http://dx.doi.org/10.35596/1729-7648-2023-21-3-96-101

Оригинальная статья
Original paper

УДК 004.056

АРХИТЕКТУРА АППАРАТНО-ПРОГРАММНОГО СРЕДСТВА ОДНОНАПРАВЛЕННОЙ ПЕРЕДАЧИ ДАННЫХ В КОМПЬЮТЕРНЫХ СЕТЯХ

Ю. И. ВОРОТНИЦКИЙ, Р. А. РУМАС

Белорусский государственный университет (г. Минск, Республика Беларусь)

Поступила в редакцию 24.02.2023

Аннотация. Представлены результаты разработки архитектуры аппаратно-программного средства однонаправленной передачи данных в компьютерных сетях. Основными структурными элементами архитектуры являются оптическая гальваническая развязка, медиаконвертеры и прокси-серверы, исключая на аппаратном уровне двунаправленную передачу данных. Работа по однонаправленной передаче данных осуществляется на базе транспортного протокола UDP, обеспечивающего ее без установления двунаправленного взаимодействия. Однонаправленная передача данных производится с прокси-сервера, на котором работает специальное программное обеспечение отправителя, осуществляющее однонаправленную передачу файлов данных, преобразуя их в однонаправленный поток UDP дейтаграмм. Для приема однонаправленного потока UDP дейтаграмм используется прокси-сервер, осуществляющий прием, обработку и формирование исходного файла данных. Достоверность однонаправленной передачи файлов данных обеспечивается путем избыточности (многократной передачи) и проверки контрольной суммы.

Ключевые слова: однонаправленная передача данных, UDP, дейтаграмма, оптическая гальваническая развязка, прокси-сервер, медиаконвертер, архитектура.

Конфликт интересов. Авторы заявляют об отсутствии конфликта интересов.

Для цитирования. Воротницкий, Ю. И. Архитектура аппаратно-программного средства однонаправленной передачи данных в компьютерных сетях / Ю. И. Воротницкий, Р. А. Румас // Доклады БГУИР. 2023. Т. 21, № 3. С. 96–101. http://dx.doi.org/10.35596/1729-7648-2023-21-3-96-101.

ARCHITECTURE OF HARDWARE AND SOFTWARE FOR UNIDIRECTIONAL DATA TRANSMISSION IN COMPUTER NETWORKS

YURY I. VARATNITSKI, RAMAN A. RUMAS

Belarusian State University (Minsk, Republic of Belarus)

Submitted 24.02.2023

Abstract. The results of a study of the architecture of hardware and software for unidirectional data transmission in computer networks are presented. The architecture is presented in the form of optical galvanic isolation, media converters and proxy servers, excluding bidirectional data transmission at the hardware level. Work on unidirectional data transmission is carried out on the basis of the UDP transport protocol, which provides operation without establishing bidirectional interaction. Unidirectional data transfer is carried out by a proxy server running a special sender's software that performs unidirectional data file transfer. This software converts the source data file into a unidirectional stream of UDP datagrams. To receive a unidirectional stream of UDP datagrams, a proxy server is used, on which the recipient's special software is running. The receiving proxy server receives, processes and generates the source data file. The reliability of the unidirectional transmission of data files is ensured by redundancy (multiple transmission) and checksum verification.

Keywords: unidirectional data transmission, UDP, datagram, optical galvanic isolation, proxy server, media converter, architecture.

Conflict of interests. The authors declare no conflict of interests.

For citation. Varatnitski Y. I., Rumas R. A. (2023) Architecture of Hardware and Software for Unidirectional Data Transmission in Computer Networks. *Doklady BGUIR*. 21 (3), 96–101. http://dx.doi.org/10.35596/1729-7648-2023-21-3-96-101 (in Russian).

Введение

В настоящее время существует большое число конфиденциальных сетей, в которых необходимо обеспечить защиту секретной или иной информации, представляющей особую ценность для ее владельца. Один из способов надежной защиты от внешних угроз – изолировать такие сети, сделав их недоступными из других внешних сетей. Тем не менее возникают случаи, когда требуется передавать информацию между такими сетями независимо от их конфиденциального характера, либо обеспечить безопасную передачу данных из недоверенных сетей в конфиденциальную сеть. По сути, речь идет о реализации модели контроля и управления доступом Белла – Лападулы, предполагающей однонаправленную передачу данных от субъекта с низким уровнем доступа к объекту с высоким уровнем конфиденциальности [1].

Однонаправленная передача данных предполагает, что устройство в компьютерных сетях может только передавать данные или только получать их. При этом устройство – источник данных – может осуществлять их передачу одному или нескольким устройствам – приемникам, но последние не могут передавать данные источнику. Однонаправленная передача данных применяется для безопасной передачи информации, например, файлов, журналов событий, почтовых сообщений, промышленных протоколов, обновлений программного обеспечения. При этом гарантия однонаправленного потока информации означает, что конфиденциальная информация может быть передана без ущерба для целостности или конфиденциальности информации в сети.

Известны различные средства однонаправленной передачи данных на основании программного решения, такие как межсетевые экраны [2, 3] и специализированные аппаратные решения (диоды данных). Первые имеют избыточный функционал, эффективно снижают уровень угроз, но не обязательно предотвращают их. Во многих случаях они достаточны, чтобы остановить незначительные угрозы информационной безопасности. Однако современные киберугрозы являются сложными и отличаются скоординированными атаками сразу с нескольких векторов. В этом случае внешние угрозы могут быть предотвращены путем их физического отделения от защищаемых сетей, например, с помощью оптической гальванической развязки между ними. Однако отсутствие маршрутизируемого и управляемого подключения в некоторой степени снижает их гибкость и не позволяет адаптироваться к требованиям конкретных информационных систем. Сложные угрозы могут использовать скоординированную и настойчивую тактику для преодоления эшелонированной защиты, паролей, многофакторной аутентификации и даже биометрии, но преодолеть физический разрыв (оптическую гальваническую развязку) в диоде данных с помощью существующих инструментов по-прежнему невозможно.

В статье проведен анализ функциональности существующих специализированных аппаратно-программных средств однонаправленной передачи данных. Предлагается решение, устраняющее их основные недостатки.

Анализ существующих решений

На основании информации, предоставленной в открытом доступе, существующие программно-аппаратные решения, предположительно, работают на основе физической реализации однонаправленной передачи путем использования в одних случаях гальванической развязки, в других – с помощью программного обеспечения. Гальваническую развязку можно реализовать, применяя оптический канал, работающий на передачу по одному оптическому волокну. Основываясь на данном методе, передать данные можно по известному транспортному протоколу UDP. Кроме того, необходимо использовать прокси-серверы на передающей и принимающей сторонах для организации двунаправленного взаимодействия с конечными пользователями. Применение прокси-серверов позволит хранить данные как на передающей стороне, так и на принимающей.

Аппаратно-программный комплекс АМТ InfoDiode (рис. 1) [4] обеспечивает изоляцию критичных информационных систем, сохраняя при этом нужный уровень их функциональности для взаимодействия со смежными информационными системами. Передача трафика возможна только в одном направлении: гальваническая развязка гарантирует отсутствие обратной связи. Прокси-серверы обеспечивают связь с внешними системами и организуют однонаправленный транспорт данных между собой. Для внешних систем прокси-сервер выступает в роли сервера данных (FTP\FTPS, SMTP\StartTLS, CIFS), на передающей системе – в роли клиента.

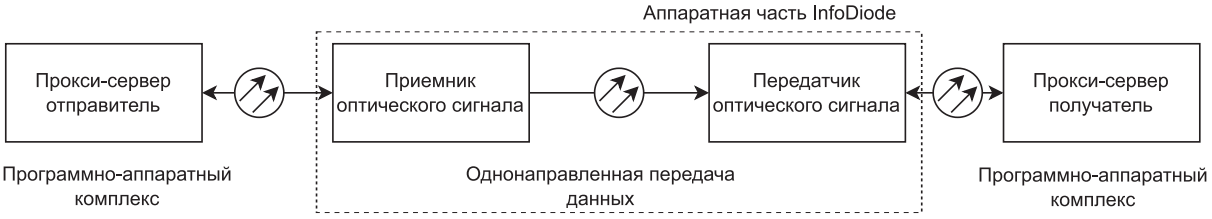

Рис. 1. Схема работы системы InfoDiode
Fig. 1. Scheme of the InfoDiode system operation

Техническое средство однонаправленной передачи данных «Диод-2С» (рис. 2) [5] предназначено для однонаправленной передачи данных из информационных систем с низкой степенью конфиденциальности (секретности), в том числе из интернета, в информационные системы с высокой степенью конфиденциальности (секретности).

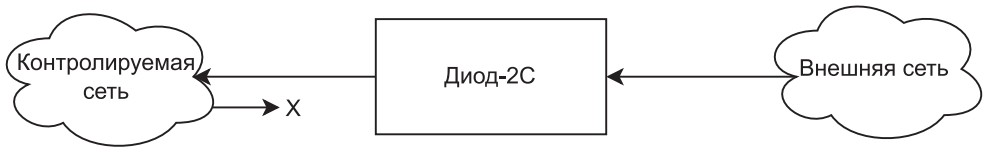

Рис. 2. Схема работы технического средства однонаправленной передачи данных «Диод-2С»
Fig. 2. Scheme of the technical means of unidirectional data transmission “Diode-2C” operation

В основе решения Fox DataDiode [6] лежит аппаратная часть, обеспечивающая одностороннее сетевое соединение. Блок Fox DataDiode уникален тем, что гарантирует односторонний трафик на физическом уровне: у него нет программного обеспечения или прошивки, следовательно, им нельзя манипулировать или произвести неправильную настройку. Однако полная инсталляция Fox DataDiode (рис. 3) включает программное обеспечение прокси-серверов с обеих сторон Fox DataDiode, которые преобразуют двунаправленные протоколы в односторонние, и наоборот.

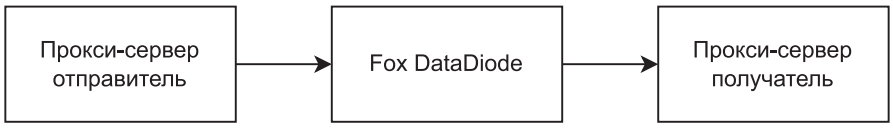

Рис. 3. Схема работы системы Fox DataDiode
Fig. 3. Scheme of Fox DataDiode system the operation

С учетом специфики области применения рассматриваемых средств можно выделить их следующие недостатки:

– невозможность однозначно определить, каким образом гарантируется однонаправленная передача данных, так как производители не предоставляют таких сведений и не раскрывают коммерческую тайну по производству этих средств;

– невозможность определить дополнительный скрытый функционал, который может присутствовать в данных средствах;

– зависимость от производителя в рамках сервисного и гарантийного обслуживания;

– невозможность замены составных частей альтернативными отечественными решениями;

– сложность внедрения в существующие информационные системы.

Разработка архитектуры аппаратно-программного средства

Архитектура аппаратно-программного средства однонаправленной передачи данных разрабатывалась на основании следующих требований:

• физическая изоляция информационных систем;

• однонаправленная передача файлов данных;
• однонаправленная передача потока данных (UDP);
• однонаправленная передача журналов событий (syslog).

Функциональность предлагаемого средства однонаправленной передачи данных обеспечивает архитектурное решение (рис. 4), включающее два медиаконвертера, два прокси-сервера, оптический разветвитель (сплиттер).

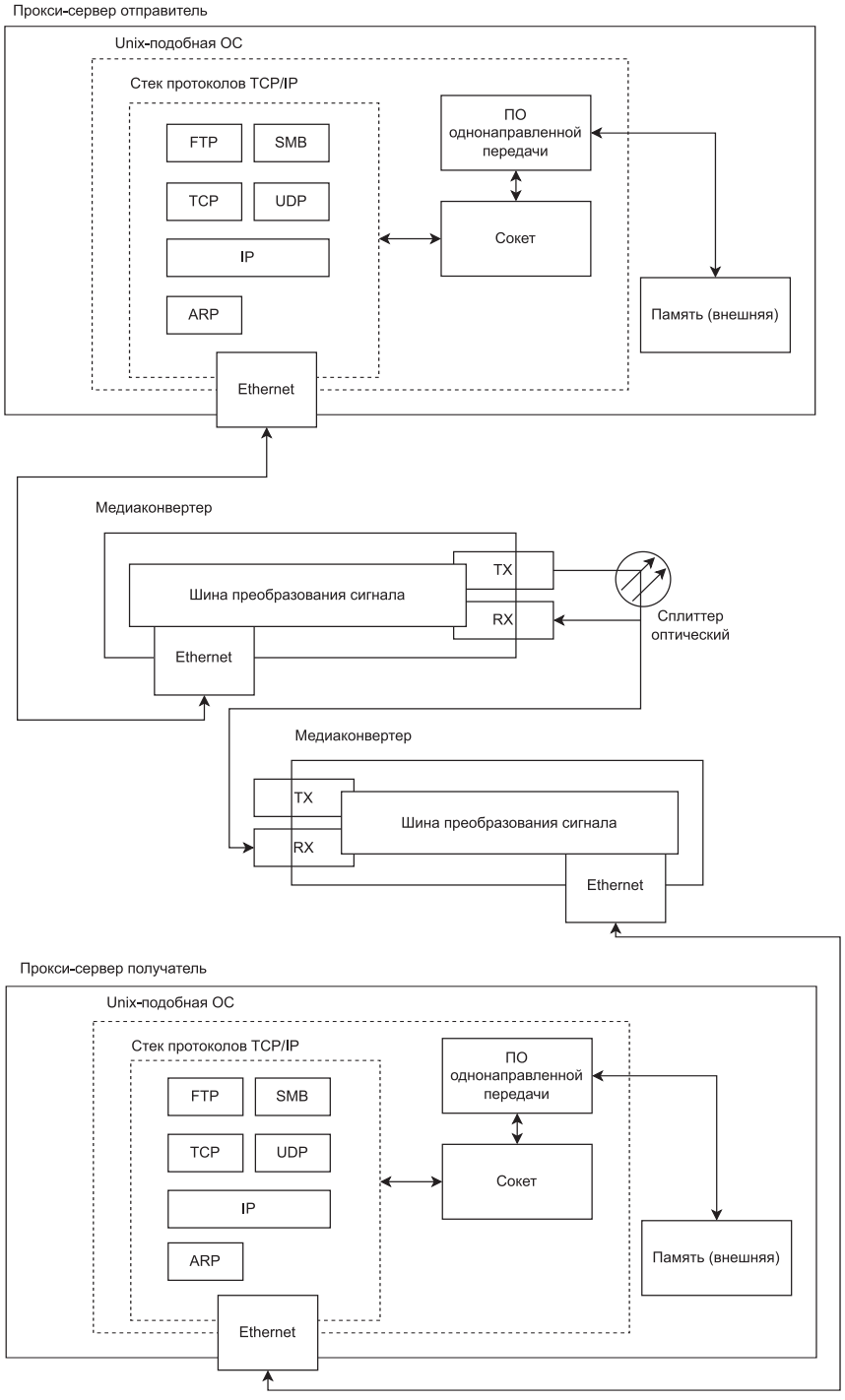

Рис. 4. Архитектура аппаратно-программного средства однонаправленной передачи в компьютерных сетях
Fig. 4. Architecture of hardware and software for unidirectional transmission in computer networks

Медиаконвертеры имеют один Ethernet-интерфейс и оптический интерфейс, представленный двумя оптическими модулями: TX – фотопередатчик, RX – фотоприемник. Разделение оптического интерфейса медиаконвертера на два модуля гарантирует физически однонаправленную передачу при использовании со стороны-отправителя TX-модуля, а на стороне-получателе – RX.

Наличие активной (по умолчанию) функции LLR (Link Loss Return) говорит о том, что передатчик оптического порта (TX) конвертера выключается, если приемник (RX) не получает сигнала. Особенностью предлагаемой архитектуры аппаратной части является наличие оптического разветвителя (сплиттера) для организации передачи сигналов на RX-модуль стороны-отправителя.

Для реализации однонаправленного шлюза на канальном уровне модели OSI источнику и приемнику информации необходимо адресовать пакеты согласно уникальным идентификаторам, называемым MAC-адресами (Media Access Control). Предварительно по протоколу ARP (Address Resolution Protocol) нужно обменяться информацией для установления соответствия MAC-адреса и IP-адреса компьютера, с которым необходимо взаимодействовать. Однако при однонаправленном канале передачи данных обмен информацией произведен не будет. Одним из способов решения данной проблемы является установление статического соответствия MAC-адреса и IP-адреса на устройстве-отправителе. Для работы на сетевом и транспортном уровнях модели взаимодействия OSI при однонаправленной передаче данных следует использовать протоколы без установления логической связи, которая подразумевает двунаправленное взаимодействие. Протокол IP на сетевом уровне является протоколом без установления логической связи.

Другой вариант реализации передачи данных на IP-адрес получателя – мультикастовая передача, которая не предполагает предварительно настроенную ARP-запись. Следовательно, устройство-отправитель данных при однонаправленной передаче будет отправлять информацию на мультикастовый адрес, например, 224.0.0.1, а устройство-получатель, в свою очередь, будет прослушивать и ожидать данные на указанный адрес. Мультикастовая передача данных имеет ряд преимуществ по сравнению с передачей на конкретный IP-адрес:

- прокси-сервер на стороне-отправителе не зависит от настроенного IP-адреса прокси-сервера на стороне-получателе;
- отсутствует необходимость настраивать статическую ARP-запись на прокси-сервере отправителя;
- нет необходимости изменять настройки прокси-сервера отправителя при изменении IP-адреса на прокси-сервере получателя;
- для повышения целостности при однонаправленной передаче данных может использоваться несколько прокси-серверов получателей, которые будут подключены через коммутатор и получать мультикастовые данные.

При использовании транспортных протоколов следует выбрать UDP, который является дейтаграммным протоколом, реализующим так называемый ненадежный сервис по возможности, не гарантирующий доставку сообщений адресату, но обеспечивающий работу без необходимости предварительного сообщения для установки специальных каналов передачи. Прокси-серверы отправителя и получателя обеспечивают однонаправленную передачу данных, например файлов, работая на транспортном уровне UDP модели OSI через медиаконвертеры следующим образом:

- прокси-сервер отправителя получает файлы данных из открытой сети посредством двунаправленного взаимодействия и протоколов SMB, FTP, SFTP и т. д.;
- ввиду отсутствия двунаправленного взаимодействия между прокси-сервером отправителя и прокси-сервером получателя, необходимо организовать статическую ARP-запись на стороне-отправителе;
- программное обеспечение (ПО) на стороне-получателе постоянно прослушивает порт на определенном IP-адресе и ожидает приема UDP-дейтаграмм, преобразуя их в исходное сообщение (файлы данных) и сохраняя их в памяти;
- ПО на стороне-отправителе постоянно проверяет наличие файлов данных в памяти и при их наличии начинает процесс однонаправленной передачи на заранее настроенный IP-адрес и порт получателя через Socket, который, в свою очередь, работает по транспортному протоколу UDP;
- после передачи на стороне-получателе проверяется контрольная сумма переданных файлов данных по предварительно переданной информации о контрольной сумме от отправителя.

Достоверность передачи обеспечивается путем избыточности (многократной передачи) и проверки контрольной суммы каждый раз. После передачи и успешной проверки контрольной суммы на стороне-получателе клиенты из закрытой сети (сети ограниченного взаимодействия) получают переданные файлы от прокси-сервера данных посредством двунаправленного взаимодействия и протоколов SMB, FTP, SFTP [7] и т. д.

Предложенное архитектурное решение было реализовано в виде макетного образца на основе медиаконвертеров DMC-F15SC [8] и сплиттера. Медиаконвертер имеет физически разделенные модули фотопередатчика и фотоприемника. Программное обеспечение прокси-серверов функционирует на аппаратной платформе в виде одноплатных компьютеров Raspberry PI 4 и написано на языке программирования Python.

Выводы

1. Предложенная архитектура аппаратной и программной частей позволила реализовать отечественное импортозамещающее средство однонаправленной передачи данных, обеспечивающее гарантированное одностороннее взаимодействие, реализуемое на физическом уровне. Особенности данной архитектуры – гарантированная однонаправленная передача данных, использование прокси-серверов для обеспечения двунаправленного взаимодействия устройства с конечными пользователями, работа на существующем стеке протоколов TCP/IP.

2. При атаке на критически важные производственные и транспортные системы средства однонаправленной передачи данных помогут сохранить элементы контроля и управления важной инфраструктурой в неприкосновенности, не нарушая при этом работу всей системы. Физическая изоляция, невозможность передачи данных в одном из направлений фактически лишают злоумышленников шансов на реализацию вредоносных замыслов.

References

1. Bell D. E., LaPadula L. J. (1976) *Secure Computer System: Unified Exposition and Multics Interpretation*. Bedford, The MITRE Corporation, Report ESD-TR-75-306.
2. *Top Firewall Vendors 2021: Reviews and Ratings*. Available: https://techdayhq.com/community/articles/top-firewall-vendors-2021-reviews-and-ratings (Accessed 20 January 2023).
3. *Network Firewalls Reviews and Ratings*. Available: https://www.gartner.com/reviews/market/network-firewalls (Accessed 20 January 2023).
4. *InfoDiode – Unidirectional Data Transmission System.* Available: http://amt.ru/web/ru/infodiode (Accessed 20 January 2023).
5. *Technical Means of Unidirectional Data Transmission "Diod-2C"*. Available: http://www.cbi-info.ru/groups/page-1180.htm (Accessed 20 January 2023).
6. *Fox DataDiode*. Available: https://www.fox-it.com/en/technology/datadiode/ (Accessed 20 January 2023).
7. Olifer V. G., Olifer N. A. (2010) *Computer Networks. Principles, Technologies, Protocols.* St. Petersburg, 4th ed. 944.
8. *Media Converter D-Link DMC-F15SC.* Available: https://www.dlink.ru/ru/products/4/1673.html (Accessed 20 January 2023).

Вклад авторов / Authors' contribution

Все авторы внесли равный вклад в написание статьи / All authors contributed equally to the writing of the article.

Сведения об авторах

Воротницкий Ю. И., к. ф.-м. н., доцент, заведующий кафедрой телекоммуникаций и информационных технологий Белорусского государственного университета

Румас Р. А, соискатель кафедры телекоммуникаций и информационных технологий Белорусского государственного университета

Адрес для корреспонденции

220064, Республика Беларусь,
г. Минск, ул. Курчатова, 1
Белорусский государственный университет
Тел.: +375 17 209-59-42
E-mail: rumas96_96@mail.ru
Румас Роман Андреевич

Information about the authors

Varatnitski Y. I., Cand. of Sci., Associate Professor, Head of the Department of Telecommunications and Information Technologies of the Belarusian State University

Rumas R. A., Applicant at the Department of Telecommunications and Information Technologies of the Belarusian State University

Address for correspondence

220064, Republic of Belarus,
Minsk, Kurchatova St., 1
Belarusian State University
Tel.: +375 17 209-59-42
E-mail: rumas96_96@mail.ru
Rumas Raman Andreevich