УДК 004.056:621.39

АППАРАТНО-ПРОГРАММНЫЙ ШЛЮЗ С АППАРАТНОЙ ИЗОЛЯЦИЕЙ КАНАЛОВ

Бабич Н.В[1]., курсант гр. 233701

Белорусский государственный университет информатики и радиоэлектроники[1]
г. Минск, Республика Беларусь

Дудак М.Н.

Аннотация. В статье рассматриваются вопросы разработки аппаратно-программного шлюза с аппаратной изоляцией каналов для применения в специальных инфокоммуникационных системах. Актуальность темы определяется необходимостью обеспечения защищенного обмена данными между сегментами сети с различной степенью доверия в интересах войск связи Вооруженных Сил Республики Беларусь. Особое внимание уделяется аппаратному разграничению каналов как способу исключения несанкционированного обратного информационного воздействия и повышения устойчивости функционирования системы в условиях повышенных требований к безопасности. Показано, что использование подобных решений позволяет повысить надежность сопряжения изолированных контуров связи и обеспечить контролируемую передачу служебной информации.

Ключевые слова. Аппаратно-программный шлюз, аппаратная изоляция каналов, однонаправленная передача данных, data diode, защищенный обмен данными, межсегментное взаимодействие, уровень доверия, изолированные контуры, инфокоммуникационные системы, сети специального назначения, исключение обратного канала, физическая изоляция, контроль целостности данных, защита информации, журналирование событий.

Современный этап развития инфокоммуникационных систем характеризуется постоянным ростом требований к защищенности межсегментного обмена данными. Для войск связи Вооруженных Сил Республики Беларусь данная задача имеет прикладное значение, поскольку в специальных системах связи и автоматизации нередко требуется организовать передачу служебной, технологической или телеметрической информации между сегментами сети с различным уровнем доверия. При этом принципиально важно исключить возможность обратного информационного воздействия со стороны менее доверенного сегмента. В подобных условиях традиционные программные средства разграничения доступа, включая межсетевые экраны и маршрутизирующие устройства с фильтрацией трафика, не всегда обеспечивают требуемый уровень гарантированности, так как сохраняют саму физическую возможность двустороннего обмена. Поэтому актуальной научно-технической задачей является разработка аппаратно-программного шлюза с аппаратной изоляцией каналов [1].

В научной литературе для описания подобных решений применяются термины data diode, unidirectional gateway, однонаправленная передача данных. При этом следует различать собственно аппаратную однонаправленную передачу и более сложные программно-аппаратные шлюзовые комплексы. В работе X. Okhravi и F. Sheldon показано, что data diode реализует физический механизм передачи данных только в одном направлении, тем самым устраняя возможность удаленного сетевого воздействия на защищаемый сегмент через канал связи. В более современных обзорах отмечается, что однонаправленные решения сегодня рассматриваются как отдельный класс средств защиты для критической инфраструктуры, промышленных систем, IoT-сред и сетей с жесткими требованиями к доверенности обмена. Российские и белорусские исследователи также подчеркивают, что однонаправленные сети передачи информации являются эффективным способом организации защищенного взаимодействия между средами с различным уровнем безопасности.

Для специальных инфокоммуникационных систем военного назначения данная проблематика приобретает дополнительное значение. На практике часто возникает необходимость вывода данных из изолированного контура: журналов событий, телеметрии, диагностической информации, данных мониторинга, сведений о техническом состоянии средств связи и автоматизации. Одновременно с этим необходимо исключить обратную передачу управляющих воздействий, вредоносного кода, деструктивных пакетов и иных форм сетевого проникновения. Таким образом, задача заключается не просто в фильтрации нежелательного трафика, а в построении такого рубежа обмена, который на физическом уровне не допускает формирования обратного канала (см. рисунок 1). Именно в этом заключается принципиальное отличие аппаратной изоляции каналов от программных методов защиты. Дополнительно следует учитывать, что применение аппаратной изоляции каналов позволяет существенно снизить зависимость уровня защищенности от корректности настройки программных средств и человеческого фактора. В отличие от традиционных решений, основанных на политике фильтрации, физическое ограничение направления передачи формирует детерминированную модель взаимодействия между сегментами сети. Это особенно важно в условиях эксплуатации систем специального назначения, где недопустимы даже единичные случаи нарушения установленного режима обмена. Таким образом, использование шлюзов с аппаратной изоляцией каналов обеспечивает переход от вероятностных методов защиты к гарантированному обеспечению безопасности межсегментного взаимодействия.

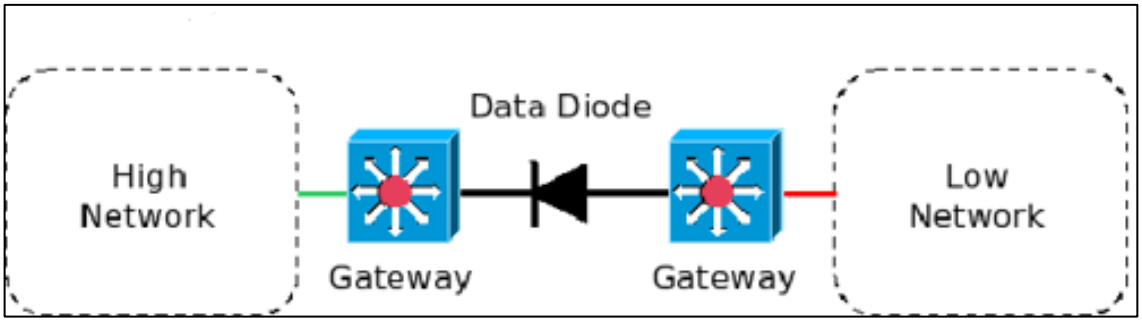

Рисунок 1 – Обобщенная схема однонаправленного шлюза между доверенным и менее доверенным сегментами

Архитектурно аппаратно-программный шлюз с аппаратной изоляцией каналов целесообразно рассматривать как совокупность трех взаимосвязанных подсистем: передающей, аппаратно-изолирующей и принимающей. Передающая подсистема размещается в доверенном сегменте и выполняет сбор, предварительное преобразование, буферизацию и подготовку данных к передаче. Аппаратно-изолирующая подсистема обеспечивает физическое ограничение направления потока. Принимающая подсистема располагается на стороне менее доверенного сегмента и реализует восстановление, верификацию, контроль целостности и предоставление данных вышестоящим приложениям. Такой подход соответствует архитектуре, описанной в работе Ю. И. Воротницкого, где аппаратно-программное средство однонаправленной передачи данных строится как совокупность модулей обмена, управления передачей и аппаратного канала с физически заданным направлением [2]. Зарубежные работы по unidirectional gateway дополнительно показывают целесообразность применения прокси-компонентов, протокольного разрыва и фильтрации содержимого.

С инженерной точки зрения аппаратная изоляция каналов может быть реализована различными способами, однако наиболее типичным является использование оптического однонаправленного тракта, в котором физически отсутствует обратный передатчик. В этом случае доверенная сторона имеет только передающий модуль, а принимающая сторона — только приемный модуль. Подобная схема обеспечивает аппаратно детерминированную однонаправленность передачи, то есть делает невозможным формирование стандартного сетевого сеанса в обратном направлении [3]. Однако физической однонаправленности самой по себе недостаточно. Для практического применения в составе инфокоммуникационной системы необходим программный уровень, который обеспечивает устойчивую доставку данных, последовательность кадров, контроль целостности, подтверждение корректности на локальном уровне и адаптацию пользовательских протоколов к однонаправленному режиму. Именно поэтому в современных однонаправленных шлюзах аппаратная защита дополняется программными модулями проксирования и реконструкции сервисов.

Для применения в войсках связи особенно важным является вопрос функционального назначения такого шлюза. Наиболее реалистичными сценариями являются: передача данных мониторинга из изолированного сегмента сети связи в сегмент централизованного наблюдения; вывод эксплуатационной информации о состоянии аппаратуры связи; передача журналов регистрации событий безопасности; вывод результатов диагностики и телеметрии из защищенных подсистем на внешние аналитические рабочие места. Во всех указанных случаях критерием эффективности выступает не полнота сетевого взаимодействия, а гарантированное отсутствие обратного управляющего воздействия на исходный сегмент. Иными словами, приоритет смещается с удобства сетевой интеграции на гарантированную безопасность сопряжения. Такой подход соответствует международной практике применения data diode в критически важных и технологических системах.

Сравнение аппаратно-программного шлюза с аппаратной изоляцией каналов и классического межсетевого экрана показывает, что эти средства не являются прямыми конкурентами, а решают различные задачи. Межсетевой экран допускает двусторонний обмен и управляет им посредством правил фильтрации, контроля соединений и анализа пакетов. Его преимуществами являются гибкость, поддержка широкого спектра протоколов и относительная простота интеграции. Вместе с тем при компрометации политики безопасности, программной реализации либо управляющей плоскости сохраняется риск несанкционированного воздействия через существующий двусторонний канал. Однонаправленный шлюз, напротив, существенно ограничивает сетевую функциональность, но обеспечивает более высокий уровень гарантированности за счет физического устранения обратного пути. Поэтому в специальных системах связи он целесообразен на тех рубежах, где цена риска обратного проникновения выше, чем потери от ограничения сетевой универсальности.

Отдельного внимания заслуживает вопрос надежности передачи данных через однонаправленный канал. В классических сетевых протоколах надежность часто обеспечивается за

счет квитирования, повторной передачи и управления сеансом в обоих направлениях. В условиях аппаратной однонаправленности такая модель неприменима в прямом виде. Поэтому в исследованиях по unidirectional gateway предлагается использовать внутренние механизмы пакетирования, последовательной нумерации, локальной буферизации, коррекции ошибок, избыточного кодирования и протокольного разрыва. В практических решениях также применяются программные прокси, которые на стороне доверенного сегмента имитируют наличие обычного сервиса, а на стороне получателя восстанавливают данные в форме, пригодной для стандартных приложений. Такой подход позволяет совместить физическую безопасность однонаправленного канала с эксплуатационной пригодностью системы.

В более широком научном контексте тематика защищенного межсегментного обмена поддерживается и смежными диссертационными исследованиями в области безопасности телекоммуникационных сетей. Так, в диссертации М. М. Монаховой исследуются модели и алгоритмы контроля инцидентов информационной безопасности в корпоративной телекоммуникационной сети, а в работе А. И. Кураленко рассматриваются методы аудита информационной безопасности информационно-телекоммуникационных систем [4], [5]. Хотя эти исследования не посвящены непосредственно однонаправленным шлюзам, они подтверждают устойчивый научный интерес к средствам, повышающим доверенность сетевого взаимодействия, контролируемость каналов обмена и устойчивость телекоммуникационной инфраструктуры в условиях усложнения угроз. Для вашей темы это важно как для обоснования научной значимости, так и для демонстрации принадлежности исследования к более широкой области специальных телекоммуникаций и защиты информации.

С учетом изложенного можно предложить следующую обобщенную структуру разрабатываемого аппаратно-программного шлюза: модуль сбора и нормализации исходных данных; модуль предварительного форматирования и буферизации; аппаратный однонаправленный канал; модуль контроля целостности и последовательности; модуль восстановления прикладного представления данных; модуль журналирования и технического контроля. При необходимости в состав шлюза могут вводиться функции криптографической защиты передаваемых данных, однако криптографические механизмы не должны подменять собой аппаратную изоляцию, а должны рассматриваться как дополнительный уровень защиты. Для условий войск связи перспективным представляется построение шлюза как специализированного изделия, ориентированного не на универсальный сетевой обмен, а на ограниченный перечень строго регламентированных сервисов передачи. Это соответствует требованиям специальных систем, где преимущество от узкой функциональной специализации часто выше, чем выгода от универсальности (см. рисунок 2).

Рисунок 2 – Предлагаемая структурная схема однонаправленного шлюза

Таким образом, разработка аппаратно-программного шлюза с аппаратной изоляцией каналов является актуальным направлением развития инфокоммуникационных систем, ориентированных на применение в специальных и защищенных контурах передачи данных. Научная и практическая значимость данной темы определяется тем, что аппаратная изоляция позволяет перейти от вероятностного ограничения угроз к физически обеспечиваемому исключению обратного сетевого воздействия. Для войск связи Вооруженных Сил Республики Беларусь это создает предпосылки для построения более устойчивых и доверенных средств сопряжения изолированных сегментов связи, предназначенных для безопасной передачи служебной информации, данных мониторинга и телеметрии. В дальнейшем развитие данной тематики может быть связано с обоснованием конкретной схемотехнической реализации шлюза, выбором интерфейсов передачи, исследованием показателей пропускной способности, задержки, отказоустойчивости и оценкой его эффективности в составе специальных инфокоммуникационных систем.

Дополнительным аспектом, требующим рассмотрения при разработке аппаратно-программного шлюза с аппаратной изоляцией каналов, является обеспечение его интеграции в существующую инфраструктуру инфокоммуникационных систем. В условиях эксплуатации сетей специального назначения важно учитывать не только функциональные возможности шлюза, но и его совместимость с используемыми протоколами передачи данных, форматами представления информации и средствами управления сетью. При этом внедрение однонаправленного шлюза не должно приводить

к нарушению штатных режимов функционирования сопрягаемых сегментов, а также должно обеспечивать минимальные задержки при передаче данных в пределах допустимых значений для конкретного типа информации.

Особое значение имеет вопрос масштабируемости предлагаемого решения. В зависимости от структуры инфокоммуникационной системы и объема передаваемых данных шлюз должен поддерживать возможность расширения пропускной способности и адаптации к изменяющимся условиям эксплуатации. Это может достигаться за счет модульного построения устройства, позволяющего наращивать вычислительные и интерфейсные ресурсы без изменения базовой архитектуры. Кроме того, при проектировании необходимо учитывать требования к отказоустойчивости, включая возможность резервирования ключевых компонентов и организацию непрерывного функционирования системы в случае отказа отдельных модулей.

Не менее важным является обеспечение контроля и диагностики работы шлюза в процессе эксплуатации. Для этого в его составе целесообразно предусмотреть средства мониторинга технического состояния, регистрации событий и анализа параметров передачи данных. Наличие таких механизмов позволяет своевременно выявлять отклонения от нормального режима работы, а также повышает общую управляемость системы. При этом доступ к диагностической информации должен быть организован таким образом, чтобы не нарушать принцип однонаправленности передачи данных и не создавать дополнительных каналов потенциального воздействия.

С точки зрения практической реализации значительное внимание должно уделяться вопросам энергопотребления и конструктивного исполнения устройства. В условиях применения в составе специальных систем связи, в том числе в полевых или ограниченных по ресурсам условиях, шлюз должен обладать компактностью, энергоэффективностью и устойчивостью к внешним воздействиям. Это накладывает дополнительные требования на выбор элементной базы, схемотехнические решения и компоновку устройства.

Таким образом, комплексный учет факторов интеграции, масштабируемости, отказоустойчивости, диагностируемости и эксплуатационных характеристик позволяет обеспечить не только функциональную реализуемость аппаратно-программного шлюза с аппаратной изоляцией каналов, но и его эффективное применение в составе современных инфокоммуникационных систем специального назначения.

Список использованных источников

1. Организация однонаправленных сетей передачи информации в условиях защищённой среды / А. Г. Воронцов, С. А. Петунин // Информационная безопасность, 2017. – С. 32–38.

2. Архитектура аппаратно-программного средства однонаправленной передачи данных в компьютерных сетях / Ю. И. Воротницкий // Вестник современных технологий, 2023. – С. 45–52.

3. Data Diodes in Support of Trustworthy Cyber Infrastructure / Hossein Okhravi, Frederick T. Sheldon // Proceedings of the 6th Annual Workshop on Cyber Security and Information Intelligence Research, 2010. – P. 1–4.

4. Модели и алгоритмы контроля инцидентов информационной безопасности в корпоративной телекоммуникационной сети : дис. … канд. техн. наук / М. М. Монахова. – М., 2015. – 150 с.

5. Методика аудита информационной безопасности информационно-телекоммуникационной системы: дис. канд. техн. наук / А. И. Кураленко. – М., 2012. – 140 с.

UDC 004.056:621.39

HARDWARE-SOFTWARE GATEWAY WITH HARDWARE ISOLATION OF CHANNELS

Babich N.V.[1]

Belarusian State University of Informatics and Radioelectronics[1]*, Minsk, Republic of Belarus*

Dudak M.N.

Annotation. The article addresses the development of a hardware-software gateway with hardware-based channel isolation intended for use in specialized info communication systems. The relevance of the topic is determined by the need to ensure secure data exchange between network segments with different levels of trust in the interests of the Signal Corps of the Armed Forces of the Republic of Belarus. Particular attention is paid to hardware-based channel separation as a means of preventing unauthorized reverse information flow and enhancing system resilience under stringent security requirements. It is shown that the use of such solutions improves the reliability of interconnection between isolated network domains and ensures controlled transmission of service information.

Keywords. Hardware-software gateway, hardware-based channel isolation, unidirectional data transmission, data diode, secure data exchange, inter-segment interaction, trust level, isolated domains, info communication systems, special-purpose networks, elimination of reverse channel, physical isolation, data integrity control, information security, event logging.