одновременно и внешний (на чтение и запись), и внутренний (на запись) компоненты через устройства передачи данных, выполненные на ПЛИС.

К устройствам передачи данных присоединяются внешний и внутренний буферы данных, предназначенных для передачи на внутренний компонент шлюза и полученных с внешнего компонента соответственно. Поскольку ПЛИС являются доверенным устройством передачи данных, предложенный однонаправленный шлюз позволяет организовать обратный канал передачи данных для обеспечения гарантированной доставки. За счет использования буферов эта модель предусматривает отслеживание создания единственно возможного скрытого канала передачи данных в системе.

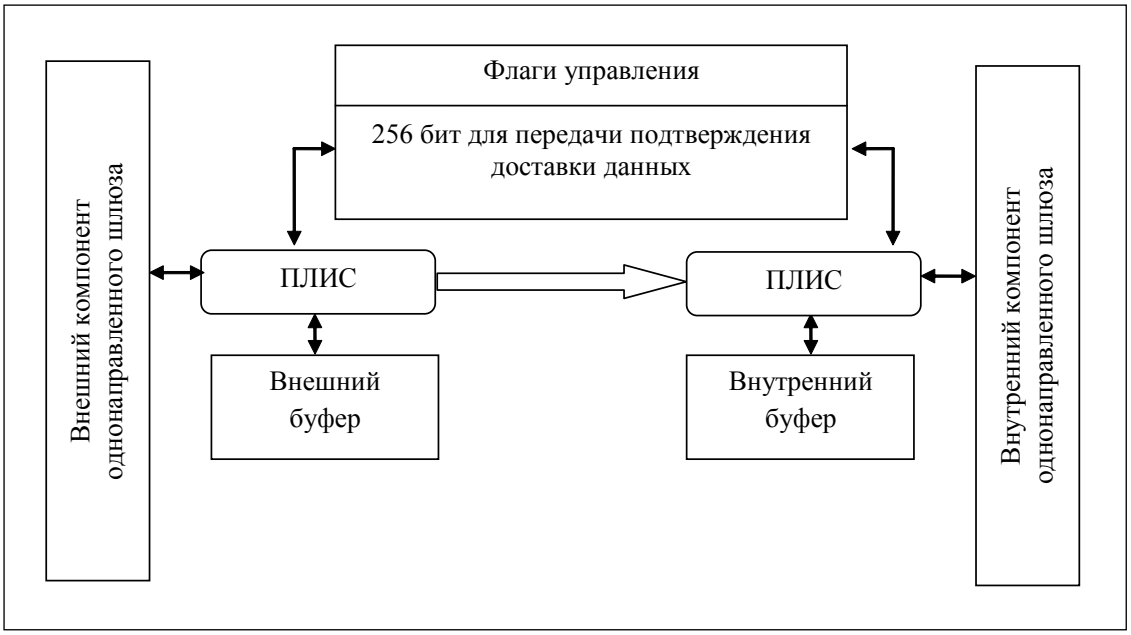

Рис. 2. Аппаратная реализация однонаправленного шлюза

Предложенная модель однонаправленного шлюза может использовать стандартный стек протоколов TCP/IP, но для усовершенствования устройства был создан протокол однонаправленной передачи данных с подтверждением, построенный с учетом аппаратных особенностей разработанной модели.

При доставке сообщения в буфер внутреннего компонента ПЛИС внутренний компонент прописывает в общей памяти информацию о получении некоторых пакетов. ПЛИС внешнего компонента, получив информацию о доставке, отправляет следующий набор пакетов. Для каждого передаваемого блока данных предполагается динамическое выделение памяти, поэтому в заголовке используемого протокола необходимо указывать объем передаваемого сообщения. После определения этого параметра ПЛИС на стороне внутреннего компонента выделяет необходимый объем памяти из расчета 1 бит на каждый отдельный пакет плюс 3 бита для служебных полей. Каждый бит устанавливается в 0 или 1 в зависимости от того, был ли получен или не получен

соответствующий пакет. В начале работы каждый бит имеет значение 1, что соответствует отсутствию пакета. После получения пакета соответствующий бит меняется на 0. Внешний компонент проверяет общий блок памяти на наличие битов с установленной единицей. Пакет с номером, соответствующим установленной единице, отправляется повторно. Объем общего блока памяти предполагается сделать равным 256 бит плюс 3 бита для служебных полей.

Таким образом, ПЛИС внутреннего компонента может записывать данные в участок общей памяти, а ПЛИС внешнего компонента – производить чтение и запись данных в этот компонент. Передача данных с внешнего компонента начинается со считывания одного из флагов управления из общего блока памяти и осуществляется путем отправки запроса на передачу данных, содержащего преамбулу, порт отправителя, количество ожидаемых пакетов и контрольную сумму.

Если внутренний компонент готов принимать данные, он выделяет необходимый объем памяти, выставляет флаг подтверждения передачи в единицу и ждет первого пакета с данными. По окончании передачи внешний компонент посылает запрос на прекращение соединения, состоящий из специального набора бит, сигнализирующего об окончании передачи информации.

Принципиальная схема работы протокола передачи данных с подтверждением приведена на рис. 3.

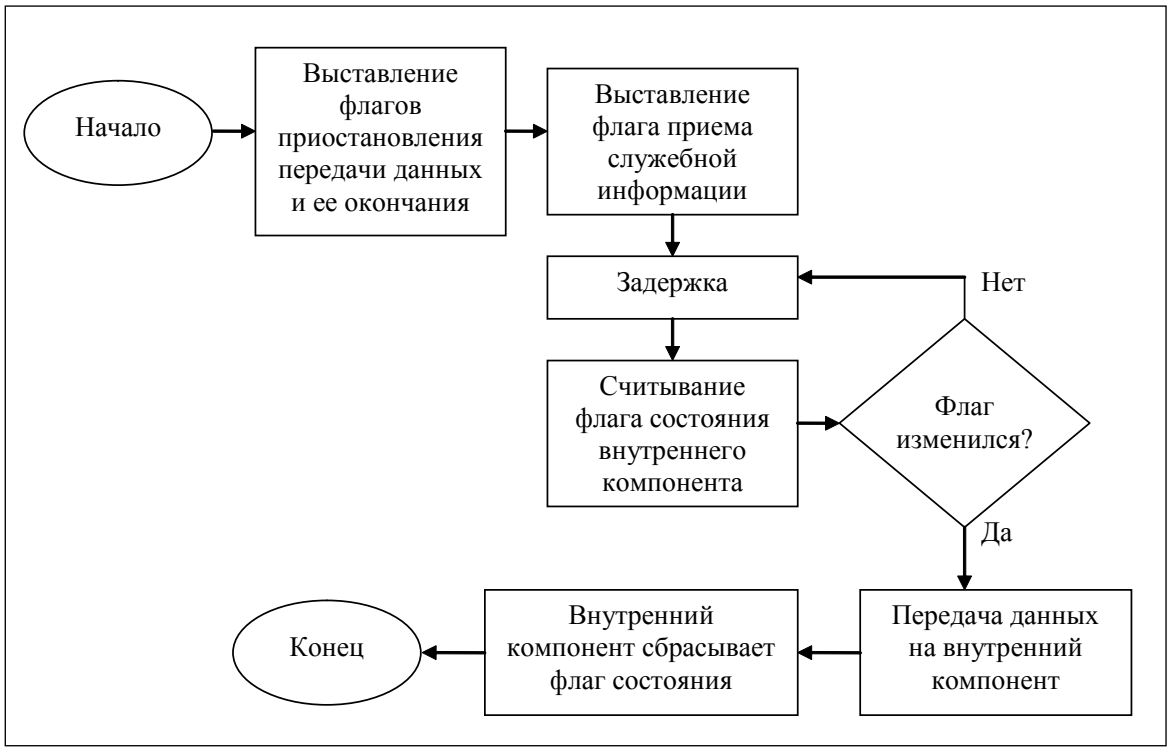

Рис. 3. Схема протокола однонаправленной передачи данных с подтверждением

Разработанный протокол обладает следующими преимуществами:

· возможность отправки пакетов напрямую, используя дополнительно только физический уровень;

· передача данных до тех пор, пока не будет получено подтверждение о доставке или завершена передача из-за отсутствия соединения приемлемого качества;

· разбиение данных на отдельные пакеты;

· простота реализации;

· наличие минимального управления потоком информации с помощью флагов приостановления и возобновления передачи данных;

· маленький объем служебной информации в передаваемых пакетах;

· получение подтверждения доставки данных только в случае правильной контрольной суммы;

· выполнение условия строго однонаправленной передачи;

· шифрование при передаче информации с внешнего компонента на внутренний;

· высокая скорость передачи информации.

К недостаткам данного протокола можно отнести:

· управление потоком происходит на низком уровне — не предусмотрено влияние внутреннего компонента на процесс передачи данных, за исключением задержек и уменьшения скорости;

· нет разделения каналов, т. е. данные передаются исключительно на один заранее заданный порт внутреннего компонента;

· отсутствуют дополнительные опции, т. е. протокол на данный момент обладает только базовым набором функций;

· не реализованы различные механизмы управления перегрузкой;

· доступен единственный способ подтверждения получения данных;

· не разделяются причины сбоя в приеме информации.

В ходе выполнения данной работы были получены следующие основные результаты:

· проанализированы известные подходы к разработке однонаправленного шлюза для передачи данных;

· выявлены возможные каналы утечки информации при использовании однонаправленных шлюзов и предложен ряд способов устранения утечки по указанным каналам;

· разработаны набор требований, которым должны удовлетворять однонаправленные шлюзы, и профиль защиты для однонаправленных шлюзов;

· разработан, проанализирован и реализован протокол однонаправленной передачи данных с подтверждением.

Результаты настоящей работы можно использовать при разработке аналогичных протоколов однонаправленной передачи данных с подтверждением, выполняющихся в различных системах. Проведенные исследования дают возможность выделить общие требования к подобным протоколам, а разработанный протокол позволяет реализовать строго однонаправленную передачу данных с возможностью подтверждения их получения.

Приведенные результаты могут быть использованы при разработке однонаправленных шлюзов, при проведении исследований по обеспечению однонаправленной передачи данных с подтверждением, по определению эффективных способов обеспечения информационной безопасности при работе с ресурсами сети Интернет с точки зрения защиты информации от доступа извне, а также при разработке требований к устройствам защиты информации.

Изложенные результаты получены в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009—2013 годы.

СПИСОК ЛИТЕРАТУРЫ:

1. Указ Президента РФ от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

2. *Стивенс М.* Применение оптического диода данных. 1996. URL: http://dspace.dsto.defence.gov.au/dspace/bitstream/1947/4386/1/DSTO-TR-0785.pdf.

3. KVM-коммутатор для управления серверами защищенной сети. URL: http://www.energoportal.ru/article287.htm.

4. Разработка компании «ЛИССИ». М., 2008. URL: http://www.lissi.ru/news/153.

5. Однонаправленный шлюз, разработанный ФГУП «Научно-технический центр «Атлас». URL: http://www.infoforum.ru/10_apr_2008/3_Atlas_Presentation.ppt.
6. Официальная документация компании Tenix America по системе Tenix One-Way File Transfer. URL: http://www.tenixamerica.com/images/white_papers/datasheet_fta.pdf.
7. Официальная документация компании Tenix America по системе Tenix One-Way Data Transfer. URL: http://www.tenixamerica.com/images/white_papers/datasheet_dfa.pdf.
8. Детализированное описание системы Secure File/Directory Transfer System DFTS. URL: http://www.owlcti.com/products/dfts.html.
9. Принцип работы технологии DualDiode. URL: http://www.owlcti.com/products/how-dual-diode-works.html.
10. Техническая документация к разработке компании Trusted Computer Solution. URL: http://www.trustedcs.com/documents/TrustedGatewayTechnicalAbstract.pdf.
11. Общее описание системы, разработанной компанией Trusted Computer Solution. URL: http://www.trustedcs.com/documents/SOTrustedGatewaySolarisFS.pdf.
12. ГОСТ 15408 – 1 – 2002. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 1. Введен 2002–04–04. М., Госстандарт России, 2002. – 35 с.
13. ГОСТ 15408 – 2 – 2002. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 2. Введен 2002–04–04. М., Госстандарт России, 2002. – 159 с.
14. ГОСТ 15408 – 3 – 2002. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 3. Введен 2002–04–04. М., Госстандарт России, 2002. – 107 с.
15. Руководящий документ Государственной технической комиссии при Президенте РФ от 25 июля 1997 г. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации.