

**ТЕХНИКА ВЫСОКИХ НАПРЯЖЕНИЙ  
(05.14.12)**

**АВТОМАТИЗАЦИЯ И УПРАВЛЕНИЕ  
ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ  
И ПРОИЗВОДСТВАМИ  
(05.13.06)**

УДК 621.31:004.716

DOI: 10.24160/1993-6982-2021-6-59-65

## **Взаимодействие энергетического оборудования с сетевыми устройствами, поддерживающими интернет-протоколы прикладного уровня**

Р.К. Борисов, С.С. Жуликов, М.Н. Смирнов, Ю.С. Турчанинова, С.И. Хренов, Р.П. Беседин, А.В. Дубинин

Реализация взаимодействия высоковольтного энергетического оборудования с сетевыми устройствами в системах мониторинга предполагает использование проприетарных интернет-протоколов, не удовлетворяющих критериям свободного программного обеспечения и не всегда совместимых с интернет-протоколами персональных компьютеров. Для решения данной проблемы предложено использование промежуточного звена между промышленной и компьютерной сетями. Звено представляет собой сетевой мост, построенный с применением протокола PPP, объединяющего средства автоматики, оснащенные UART-интерфейсами, с компьютерной сетью стандарта 802.11n (Wi-Fi). Представлено несколько моделей организации мостов: централизованный сетевой мост на стороне роутера и клиентского компьютера, распределенная система мостов, выделенный мост. На основе проведенного анализа рекомендовано применение централизованной модели для сети, к которой предъявляются повышенные требования надежности. При необходимости одновременного доступа к нескольким устройствам автоматики и высокой скорости обмена данными следует использовать распределенную модель. Выделенный мост нужен лишь в особых случаях, например, когда при реализации системы мониторинга требуется высокая компактность.

*Ключевые слова:* система мониторинга энергетического оборудования, проприетарный протокол, интернет-протокол, микроконтроллер, роутер, сетевой мост, персональный компьютер, автоматизированное рабочее место.

*Для цитирования:* Борисов Р.К., Жуликов С.С., Смирнов М.Н., Турчанинова Ю.С., Хренов С.И., Беседин Р.П., Дубинин А.В. Взаимодействие энергетического оборудования с сетевыми устройствами, поддерживающими интернет-протоколы прикладного уровня // Вестник МЭИ. 2021. № 6. С. 59—65. DOI: 10.24160/1993-6982-2021-6-59-65.

## **Power Equipment Interaction with Network Devices Supporting Internet Application-level Protocols**

R.K. Borisov, S.S. Zhulikov, M.N. Smirnov, Yu.S. Turchaninova, S.I. Khrenov, R.P. Besedin, A.V. Dubinin

The implementation of interaction between high-voltage power equipment with computer network devices in monitoring systems involves the use of proprietary Internet protocols that do not meet the criteria of free software and are not always compatible with the Internet protocols of personal computers. To solve this problem, it is proposed to use an intermediate link between the industrial and computer networks. This link is a network bridge built using the PPP protocol, which unites automatic devices equipped with UART interfaces with a computer network of the 802.11n (Wi-Fi) standard. The article presents several models for organizing bridges: a centralized network bridge on the side of a router and a client computer, a distributed system of bridges, a dedicated bridge. Based on the analysis conducted, it is recommended to use a centralized model for the network, to which increased reliability requirements are applied. In the case of simultaneous access to several automation devices and high data exchange speed, a distributed model should be used. A dedicated bridge is only needed in special cases, for example, when high compactness is required for the implementation of the monitoring system.

and client computer, a distributed bridging system, and a dedicated bridge. Based on the accomplished analysis, it is recommended to use a centralized model for a network that has to comply with more stringent reliability requirements. If there is a need to have simultaneous access to several automation devices and high data exchange rates, a distributed model should be used. A dedicated bridge is used only in special cases, for example, when a high compactness is required in implementing a monitoring system.

*Key words:* power equipment monitoring system, proprietary protocol, Internet protocol, microcontroller, router, network bridge, personal computer, workstation.

*For citation:* Borisov R.K., Zhulikov S.S., Smirnov M.N., Turchaninova Yu.S., Khrenov S.I., Besedin R.P., Dubinin A.V. Power Equipment Interaction with Network Devices Supporting Internet Application-level Protocols. Bulletin of MPEI. 2021;6:59—65. (in Russian). DOI: 10.24160/1993-6982-2021-6-59-65.

## Введение

В настоящее время на объектах энергетики используются системы мониторинга (СМ) высоковольтного энергетического оборудования:

- силовых трансформаторов (автотрансформаторов) и шунтирующих реакторов [1];
- выключателей [2];
- комплектных распределительных устройств газовых (КРУЭ) [3];
- кабельных линий (КЛ) [2, 4];
- ограничителей перенапряжений нелинейных (ОПН) [5, 11].

Основными целями применения СМ являются:

- переход от системы плано-предупредительных ремонтов (со строгой регламентацией сроков и объемов ремонта электрооборудования) к ремонтам в зависимости от технического состояния оборудования по результатам мониторинга;
- снижение количества внезапных отказов, сопровождающихся значительным масштабом повреждений оборудования, негативными экономическими и экологическими последствиями;
- достоверная оценка остаточного ресурса оборудования.

Взаимодействие высоковольтного энергетического оборудования с СМ или автоматизированными системами управления технологическим процессом (АСУ ТП) осуществляется по специальным промышленным протоколам, например, Modbus, Profibus, CANopen, IEC 60870-5-104 и др. [6]. Для решения конкретных задач берут проприетарные протоколы, являющиеся частной собственностью авторов или правообладателей и не удовлетворяющие критериям свободного программного обеспечения (ПО). Указанные протоколы не всегда совместимы с интернет-протоколами персональных компьютеров (ПК). Например, протокол Modbus TCP обеспечивает передачу собственных пакетов посредством TCP/IP стека, но дальнейшая обработка этих пакетов возможна только с помощью специализированного ПО. В случае с Modbus TCP это будет специализированный OPC-сервер.

При необходимости реализации (FTP, HTTP, SNMP, ICMP и др. [7, 8]) может потребоваться отказ от указанных промышленных стандартов, что, однако, приведет к невозможности непосредственного взаимодействия энергетического оборудования и сетевых устройств,

поддерживающих интернет-протоколы. Решить эту проблему можно с помощью промежуточного звена между промышленной и компьютерной сетями. В настоящей работе в качестве такого звена рассмотрен мост, построенный с применением протокола PPP, позволяющего объединить средства автоматики, оснащенные UART-интерфейсами, с компьютерной сетью стандарта 802.11n (Wi-Fi). Выбор протокола UART и стандарта Wi-Fi связан с их широкой распространенностью, что обеспечивает универсальность предлагаемых решений.

## Способы реализации сетевого моста

На рисунке 1 представлена модель сети, обеспечивающей взаимодействие между компьютерами, серверами и устройствами СМ. Центральное место в этой модели занимает роутер — устройство, гарантирующее связь между всеми вышеуказанными узлами сети.

Наиболее очевидным является вывод о том, что именно роутер должен быть мостом между промышленной и компьютерной сетями. Однако такое решение не является единственным, возможны три варианта:

- роутер является сетевым мостом (централизованным мостом);
- каждое отдельное устройство автоматики оснащено собственным сетевым мостом (распределенная система мостов);
- мостом считается один из персональных компьютеров, находящихся в сети (выделенный мост).

Применение протокола PPP предполагает реализацию TCP/IP-стека непосредственно в самих устройствах автоматики. Авторы имеют опыт реализации стека TCP/IP на микроконтроллерах семейства STM32 с применением среды разработки Keil uVision 5. Реализация сетевого стека возможна, например, с применением библиотек Keil Middleware, включающих в себя описание таких протоколов, как PPP, TCP, UDP, FTP, NTP (SNTP) и др.

Модель организации программного обеспечения микроконтроллера на примере датчика тока системы мониторинга ОПН, использующего все указанные протоколы, изображена на рис. 2.

Она предполагает реализацию двух Internet-протоколов прикладного уровня — FTP (серверная часть) и NTP (клиентская часть). FTP-сервер обеспечивает доступ к SD-карте, на которой расположены файлы данных.

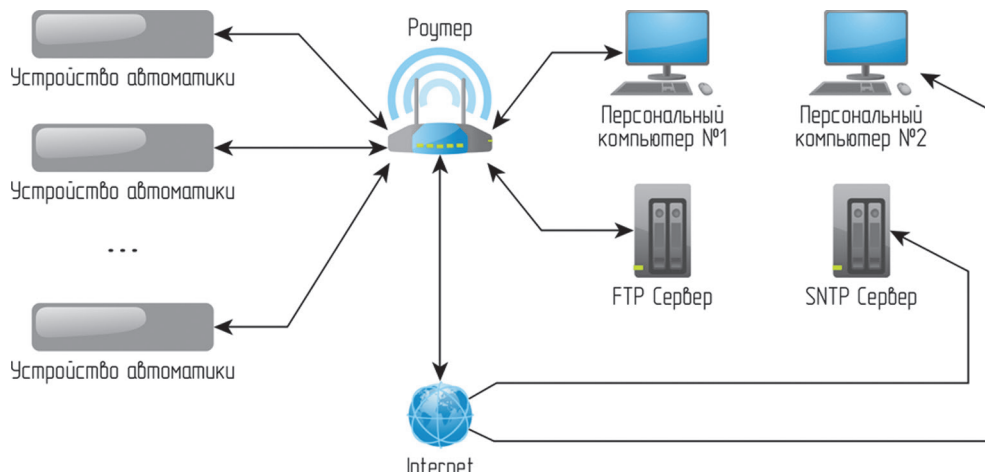


Рис. 1. Схема модели сети

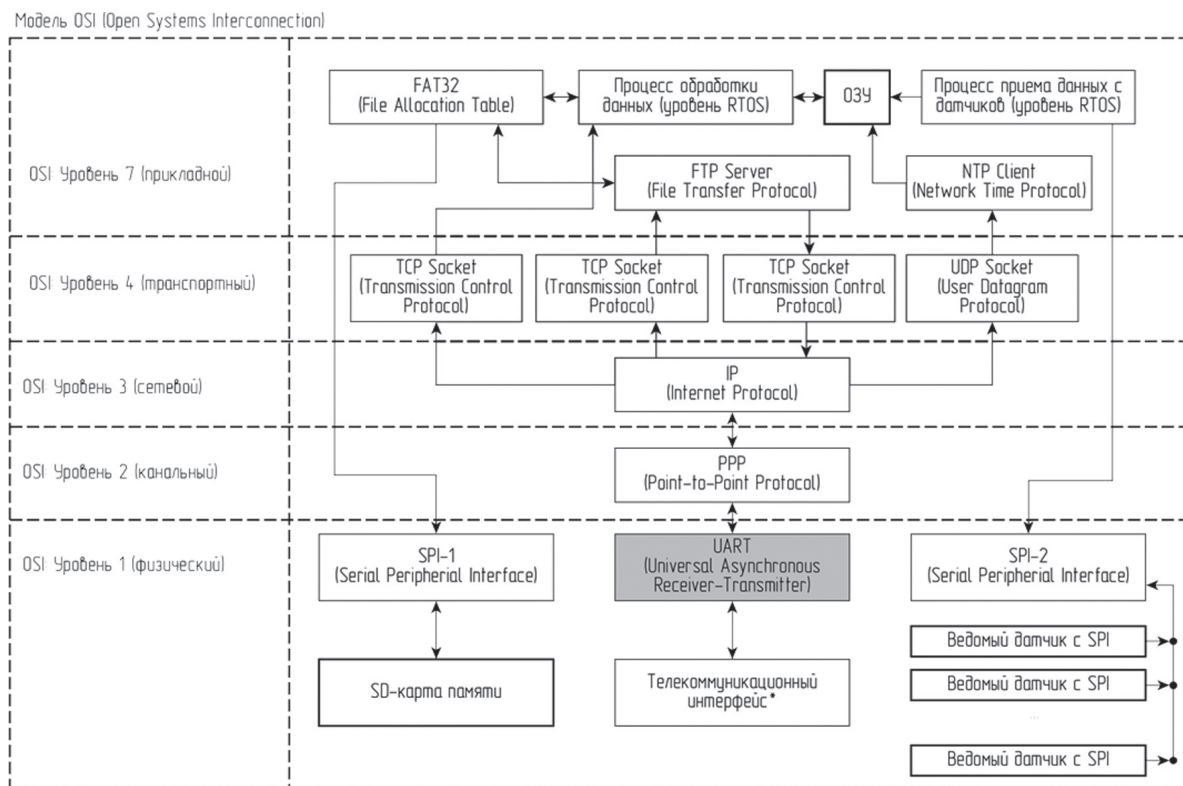


Рис. 2. Модель организации программного обеспечения микроконтроллера

Транспортный уровень модели OSI представлен двумя TCP-сокетами, обслуживающими FTP-сервер (соответственно, один — на прием и один — на передачу данных) и одним UDP-сокетом, обслуживающим NTP-клиент. Дополнительно в программу введен еще один TCP-сокет, используемый для реализации проприетарного протокола прикладного уровня.

Сетевой уровень представлен протоколом IP, а канальный — протоколом PPP (серверная часть), к которому и подключается сетевой мост.

Физический уровень включает в себя два протокола — SPI, используемый для взаимодействия микро-

контроллера с другими блоками устройства (SD-картой и датчиками), и UART, подключаемый к преобразователю интерфейсов, выбор которого зависит от модели используемого сетевого моста.

### Централизованный мост

При реализации централизованного моста к UART-интерфейсу микроконтроллера подключается ZigBee или Wi-Fi-адаптер (возможны и другие варианты, например, Open LRS), представляющий собой преобразователь интерфейсов UART-ZigBee или UART-Wi-Fi, соответственно. В качестве примера взята реализация

централизованного моста на основе радиомодулей UART-ZigBee производства компании Digi, модель XBP24CZ7UIS-004 [9]. Ответной частью указанных радиомодулей на стороне роутера выступают два преобразователя интерфейсов USB-ZigBee производства той же компании. Модель указанной схемы со стороны роутера и клиентского ПК дана на рис. 3.

При использовании централизованной модели PPP-клиент располагается в центральном узле сети, т. е. роутере. Роутер подключается к одному из ZigBee-адаптеров в так называемом «прозрачном режиме» (режиме AT), при этом роутер воспринимает адаптер, как виртуальный UART-интерфейс (на физическом уровне), а затем автоматически организует PPP-сессию с удаленным сервером. На канальном уровне мост имеет статический IP-адрес, к которому можно подключиться с любого компьютера, находящегося в одной сети с роутером (см. рис. 1).

Основная проблема указанной модели взаимодействия заключается в том, что мост может быть организован одновременно только с одним устройством автоматки, при этом все остальные устройства, хотя и подключены к ZigBee-сети, но не могут осуществлять сетевое взаимодействие с устройствами, находящимися в локальной сети Wi-Fi и глобальной сети Internet.

Устройства автоматки переключаются с помощью второго ZigBee-адаптера, находящегося в режиме API, что позволяет ему управлять любыми другими устройствами в сети ZigBee. На прикладном уровне переключение выполняется с помощью специальной компьютерной программы.

При реализации указанной модели моста к роутеру предъявляют особые требования, по этой причине его выбор является важной задачей. Авторами были

использованы различные модели роутеров компании Mikrotik, в частности, модель RB912UAG-2HPnD [10].

Главное преимущество централизованной модели моста — возможность использования одновременно двух стандартов радиосвязи (например, ZigBee и Wi-Fi), при этом первый стандарт (ZigBee) обеспечивает высокую надежность сетевого подключения, а второй (Wi-Fi) — высокое быстродействие и совместимость с компьютерной сетью.

### Распределенная система мостов

При реализации распределенной системы мостов, каждое устройство автоматки оснащается собственным мини-роутером, подключаемым к микроконтроллеру по интерфейсу UART (на физическом уровне) и обеспечивающим клиентское PPP-подключение на канальном уровне. Он подключается к центральному роутеру по протоколу 802.11n в качестве Wi-Fi-клиента.

Модель указанной схемы со стороны центрального роутера и клиентского ПК продемонстрирована на рис. 4.

Роутер и компьютер АРМ взаимодействуют по классической схеме, используемой в большинстве офисных и домашних сетей, при этом переключение устройств автоматки не требуется, поскольку все они находятся в одной сети с роутером, ПК и серверами одновременно и непрерывно. Таким образом, для подключения к FTP-серверу одного из устройств автоматки достаточно лишь стандартного программного обеспечения, например, Total Commander.

Благодаря тому, что сетевое подключение всех средств СМ непрерывно, появляется ряд возможностей, например, использование протокола NTP в режиме широковещательной рассылки, что гарантирует

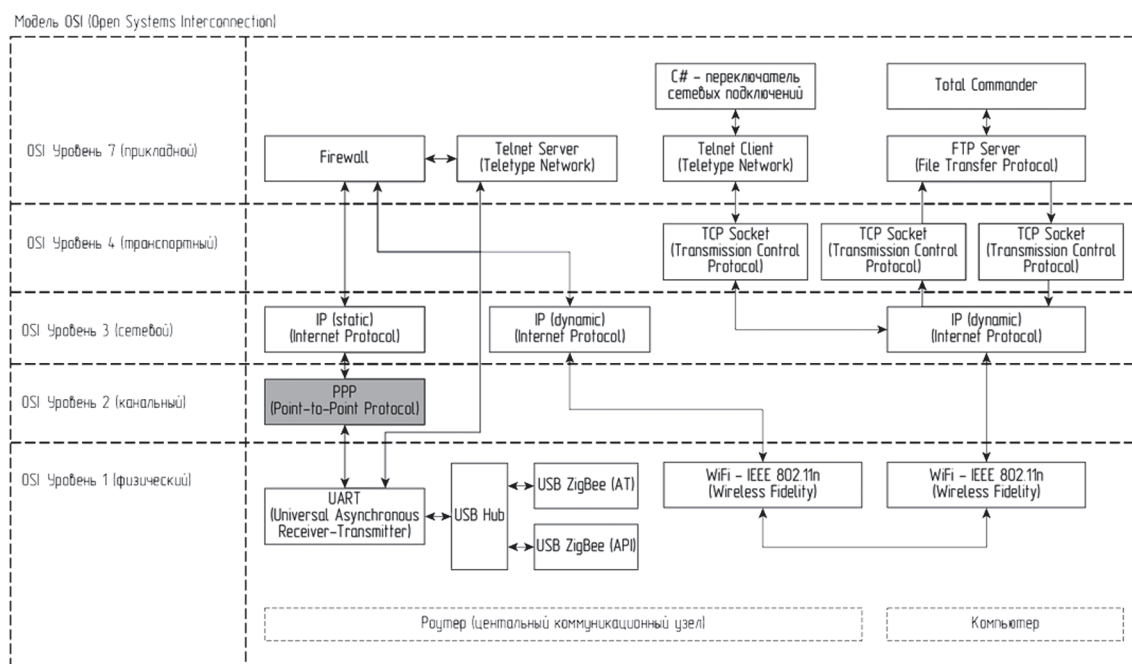


Рис. 3. Модель организации централизованного сетевого моста на стороне роутера и клиентского компьютера

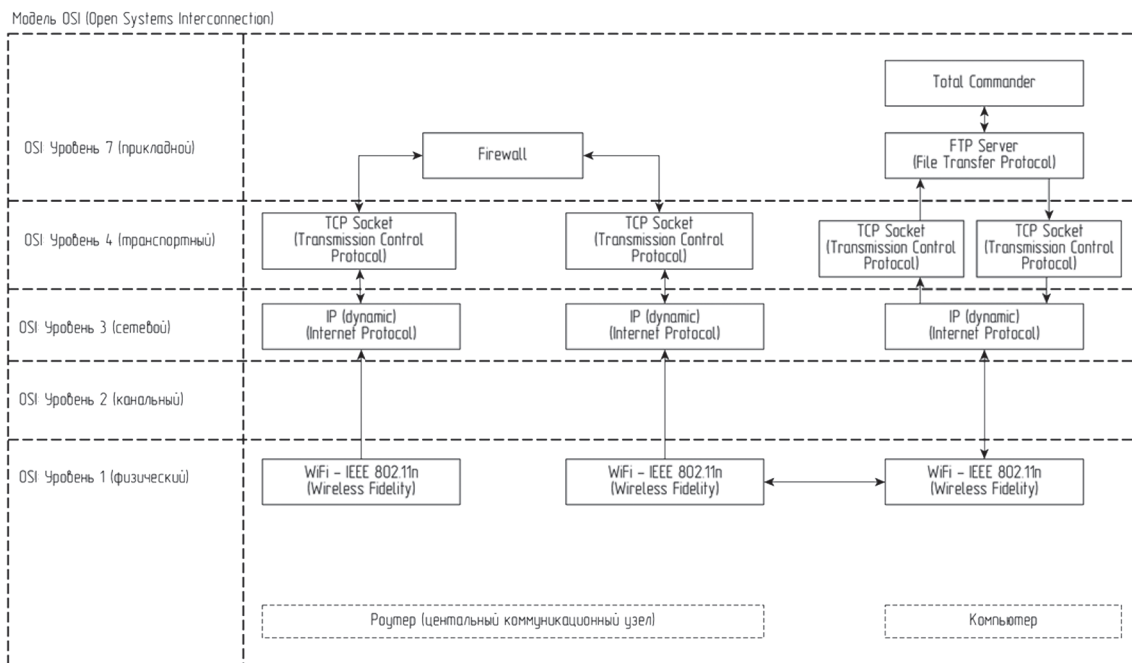


Рис. 4. Модель организации распределенной системы мостов на стороне роутера и компьютера АРМ

корректную синхронизацию часов реального времени между всеми участниками сетевого взаимодействия.

Недостаток указанной схемы — ее большая сложность, а также привязка к протоколу Wi-Fi.

В качестве примера реализации распределенной системы мостов можно привести аппаратно-программный комплекс удаленного мониторинга линейных ограничителей перенапряжения (ОЛН) под рабочим напряжением, находящийся в опытной эксплуатации на ВЛ 150 кВ Мурманского филиала ПАО «МРСК Северо-Запада» с 2018 г. [11]. Комплекс представляет собой двухуровневую распределенную систему с несколькими автономными точками мониторинга ОЛН на опорах ВЛ и АРМ, расположенную в диспетчерской участка электрических сетей [5].

**Выделенный мост**

При реализации выделенного моста к UART-интерфейсам микроконтроллеров подключаются особые UART-Wi-Fi модули, обеспечивающие передачу данных в «прозрачном» режиме. При этом данные с интерфейса UART преобразуются в кадры определенной длины, а затем отправляются на определенный IP-адрес и порт по одному из протоколов транспортного уровня, например, TCP.

Модель указанной схемы со стороны роутера и ПК АРМ приведена на рис. 5.

Передача данных между UART-Wi-Fi адаптером и ПК АРМ происходит также, как и в распределенной модели, различие есть на стороне ПК: на персональном компьютере располагается специализированное программное обеспечение, работающее с TCP пакетами устройств автоматики в режиме «виртуального

UART-порта» (далее, TCP-UART мост), с которым, в свою очередь, создается клиентское PPP подключение. Дальнейшая работа с указанным подключением аналогична двум другим моделям.

Недостаток указанной схемы заключается в необходимости написания дополнительного программного обеспечения для создания TCP-UART моста. Другим недостатком является то, что одновременная работа с большим количеством устройств автоматики затруднена в связи с высокой сложностью настройки системы (для каждого подключения требуются отдельные TCP-UART мост и PPP-подключение).

Преимущество рассматриваемой схемы — высокая компактность оборудования по сравнению с двумя приведенными схемами. Адаптер типа UART-Wi-Fi, как правило, значительно компактнее мини-роутера. Отсутствие необходимости использования USB-ZigBee адаптеров позволяет выбрать более компактный центральный роутер.

**Информационная безопасность**

В соответствии с п. 8 статьи 2 [12] энергетика и топливно-энергетический комплекс относятся к субъектам критической информационной инфраструктуры Российской Федерации. В связи с этим в СМ энергетического оборудования должны обеспечиваться защита информации от несанкционированного доступа и ее сохранность в процессе содержания на машинных носителях АРМ. Применительно к предложенному сетевому мосту защита передаваемой по каналу UART информации обеспечена отдельным ее шифрованием с помощью криптографического алгоритма RSA [13, 14], для реализации которого микроконтроллеры

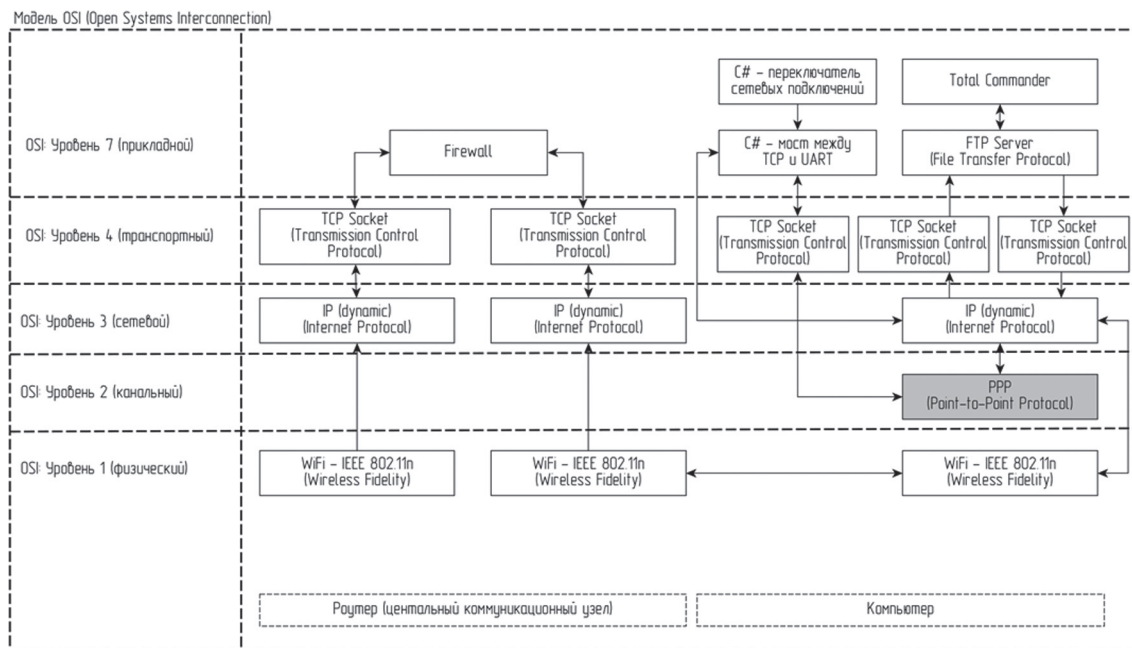


Рис. 5. Модель организации сетевой модели при использовании выделенного моста

СМ оснащены соответствующими аппаратными модулями.

### Заключение

Выбор модели моста зависит от конкретной задачи. Авторы рекомендуют использовать централизованную модель в случае, если основным требованием, предъявляемым к сети, является надежность (в ущерб

скорости и функционалу). Если же к основным требованиям относятся возможность одновременного доступа к нескольким устройствам автоматики и высокая скорость обмена данными, то выбор следует сделать в пользу распределенной модели. Выделенный мост следует применять лишь в особых случаях, например, когда при реализации СМ требуется особая компактность.

### Литература

1. **СТО 56947007-29.200.10.011—2008.** Системы мониторинга силовых трансформаторов и автотрансформаторов. Общие технические требования.
2. **Ботов С.В., Русов В.А.** Управление эксплуатацией высоковольтных кабельных линий и комплектных распределительных устройств по техническому состоянию // Энергоэксперт. 2020. № 2. С. 57—61.
3. **СТО 56947007-29.240.35.270—2019.** Автоматизированная система мониторинга и технического диагностирования КРУЭ. Общие технические требования.
4. **СТО 56947007-29.060.20.243—2017.** Системы мониторинга КЛ с изоляцией из сшитого полиэтилена 110 кВ и выше. Типовые технические требования.
5. **Борисов Р.К. и др.** Аппаратно-программный комплекс удаленного мониторинга линейных ОПН под рабочим напряжением // Электротехника. 2019. № 2. С. 42—47.
6. **Кангин В.В., Козлов В.Н.** Аппаратные и программные средства систем управления. Промышленные сети и контроллеры. М.: Бином, 2010.
7. **Новиков Ю.В., Кондратенко С.В.** Локальные сети: архитектура, алгоритмы, проектирование. М.: ЭКОМ, 2000.

### References

1. **СТО 56947007-29.200.10.011—2008.** Sistemy Monitoringa Silovykh Transformatorov i Avtotransformatorov. Obshchie Tekhnicheskie Trebovaniya. (in Russian).
2. **Botov S.V., Rusov V.A.** Upravlenie Ekspluatatsiey Vysokovol'tnykh Kabel'nykh Liniy i Komplektnykh Raspre-delitel'nykh Ustroystv po Tekhnicheskomu Sostoyaniyu. Energoekspert. 2020;2:57—61. (in Russian).
3. **СТО 56947007-29.240.35.270—2019.** Avtomatizirovannaya Sistema Monitoringa i Tekhnicheskogo Diagnostirovaniya KRUE. Obshchie Tekhnicheskie Trebovaniya. (in Russian).
4. **СТО 56947007-29.060.20.243—2017.** Sistemy Monitoringa KL s Izolyatsiey iz Sshitogo Polietilena 110 kV i Vyshe. Tipovye Tekhnicheskie Trebovaniya. (in Russian).
5. **Borisov R.K. i dr.** Apparatno-programmnyy Kompleks Udalennogo Monitoringa Lineynykh OPN pod Rabochim Napryazheniem. Elektrotehnika. 2019;2:42—47. (in Russian).
6. **Kangin V.V., Kozlov V.N.** Apparatnye i Programmnye Sredstva Sistem Upravleniya. Promyshlennye Seti i Kontrolyery. M.: Binom, 2010. (in Russian).
7. **Novikov Yu.V., Kondratenko S.V.** Lokal'nye Seti: Arkhitektura, Algoritmy, Proektirovanie. M.: EKOM, 2000. (in Russian).

8. **Кульгин М.В.** Компьютерные сети. Практика построения. СПб.: Питер, 2003.

9. **DIGI** [Официальный сайт] [www.digi.com/products/models/xb24cz7uis-004](http://www.digi.com/products/models/xb24cz7uis-004) (дата обращения 30.05.2021).

10. **Mikrotik Routers and Wireless** [Официальный сайт] [www.mikrotik.com/product/RB912UAG-2HPnD-OUT](http://www.mikrotik.com/product/RB912UAG-2HPnD-OUT) (дата обращения: 30.05.2021).

11. **Беседин Р.П. и др.** Разработка и применение системы удаленного мониторинга линейных ОПН под рабочим напряжением в ПАО «МРСК Северо-Запада» // Электроэнергия. Передача и распределение. 2019. № 2(13). С. 28—33.

12. **Федеральный закон № 187-ФЗ** от 26 июля 2017 г. О безопасности критической информационной инфраструктуры Российской Федерации.

13. **Шнайер Б.** Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2002.

14. **Столлингс В.** Криптография и защита сетей: принципы и практика. М.: Издат. дом «Вильямс», 2001.

8. **Kul'gin M.V.** Komp'yuternye seti. Praktika Postroeniya. SPb.: Piter, 2003. (in Russian).

9. **DIGI** [Ofits. Sayt] [www.digi.com/products/models/xb24cz7uis-004](http://www.digi.com/products/models/xb24cz7uis-004) (Data Obrashcheniya 30.05.2021).

10. **Mikrotik Routers and Wireless** [Ofits. Sayt] [www.mikrotik.com/product/RB912UAG-2HPnD-OUT](http://www.mikrotik.com/product/RB912UAG-2HPnD-OUT) (Data Obrashcheniya: 30.05.2021).

11. **Besedin R.P. i dr.** Razrabotka i Primenenie Sistemy Udalennogo Monitoringa Lineynykh OPN pod Rabochim Napryazheniem v PAO «MRSK Severo-Zapada». Elektroenergiya. Peredacha i Raspredelenie. 2019;2(13):28—33. (in Russian).

12. **Federal'nyy Zakon № 187-FZ** ot 26 Iyulya 2017 g. O Bezopasnosti Kriticheskoy Informatsionnoy Infrastruktury Rossiyskoy Federatsii. (in Russian).

13. **Shnayer B.** Prikladnaya Kriptografiya. Protokoly, Algoritmy, Iskhodnye Teksty na Yazyke Si. M.: Triumf, 2002. (in Russian).

14. **Stollings V.** Kriptografiya i Zashchita Setey: Printsipy i Praktika. M.: Izdat. Dom «Vil'yams», 2001. (in Russian).

#### Сведения об авторах:

**Борисов Руслан Константинович** — кандидат технических наук, ведущий научный сотрудник кафедры техники и электрофизики высоких напряжений НИУ «МЭИ», e-mail: [BorisovRK@mpei.ru](mailto:BorisovRK@mpei.ru)

**Жуликов Сергей Сергеевич** — кандидат технических наук, доцент кафедры техники и электрофизики высоких напряжений НИУ «МЭИ», e-mail: [ZhulikovSS@mpei.ru](mailto:ZhulikovSS@mpei.ru)

**Смирнов Максим Николаевич** — инженер кафедры техники и электрофизики высоких напряжений НИУ «МЭИ», e-mail: [mns2000@mail.ru](mailto:mns2000@mail.ru)

**Турчанинова Юлия Сергеевна** — ассистент кафедры техники и электрофизики высоких напряжений НИУ «МЭИ», e-mail: [TurchaninovaJS@mpei.ru](mailto:TurchaninovaJS@mpei.ru)

**Хренов Сергей Иванович** — кандидат технических наук, заведующий кафедрой техники и электрофизики высоких напряжений НИУ «МЭИ», e-mail: [KhrenovSI@mpei.ru](mailto:KhrenovSI@mpei.ru)

**Беседин Роман Петрович** — главный специалист департамента технического перевооружения и реконструкции, обслуживания и ремонта объектов электросетевого хозяйства ПАО «Россети Северо-Запад», e-mail: [besedinrp@mrsksevzap.ru](mailto:besedinrp@mrsksevzap.ru)

**Дубинин Александр Викторович** — главный специалист департамента технического перевооружения и реконструкции, обслуживания и ремонта объектов электросетевого хозяйства ПАО «Россети Северо-Запад», e-mail: [dubininav@mrsksevzap.ru](mailto:dubininav@mrsksevzap.ru)

#### Information about authors:

**Borisov Ruslan K.** — Ph.D. (Techn.), Leading Researcher of High Voltage Engineering and Electrophysics Dept., NRU MPEI, e-mail: [BorisovRK@mpei.ru](mailto:BorisovRK@mpei.ru)

**Zhulikov Sergey S.** — Ph.D. (Techn.), Assistant Professor of High Voltage Engineering and Electrophysics Dept., NRU MPEI, e-mail: [ZhulikovSS@mpei.ru](mailto:ZhulikovSS@mpei.ru)

**Smirnov Maksim N.** — Engineer of High Voltage Engineering and Electrophysics Dept., NRU MPEI, e-mail: [mns2000@mail.ru](mailto:mns2000@mail.ru)

**Turchaninova Yuliya S.** — Assistant of High Voltage Engineering and Electrophysics Dept., NRU MPEI, e-mail: [TurchaninovaJS@mpei.ru](mailto:TurchaninovaJS@mpei.ru)

**Khrenov Sergey I.** — Ph.D. (Techn.), Head of High Voltage Engineering and Electrophysics Dept., NRU MPEI, e-mail: [KhrenovSI@mpei.ru](mailto:KhrenovSI@mpei.ru)

**Besedin Roman P.** — Chief Specialist of Technical Re-equipment and Reconstruction, Maintenance and Repair of Electric Grid Facilities Dept., Rosseti North-West, PJSC, e-mail: [besedinrp@mrsksevzap.ru](mailto:besedinrp@mrsksevzap.ru)

**Dubinin Aleksandr V.** — Chief Specialist of Technical Re-equipment and Reconstruction, Maintenance and Repair of Electric Grid Facilities Dept., Rosseti North-West, PJSC, e-mail: [dubininav@mrsksevzap.ru](mailto:dubininav@mrsksevzap.ru)

**Конфликт интересов:** авторы заявляют об отсутствии конфликта интересов

**Conflict of interests:** the authors declare no conflict of interest

**Статья поступила в редакцию:** 31.05.2021

**The article received to the editor:** 31.05.2021