http://dx.doi.org/10.35596/1729-7648-2026-24-2-55-61

УДК 004.056

# УСОВЕРШЕНСТВОВАННАЯ МОДЕЛЬ СИСТЕМЫ ОДНОНАПРАВЛЕННОЙ ПЕРЕДАЧИ ДАННЫХ

Ю. И. ВОРОТНИЦКИЙ, Р. А. РУМАС

*Белорусский государственный университет (Минск, Республика Беларусь)*

**Аннотация.** Использование современных средств защиты информации для защиты объектов информационной инфраструктуры при взаимодействии с иными информационными системами не гарантирует обеспечение кибербезопасности в случае попыток проведения сложных и целенаправленных кибератак. Для решения указанной проблемы целесообразно применять средства однонаправленной передачи данных. В статье приведены результаты обоснования и разработки усовершенствованной модели однонаправленной передачи данных, в которой гарантированность однонаправленной передачи данных обеспечивается аппаратным средством, а работа уровня приложений – специальным программным обеспечением. Для гарантии отказоустойчивости применяется резервирование прокси-серверов, используемых при организации работы специального программного обеспечения. Представлен алгоритм усовершенствованной модели, в котором предусмотрено применение обратного канала передачи данных для подтверждения успешной передачи, а также реализован механизм вероятностного характера, что позволяет снизить риск использования злоумышленником обратного канала для передачи информации путем модуляции по частоте или по времени.

**Ключевые слова:** кибербезопасность, компьютерные сети, межсетевое экранирование, критически важные объекты информатизации, однонаправленная передача данных, протокол UDP, оптическая развязка, прокси-сервер.

**Конфликт интересов.** Авторы заявляют об отсутствии конфликта интересов.

**Для цитирования.** Воротницкий, Ю. И. Усовершенствованная модель системы однонаправленной передачи данных / Ю. И. Воротницкий, Р. А. Румас // Доклады БГУИР. 2026. Т. 24, № 2. С. 55–61. http://dx.doi.org/10.35596/1729-7648-2026-24-2-55-61.

# IMPROVED MODEL OF UNIDIRECTIONAL DATA TRANSMISSION SYSTEM

YURY VARATNITSKI, RAMAN RUMAS

*Belarusian State University (Minsk, Republic of Belarus)*

**Abstract.** The use of modern information security tools to protect information infrastructure objects interacting with other information systems does not guarantee cybersecurity in the event of complex and targeted cyberattacks. To address this issue, it is advisable to use unidirectional data transmission tools. This article presents the results of the substantiation and development of an improved unidirectional data transmission model, in which guaranteed unidirectional data transmission is ensured by hardware, and application-level operation is ensured by special software. To ensure fault tolerance, redundant proxy servers are used to organize the operation of special software. An algorithm for the improved model is presented, which provides for the use of a reverse data transmission channel to confirm successful transmission, and also implements a probabilistic mechanism, which reduces the risk of an attacker exploiting the reverse channel to transmit information using frequency or time modulation.

**Keywords:** cybersecurity, computer networks, firewalling, critical information technology facilities, one-way data transmission, UDP protocol, optical isolation, proxy server.

**Conflict of interests.** The authors declare that there is no conflict of interests.

**For citation.** Varatnitski Y., Rumas R. (2026) Improved Model of Unidirectional Data Transmission System. *Doklady BGUIR*. 24 (2), 55–61. http://dx.doi.org/10.35596/1729-7648-2026-24-2-55-61 (in Russian).

**Введение**

В настоящее время с ростом числа кибератак появляется необходимость эффективного и надежного обеспечения кибербезопасности различных объектов информационной инфраструктуры [1], в том числе критически важных объектов информатизации (КВОИ) [2]. При этом функционирование КВОИ, как правило, предполагает взаимодействие с иными информационными системами, автоматизированными системами управления технологическими процессами или информационно-телекоммуникационными сетями. Следует отметить, что современные межсетевые экраны (рис. 1) не гарантируют стопроцентную безопасность взаимодействия и исключения несанкционированного доступа (сетевых атак) на КВОИ [3]. На рис. 1 ЛВС – локальная вычислительная сеть.

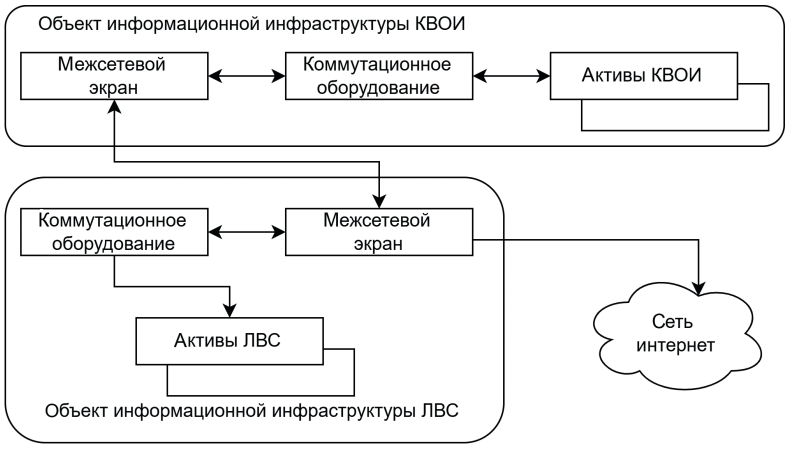


**Рис. 1.** Схема обеспечения взаимодействия критически важных объектов информатизации с внешними системами при использовании межсетевых экранов
**Fig. 1.** Scheme for ensuring interaction of critical information technology objects with external systems using firewalls

Для решения возникающих проблем обеспечения кибербезопасности КВОИ при информационных взаимодействиях целесообразно использовать надежные решения – средства однонаправленной передачи данных (ОПД) [4]. В частности, их применение уместно при обновлении программного обеспечения, синхронизации времени, мониторинге параметров функционирования КВОИ, сборе информации о событиях информационной безопасности, получении данных от датчиков, при передаче почтовых сообщений и т. п. Для обеспечения полноценной передачи такой информации через однонаправленный канал передачи данных в статье рассмотрены соответствующие модели системы ОПД, которые позволяют описать процесс информационного взаимодействия при отсутствии привычного двунаправленного канала взаимодействия.

**Анализ существующих моделей однонаправленной передачи данных**

С целью передачи данных из внешних систем, в том числе корпоративных, для КВОИ предлагается модель системы ОПД, показанная на рис. 2 (модель № 1).

Модель № 1 предполагает использование средства ОПД для гарантии невозможности компрометации данных и активов КВОИ. При этом не применяются программные средства, обеспечивающие преобразование двунаправленных протоколов в однонаправленные, используемые системой ОПД. Средство ОПД в этом случае работает на физическом уровне модели OSI, и реализация передачи данных на более высоких уровнях ложится на передающие и принимающие устройства. К недостаткам данной модели можно отнести то, что для организации привычной работы по двунаправленному взаимодействию с применением протоколов FTP, SMB, SMTP и других необходимо наличие специального программного обеспечения (СПО), преобразующего работу двунаправленных протоколов в однонаправленный поток данных, например транспортного протокола UDP, без установления связи.

На практике, как правило, необходимо наличие функционала ОПД, который подразумевает модель «все включено» (модель № 2). Такой вариант представлен на рис. 3.

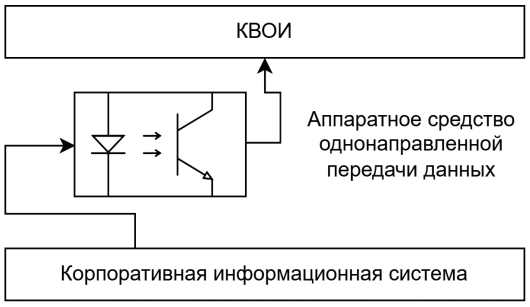


**Рис. 2.** Модель № 1 однонаправленной передачи данных
**Fig. 2.** Model No 1 of unidirectional data transmission

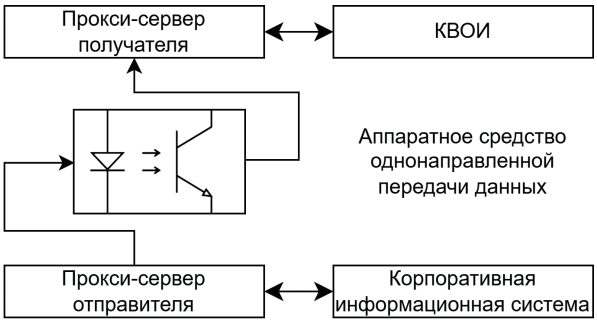


**Рис. 3.** Модель № 2 однонаправленной передачи данных
**Fig. 3.** Model No 2 of unidirectional data transmission

Модель № 2 имеет ряд преимуществ:

– реализация ОПД на всех уровнях без необходимости использования (установки) СПО на рабочие места пользователей;

– минимизация настройки прокси-серверов, обеспечивающей ОПД;

– исключение человеческого фактора (ошибок) в процессе настройки клиентских программных средств, обеспечивающих ОПД при использовании привычных протоколов (FTP, SMB, SMTP и т. д.), которые в данной модели реализованы на прокси-серверах самого аппаратно-программного средства ОПД [5].

К недостаткам модели № 2 отнесем следующее:

– возможны ошибки при ОПД ввиду отсутствия сообщений об успешном приеме данных на прокси-сервере получателя;

– отсутствие принципа отказоустойчивости компонентов модели.

Принимая во внимание недостатки модели № 2, можно создать модель № 3 (рис. 4), учитывающую следующие требования:

– отказоустойчивая работа по ОПД на стороне получателя (на его прокси-серверах);

– параллельный прием данных на нескольких прокси-серверах получателя с целью минимизации вероятности появления возможных ошибок передачи данных и обеспечения проверки контрольных сумм между прокси-серверами получателя.

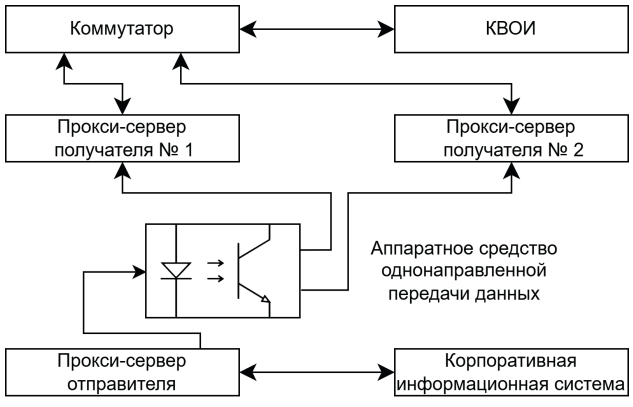


**Рис. 4.** Модель № 3 однонаправленной передачи данных
**Fig. 4.** Model No 3 of unidirectional data transmission

Модель № 3 хотя и обеспечивает дублирование прокси-сервера, но не исключает возможность потери сетевых пакетов (файлов данных) при передаче UDP потока данных. Прокси-серверы получателя, постоянно ожидая поток UDP-данных, готовы принимать и обрабатывать их, однако это не исключает вероятность ошибок в процессе передачи сетевых пакетов. Предлагается обеспечить «голосование» между прокси-серверами и проверку (сравнение) полученных данных. Например, при передаче файлов данных проверять передаваемую контрольную сумму

и размер файла данных, а при передаче потока UDP-трафика (журналов событий, syslog, видеопотока и т. д.) – количество переданных (принятых) пакетов.

Рассмотренные модели систем ОПД не могут подтверждать факт успешной передачи данных. Для решения этой проблемы предлагается модель № 4 (рис. 5), в которой присутствует функционал обратного однонаправленного канала передачи данных для подтверждения успешной доставки данных.

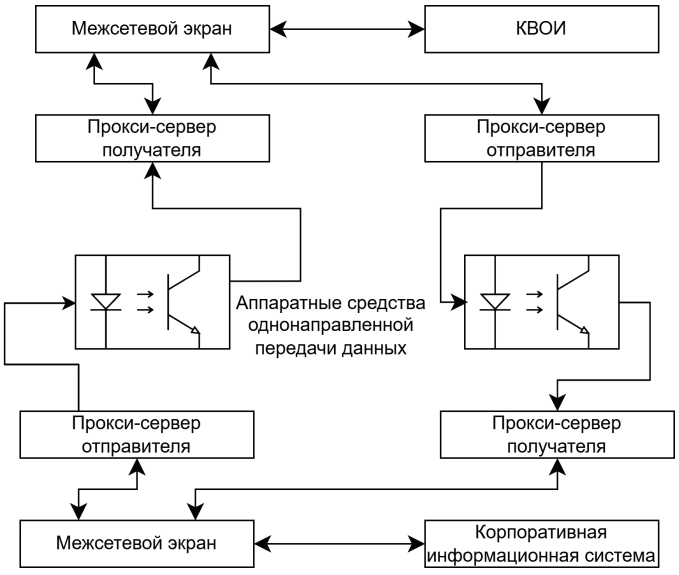


**Рис. 5.** Схема модели № 4, ставшей основной для усовершенствованной модели
**Fig. 5.** The diagram of model No 4, which became the basis for the improved model

Модель № 4, ставшая основной для усовершенствованной модели, по сравнению с № 1–3 имеет дополнительный физически выделенный обратный канал, позволяющий на аппаратном уровне средства ОПД ограничить объемы и содержание передаваемых данных квитанциями о получении. В то же время в случае проникновения нарушителя (злоумышленника) в обе информационные системы возникает риск получения несанкционированного доступа к прокси-серверам с последующей модуляцией передаваемых (по частоте и времени) квитанций из информационной системы с высокой степенью конфиденциальности в информационную систему с низкой степенью конфиденциальности.

**Предлагаемая усовершенствованная модель**

Схема усовершенствованной модели № 5 представлена на рис. 6. В нее введен дополнительный механизм вероятностного характера при использовании обратного канала связи для передачи квитанций. Такая модель предполагает передачу подтверждений доставки (квитанций) с определенной вероятностью. При этом снижается риск того, что злоумышленник сможет использовать обратный канал для передачи информации путем модуляции по частоте или по времени, так как он не знает, будет ли отправлена квитанция, передаваемая взломанным прокси-сервером, в конкретный момент времени.

Для модели № 5 предлагается алгоритм передачи квитанции, приведенный на рис. 7. Алгоритм выполняет проверку на прокси-сервере получателя факта успешного получения передаваемой информации [5]. При этом в случае успешного получения файлов данных формируется сообщение (квитанция) об успешном получении файла данных, которое отправляется средству ОПД для передачи через обратный однонаправленный канал передачи данных. Однако передача подтверждений доставки (квитанции) осуществляется в цикле с определенной вероятностью $P$ для снижения риска того, что злоумышленник на стороне получателя сообщения сможет использовать обратный канал для утечки защищаемой информации путем модуляции по частоте или по времени, так как он не знает, будет ли отправлена квитанция в конкретный момент времени. Попытки отправки квитанции осуществляются в цикле и после какого-либо числа попыток $n \le N$, которые происходят с задержкой $\Delta t$; квитанция будет доставлена на прокси-сервер

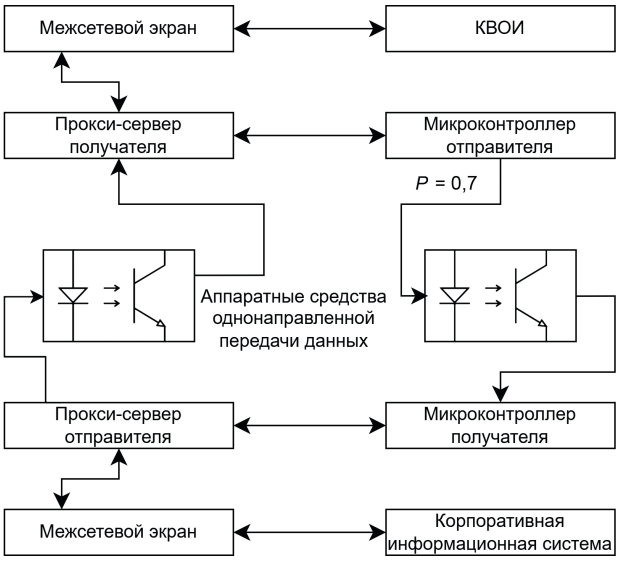


**Рис. 6.** Схема усовершенствованной модели № 5
**Fig. 6.** Improved model diagram No 5

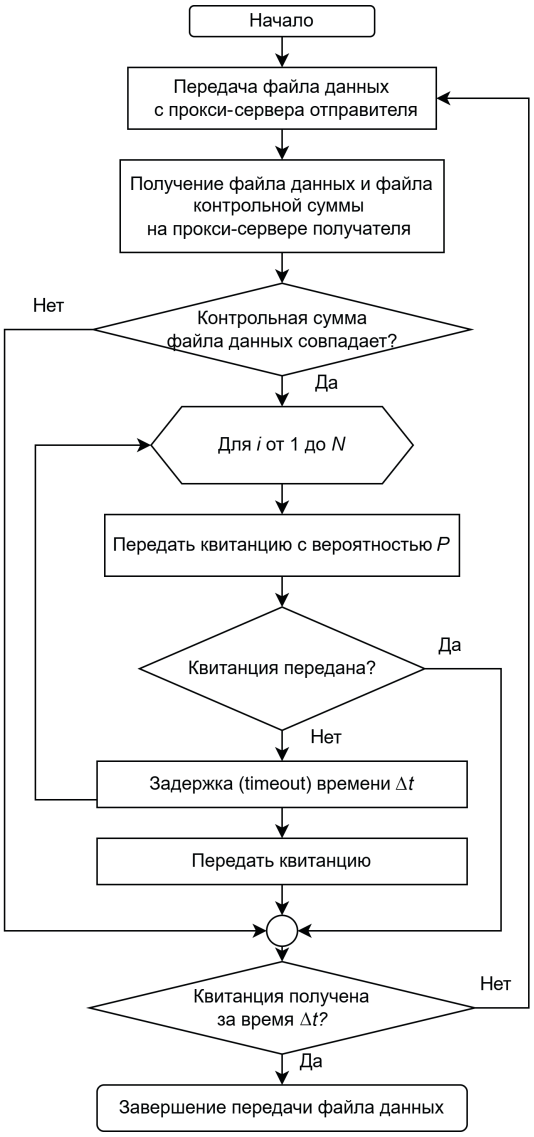


**Рис. 7.** Алгоритм передачи квитанции при однонаправленной передаче данных
**Fig. 7.** Receipt transmission algorithm for unidirectional data transmission

отправителя для подтверждения факта успешной доставки. В случае ошибки передачи данных (несовпадения контрольной суммы) квитанция не будет отправлена, и прокси-сервер отправителя повторит отправку исходной полезной информации. Число попыток $N$ может быть переменным и вычисляться по определенному одному и тому же алгоритму в доверенной среде средства ОПД как на стороне отправителя, так и на стороне получателя.

**Заключение**

1. Рассмотренные модели однонаправленной передачи данных, с одной стороны, позволяют информационным системам взаимодействовать между собой, а с другой – исключают проведение кибератак на информационные системы, кибербезопасность которых необходимо обеспечивать. Так, модель № 1 представляет собой минимальную аппаратную систему без специального программного обеспечения с реализацией функционала гарантированной однонаправленной передачи данных на физическом уровне. Модель № 2 включает в себя модель № 1, а также прокси-серверы отправителя и получателя для обеспечения преобразования на них двунаправленных протоколов уровня приложения в однонаправленный поток данных. Модель № 3 включает в себя модель № 2 с возможностью отказоустойчивости и контроля целостности при приеме за счет использования двух и более прокси-серверов получателя, которые обеспечивают «голосование» и контроль получаемых данных. Модель № 4, ставшая основной для усовершенствованной модели № 5, включает в себя как функционал моделей № 2 и 3, так и дополнительный функционал обратного однонаправленного канала передачи данных для подтверждения успешной доставки данных.

2. Представлен алгоритм усовершенствованной модели с обратным каналом передачи данных для подтверждения успешной передачи и с механизмом вероятностного характера. Это позволяет снизить риск использования злоумышленником обратного канала для передачи информации путем модуляции по частоте или по времени.

**Список литературы**

1. О кибербезопасности: Указ Президента Республики Беларусь от 14 февраля 2025 г. № 40. Режим доступа: https://pravo.by/document/?guid=12551&p0=P32300040. Дата доступа: 28.11.2025.
2. О некоторых мерах по совершенствованию защиты информации: Указ Президента Республики Беларусь от 16 апреля 2013 г. № 196. Режим доступа: https://pravo.by/document/?guid=12551&p0=P31300196. Дата доступа: 28.11.2025.
3. Краткий обзор основных инцидентов в области промышленной кибербезопасности за третий квартал 2025 года [Электронный ресурс]. Режим доступа: https://ics-cert.kaspersky.ru/publications/reports/2025/12/18/a-brief-overview-of-the-main-incidents-in-industrial-cybersecurity-q3-2025. Дата доступа: 10.01.2026.
4. 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.
5. Румас, Р. А. Алгоритмы однонаправленной передачи данных в компьютерных сетях / Р. А. Румас // Информационные технологии и системы – 2024: материалы Междунар. науч. конф., Минск, 20 нояб. 2024 г. Минск: Белор. гос. ун-т информ. и радиоэлектрон., 2024. С. 177–178.

Поступила 27.01.2026 Принята в печать 25.02.2026

**References**

1. On Cybersecurity. *Decree of the President of the Republic of Belarus of Feb. 14, 2025 No 40*. Available: https://pravo.by/document/?guid=12551&p0=P32300040 (Accessed 28 November 2025) (in Russian).
2. On Some Measures to Improve Information Security. *Decree of the President of the Republic of Belarus of Apr. 16, 2013 No 196*. Available: https://pravo.by/document/?guid=12551&p0=P31300196 (Accessed 28 November 2025) (in Russian).
3. *A Brief Overview of the Main Industrial Cybersecurity Incidents for the Third Quarter of 2025*. Available: https://ics-cert.kaspersky.ru/publications/reports/2025/12/18/a-brief-overview-of-the-main-incidents-in-industrial-cybersecurity-q3-2025 (Accessed 10 January 2026) (in Russian).
4. 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).

5. Rumas R. A. (2024) Algorithms of Unidirectional Data Transmission in Computer Networks. *In Information Technologies and Systems – 2024, Materials of the International Scientific Conference, Minsk, Nov. 20*. Minsk, Belarusian State University of Informatics and Radioelectronics. 177–178 (in Russian).

Received: 27 January 2026 Accepted: 25 February 2026

**Вклад авторов / Authors' contribution**

Авторы внесли равный вклад в написание статьи / The authors contributed equally to the writing of the article.

**Сведения об авторах**

**Воротницкий Ю. И.,** канд. физ.-мат. наук, доц., зав. каф. телекоммуникаций и информационных технологий, Белорусский государственный университет

**Румас Р. А.,** соискатель каф. телекоммуникаций и информационных технологий, Белорусский государственный университет

**Адрес для корреспонденции**

220064, Республика Беларусь,
Минск, ул. Курчатова, 1
Белорусский государственный университет
Тел.: +375 17 209-59-42
E-mail: y.vorotn@gmail.com
Воротницкий Юрий Иосифович

**Information about the authors**

**Varatnitski Y.,** Cand. Sci. (Phys. and Math.), Associate Professor, Head of the Department of Telecommunications and Information Technologies, Belarusian State University

**Rumas R.,** Applicant of the Department of Telecommunications and Information Technologies, 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: y.vorotn@gmail.com
Varatnitski Yury