ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 71077— 2023

Единая энергетическая система и изолированно работающие энергосистемы

ОПЕРАТИВНО-ДИСПЕТЧЕРСКОЕ УПРАВЛЕНИЕ

Дистанционное управление. Правила применения защищенных протоколов при организации информационного обмена

Издание официальное

Москва
Российский институт стандартизации
2023

Предисловие

1 РАЗРАБОТАН Акционерным обществом «Системный оператор Единой энергетической системы» (АО «СО ЕЭС»)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 016 «Электроэнергетика»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 31 октября 2023 г. № 1317-ст

4 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.rst.gov.ru)

Содержание

Введение

Настоящий стандарт входит в серию национальных стандартов «Единая энергетическая система и изолированно работающие энергосистемы. Оперативно-диспетчерское управление. Дистанционное управление», устанавливающих требования к осуществлению изменения технологического режима работы и эксплуатационного состояния электросетевого оборудования, устройств релейной защиты и автоматики, изменения нагрузки генерирующего оборудования электростанций с использованием средств дистанционного управления из диспетчерских центров субъекта оперативно-диспетчерского управления в электроэнергетике.

Настоящий стандарт разработан во исполнение положений [1] в целях формирования единых подходов к реализации защиты информационного обмена при осуществлении дистанционного управления из диспетчерских центров субъекта оперативно-диспетчерского управления в электроэнергетике.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Единая энергетическая система и изолированно работающие энергосистемы

ОПЕРАТИВНО-ДИСПЕТЧЕРСКОЕ УПРАВЛЕНИЕ

Дистанционное управление. Правила применения защищенных протоколов при организации информационного обмена

United power system and isolated power systems. Operative-dispatch management. Remote control. Rules of engagement of secure protocols of information exchange

Дата введения — 2023—12—01

1 Область применения

1.1 Настоящий стандарт определяет условия и правила использования защищенных протоколов для обеспечения информационной безопасности при организации и осуществлении из диспетчерских центров субъекта оперативно-диспетчерского управления в электроэнергетике следующих видов дистанционного управления:

- дистанционного управления коммутационными аппаратами, заземляющими разъединителями, технологическим режимом работы электросетевого оборудования и устройствами релейной защиты и автоматики на объектах электроэнергетики;
- дистанционного управления активной и реактивной мощностью генерирующего оборудования ветровых и солнечных электростанций;
- дистанционного управления активной и реактивной мощностью гидравлических электростанций установленной генерирующей мощностью 50 МВт и менее, автоматизированная система управления которых обеспечивает работу такой электростанции в автоматическом режиме без вмешательства оперативного персонала с обеспечением управления водным режимом и выполнением установленных ограничений работы основного и вспомогательного оборудования, а также безопасную эксплуатацию гидротехнических сооружений;
- дистанционного управления активной мощностью гидравлических и гидроаккумулирующих электростанций путем передачи команд на изменение задания плановой мощности в системах группового регулирования активной мощности таких электростанций, подключенных к централизованной (центральной координирующей) системе автоматического регулирования частоты и перетоков активной мощности;
- дистанционного управления активной мощностью тепловых электростанций путем автоматического доведения плановых диспетчерских графиков до таких электростанций;
- дистанционного ввода в действие графиков временного отключения потребления путем автоматизированной передачи команд на введение таких графиков из оперативно-информационных комплексов диспетчерских центров в программно-технические комплексы автоматизированной системы технологического управления центров управления сетями сетевых организаций.

1.2 Настоящий стандарт предназначен для субъектов оперативно-диспетчерского управления в электроэнергетике, организаций, являющихся собственниками или иными законными владельцами объектов электроэнергетики, в отношении которых организуется или осуществляется дистанционное управление из диспетчерских центров субъекта оперативно-диспетчерского управления в электроэнергетике, а также организаций, осуществляющих деятельность по проектированию (разработке), изготов-

Издание официальное

лению, монтажу, наладке, эксплуатации и проверке автоматизированных систем управления технологическими процессами объектов электроэнергетики.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р 57114 Единая энергетическая система и изолированно работающие энергосистемы. Электроэнергетические системы. Оперативно-диспетчерское управление в электроэнергетике и оперативно-технологическое управление. Термины и определения

ГОСТ Р 59947 Единая энергетическая система и изолированно работающие энергосистемы. Оперативно-диспетчерское управление. Дистанционное управление. Требования к информационному обмену при организации и осуществлении дистанционного управления

ГОСТ Р МЭК 60870-5-104 Устройства и системы телемеханики. Часть 5. Протоколы передачи. Раздел 104. Доступ к сети для ГОСТ Р МЭК 870-5-101 с использованием стандартных транспортных профилей

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины, определения и сокращения

3.1 Термины и определения

В настоящем стандарте применены термины по ГОСТ Р 57114, а также следующие термины с соответствующими определениями:

3.1.1 **удостоверяющий центр;** УЦ: Юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей.

Примечание — Функции по созданию и выдаче сертификатов ключей проверки электронных подписей предусмотрены федеральным законом [2].

3.1.2 **аутентификация:** Действия по проверке подлинности субъекта доступа и/или объекта доступа, а также по проверке принадлежности субъекту доступа и/или объекту доступа предъявленного идентификатора доступа и аутентификационной информации.

3.1.3 **канал связи:** Комплекс технических средств и среды распространения, обеспечивающий передачу информации между источником и получателем в виде сигналов электросвязи в определенной полосе частот или с определенной скоростью передачи.

3.1.4 **сервер [контроллер] телемеханики:** Программно-аппаратное устройство, обеспечивающее обмен телеинформацией, включая передачу команд дистанционного управления, между объектом электроэнергетики и диспетчерским центром субъекта оперативно-диспетчерского управления в электроэнергетике, центром управления сетевыми организациями или центром управления ветровыми (солнечными) электростанциями.

3.1.5 **защищенный протокол для информационного обмена:** Протокол передачи данных, обеспечивающий их конфиденциальность и целостность.

3.1.6 **криптографическая защита:** Защита информации путем применения криптографических алгоритмов.

3.2 Сокращения

В настоящем стандарте использованы следующие сокращения:

АСУ ТП — автоматизированная система управления технологическими процессами объекта электроэнергетики;

ДУ — дистанционное управление из диспетчерского центра субъекта оперативно-диспетчерского управления в электроэнергетике;

ДЦ — диспетчерский центр субъекта оперативно-диспетчерского управления в электроэнергетике;

ТМ — телемеханика;

ESP — инкапсулирующий протокол безопасности (Encapsulating Security Protocol);

IKEv2 — протокол обмена ключами в сети Интернет версии 2 (Internet Key Exchange Protocol Version 2);

IP — маршрутизируемый протокол сетевого уровня стека TCP/IP (Internet Protocol) (см. [3]);

IPsec — набор протоколов для обеспечения защиты данных, передаваемых по межсетевому протоколу IP — IP Security (см. [4]);

TCP — протокол передачи данных интернета (Transmission Control Protocol) (см. [5]);

TLS — протокол безопасности транспортного уровня (Transport Layer Security) (см. [6]).

4 Реализация криптографической защиты данных, передаваемых при выполнении дистанционного управления

4.1 Общие требования к реализации криптографической защиты данных, передаваемых при выполнении ДУ

При реализации криптографической защиты данных, передаваемых при выполнении ДУ, должны учитываться ограничения и особенности информационного обмена при осуществлении ДУ, указанные в приложении А.

Криптографической защитой должны обеспечиваться следующие виды данных, передаваемых с использованием протоколов передачи телеинформации между объектами электроэнергетики и ДЦ:

- команды ДУ;
- файлы, передача которых предусмотрена ГОСТ Р МЭК 60870-5-104.

В случаях технических ограничений сервера (контроллера) ТМ объекта электроэнергетики, не позволяющих реализовать разделение трафика телеметрии и команд ДУ, по согласованию с субъектом оперативно-диспетчерского управления в электроэнергетике допускается организация защиты трафика телеметрии и команд ДУ.

При установлении защищенного соединения с использованием протоколов криптографической защиты IPsec или TLS необходимо выполнять двустороннюю аутентификацию сервера ТМ ДЦ и сервера ТМ объекта электроэнергетики. Выполнение двусторонней аутентификации допускается с использованием сертификатов открытых ключей или предварительно распределенных секретов.

При использовании сертификатов электронных подписей доверие к самоподписанным сертификатам и к ведомственным УЦ должно определяться по согласованию между субъектом оперативно-диспетчерского управления в электроэнергетике и собственником или иным законным владельцем объектов электроэнергетики, в отношении которых организуется или осуществляется ДУ, путем указания сведений о корневых и самоподписанных сертификатах электронных подписей, включая следующую информацию:

- серийный номер;
- кем и кому выдано;
- дату выдачи;
- срок действия сертификата;
- отпечаток сертификата электронной подписи.

По усмотрению вышеуказанных лиц состав сведений о корневых и самоподписанных сертификатах электронных подписей может быть расширен.

При использовании предварительно распределенных секретов объект электроэнергетики и ДЦ обмениваются сформированным общим секретом длинной от 256 до 512 бит. Способ обмена выбирается объектом электроэнергетики и ДЦ при установлении защищенного соединения.

Криптографическая защита должна осуществляться с использованием средств криптографической защиты информации, прошедших процедуру оценки соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности.

4.2 Варианты применения протоколов криптографической защиты

Для обеспечения безопасности передачи команд ДУ необходимо использовать протоколы криптографической защиты IPsec или TLS. Выбор используемого протокола должен учитывать возможности сетевого оборудования, через которое будет проходить передача команд ДУ, а также способы реализации и рекомендации субъекта оперативно-диспетчерского управления в электроэнергетике.

Протокол IPsec или TLS может быть реализован в программной среде сервера (контроллера) ТМ, межсетевых экранах, маршрутизаторах или криптошлюзах. Реализация протоколов IPsec и TLS выполняется в соответствии с рекомендациями по криптографической защите информации:

- протокол TLS 1.2 — см. [7];
- протокол TLS 1.3 — см. [8];
- протокол IKEv2 — см. [9];
- протокол ESP — см. [10].

Безопасное соединение для передачи защищаемой информации с использованием протокола криптографической защиты может устанавливаться между сервером (контроллером) ТМ, телекоммуникационным оборудованием объекта электроэнергетики (маршрутизатор, межсетевой экран, криптошлюз) и сервером ТМ ДЦ или криптошлюзом ДЦ.

В случае необходимости определения роли сервера и клиента защищенного соединения соотношение ролей должно соответствовать ГОСТ Р МЭК 60870-5-104, согласно которому сервером защищенного соединения считается объект электроэнергетики, а клиентом защищенного соединения считается ДЦ.

Применение конкретных криптографических алгоритмов и протоколов для защиты ДУ, указанных в настоящем стандарте, должно быть согласовано собственником или иным законным владельцем объекта электроэнергетики, в отношении объекта электроэнергетики которого организуется ДУ, с соответствующим ДЦ, из которого планируется осуществлять ДУ.

4.3 Применение протокола IPsec

4.3.1 Применение протокола IPsec для обеспечения защиты данных

Протокол IPsec применяется для обеспечения защиты данных, передаваемых по межсетевому протоколу IP, и позволяет обеспечивать подтверждение подлинности (аутентификацию) сторон взаимодействия, целостность и/или конфиденциальность IP-пакетов.

При использовании протокола IPsec должна применяться аутентификация на базе сертификатов, выданных доверенным УЦ, либо на основе самоподписанных сертификатов, либо на основе предварительно распределенного секрета («pre-shared-key») в соответствии с соглашением участников информационного обмена, предусматривающим использование типа аутентификации.

Протокол IPsec в реализации IKEv2 выполняется согласно [9]. В таблице 1 представлены идентификаторы трансформов, допустимых к использованию в протоколе IKEv2 (см. [9]).

При выполнении аутентификации с помощью цифровой подписи необходимо использовать параметры эллиптических кривых, определенных в [11].

Таблица 1 — Идентификаторы трансформов для протокола IKEv2

Номер	Имя
Трансформы типа 1 (алгоритм шифрования)	
32	ENCR_KUZNYECHIK_MGM_KTREE
33	ENCR_MAGMA_MGM_KTREE
Трансформы типа 2 (псевдослучайная функция)	
9	PRF_HMAC_STREEBOG_512

Окончание таблицы 1

Номер	Имя
Трансформы типа 4 (алгоритм обмена ключами)	
33	GOST3410_2012_256
34	GOST3410_2012_512
Алгоритм хэширования	
6	STREEBOG_256
7	STREEBOG_512

Протокол IPsec ESP должен соответствовать [10]. В таблице 2 представлены идентификаторы трансформов, допустимых к использованию в протоколе ESP, определенных в [10].

Таблица 2 — Идентификаторы трансформов для протокола ESP

Номер	Имя
Трансформы типа 1 (алгоритм шифрования)	
32	ENCR_KUZNYECHIK_MGM_KTREE
33	ENCR_MAGMA_MGM_KTREE

4.3.2 Применение протокола IPsec на двух независимых каналах связи

При использовании двух независимых каналов связи между объектом электроэнергетики и ДЦ, организованных оборудованием транспортной телекоммуникационной инфраструктуры, необходимо обеспечить два независимых соединения — по одному на каждый канал связи.

По согласованию с ДЦ возможно использование иных способов обеспечения надежности соединений.

4.4 Применение протокола TLS

В реализации протокола защиты транспортного уровня TLS допускается использовать асимметричные криптографические алгоритмы с применением электронной подписи и симметричные криптографические алгоритмы с применением предварительно распределенных секретов («pre-shared-key»).

Протокол TLS необходимо применять для обеспечения прямого взаимодействия между защищаемыми узлами обмена через активное сетевое оборудование с применением трансляции сетевых адресов, исключая вмешательство в передаваемые данные на сетевом оборудовании (инспектирование трафика).

При защите ДУ с применением протокола TLS необходимо использовать версию 1.2 протокола, определенную в [7], или версию 1.3 протокола, определенную в [8].

При использовании протокола TLS версии 1.3 должно применяться подтверждение подлинности на основе сертификатов, выданных доверенным УЦ, либо на основе самоподписанных сертификатов[1)], когда взаимодействие выполняется в тестовых целях, в рамках одной организации или в рамках подписанного соглашения между участниками обмена, в котором предусмотрено использование самоподписанных сертификатов.

При использовании протокола TLS для защиты ДУ рекомендуется использовать TCP-порт назначения 44304 согласно ГОСТ Р МЭК 60870-5-104.

В таблице 3 указаны идентификаторы российских криптографических алгоритмов протокола TLS 1.3, определенные в [8].

[1)] При использовании самоподписанных сертификатов применяется следующая схема обмена: у участника, получающего самоподписанный сертификат от другой стороны обмена, данный сертификат должен быть предварительно определен как доверенный сертификат.

Таблица 3 — Идентификаторы для российских криптографических алгоритмов и схем протокола TLS 1.3

Значение	Имя
Криптонаборы (Cipher Suites)	
0×C1, 0×03	TLS_GOSTR341112_256_WITH_KUZNYECHIK_MGM_L
0×C1, 0×04	TLS_GOSTR341112_256_WITH_MAGMA_MGM_L
0×C1, 0×05	TLS_GOSTR341112_256_WITH_KUZNYECHIK_MGM_S
0×C1, 0×06	TLS_GOSTR341112_256_WITH_MAGMA_MGM_S
Поддерживаемые эллиптические кривые (Supported Groups):	
GC256A (0×0022)	id-tc26-gost-3410-2012-256-paramSetA
GC256B (0×0023)	id-tc26-gost-3410-2012-256-paramSetB
GC256C (0×0024)	id-tc26-gost-3410-2012-256-paramSetC
GC256D (0×0025)	id-tc26-gost-3410-2012-256-paramSetD
GC512A (0×0026)	id-tc26-gost-3410-12-512-paramSetA
GC512B (0×0027)	id-tc26-gost-3410-12-512-paramSetB
GC512C (0×0028)	id-tc26-gost-3410-2012-512-paramSetC
Схемы подписи (SignatureScheme)	
0×0709	gostr34102012_256a
0×070A	gostr34102012_256b
0×070B	gostr34102012_256c
0×070C	gostr34102012_256d
0×070D	gostr34102012_512a
0×070E	gostr34102012_512b
0×070F	gostr34102012_512c

В таблице 4 указаны идентификаторы российских криптографических алгоритмов протокола TLS 1.2, определенные в [7].

Таблица 4 — Идентификаторы для российских криптографических алгоритмов и схем протокола TLS 1.2

Значение	Имя
Криптонаборы (Cipher Suites)	
0×C1, 0×00	TLS_GOSTR341112_256_WITH_KUZNYECHIK_CTR_OMAC
0×C1, 0×01	TLS_GOSTR341112_256_WITH_MAGMA_CTR_OMAC
Алгоритм подписи (Signature Algorithm)	
0×40	gostr34102012_256
0×41	gostr34102012_512
Тип сертификата (Client Certificate Type)	
0×43	gost_sign256
0×44	gost_sign512

4.5 Ключевая система

Для протоколов TLS и IPsec допускается применять асимметричную ключевую систему с использованием внешней системы изготовления ключей на основе спецификаций инфраструктуры открытых ключей в соответствии с рекомендациями [12] и симметричной ключевой системы с предварительно распределенным секретом. Выбранный сценарий работы протоколов должен быть согласован с ДЦ, с которым планируется информационный обмен.

При использовании асимметричной ключевой системы с применением внешней системы изготовления ключей на основе спецификаций инфраструктуры открытых ключей необходимо пользоваться сертификатами открытых ключей, соответствующими спецификациям PKCS #10 и PKCS #15, и их расширениям для стандартизованных в Российской Федерации криптографических алгоритмов в соответствии с [13] и [14].

5 Проверка совместимости реализаций криптографической защиты

5.1 При проектировании и/или установке криптографической защиты собственником или иным законным владельцем объекта электроэнергетики, в отношении оборудования которого организуется или осуществляется ДУ, должна быть обеспечена совместимость такой защиты со средствами криптографической защиты, используемыми в соответствующем ДЦ.

5.2 При рассмотрении проектной документации на создание (модернизацию) АСУ ТП с функцией ДУ, а также при проверке информационного обмена в соответствии с ГОСТ Р 59947 ДЦ должен проводить проверку совместимости следующих параметров:

- применяемого протокола (IPsec или TLS);
- поддерживаемых алгоритмов шифрования и имитозащиты;
- поддерживаемых эллиптических кривых;
- алгоритмов и схем цифровой подписи;
- алгоритмов хэширования.

Приложение А
(справочное)

Ограничения и особенности информационного обмена при осуществлении дистанционного управления из диспетчерских центров субъекта оперативно-диспетчерского управления в электроэнергетике

Выделяют следующие особенности обмена информацией, обусловленные технологическими процессами в электроэнергетике и применяемыми технологиями обмена:

А.1 Передача команд ДУ осуществляется по каналам передачи телеинформации.

А.2 Для передачи команд ДУ между объектами электроэнергетики и ДЦ используются протоколы передачи телеинформации в соответствии с ГОСТ Р МЭК 60870-5-104, не имеющие встроенных механизмов защиты передаваемых данных от несанкционированного доступа и их дискредитации.

А.3 Телеинформация, включая команды ДУ, не относится к информации, доступ к которой ограничен в соответствии с законодательством Российской Федерации.

А.4 Существуют постоянно поддерживаемые соединения для передачи телеинформации, исключая команды ДУ.

А.5 Инициатором соединения и передачи телеинформации может выступать как сервер (контроллер) ТМ объекта электроэнергетики, так и сервер ТМ ДЦ. При этом контролирующая станция эквивалентна клиенту (ДЦ), а контролируемая станция эквивалентна серверу (объект электроэнергетики) (см. ГОСТ Р МЭК 60870-5-104).

А.6 Сервер ТМ ДЦ может в любое время запросить от сервера (контроллера) ТМ объекта электроэнергетики все текущие значения путем выдачи команды опроса.

А.7 Сервер ТМ ДЦ может передавать серверу (контроллеру) ТМ объекта электроэнергетики одиночные (прямые) или двухстадийные (предварительным выбором) команды ДУ. Одиночные (прямые) команды ДУ контролируемой станции выполняются безусловно. Двухстадийные команды (команды с предварительным выбором) ДУ предназначены для переключения коммутационного оборудования объектов электроэнергетики и включают операцию выбора объекта управления. Каждый тип команд ДУ имеет версию, содержащую метку времени.

А.8 В качестве серверов (контроллеров) ТМ на объектах электроэнергетики могут использоваться промышленные серверы или контроллеры с процессорами архитектуры ARM и x86, x64, E2k, RISC-V и другими, зачастую обладающие ограниченными вычислительными возможностями.

А.9 Во многих случаях полоса пропускания каналов связи для передачи телеинформации ограничена и составляет 64 или 128 кбит/с.

А.10 Технологические сети связи объектов электроэнергетики используют подключение по выделенным каналам связи и не имеют подключения к серверам УЦ, использующим сети связи общего пользования (Интернет).

А.11 Серверы (контроллеры) ТМ могут располагаться на удаленных объектах электроэнергетики с небольшим количеством обслуживающего персонала или вообще без постоянного присутствия оперативного персонала.

Библиография

[1] Энергетическая стратегия Российской Федерации на период до 2035 года (утверждена распоряжением Правительства Российской Федерации от 9 июня 2020 г. № 1523-р)

[2] Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»

[3] IETF RFC 791 Интернет протокол [Internet Protocol (IP)]

[4] IETF RFC 4301 Архитектура безопасности для интернет протокола [Security Architecture for the Internet Protocol (IP Security)]

[5] IETF RFC 9293 Протокол передачи данных интернета [Transmission Control Protocol (TCP)]

[6] IETF RFC 8446 Протокол безопасности транспортного уровня (TLS) версии 1.3 [The Transport Layer Security (TLS) Protocol Version 1.3]

[7] Р 1323565.1.020—2020 Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2)

[8] Р 1323565.1.030—2020 Информационная технология. Криптографическая защита информации. Использование криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.3)

[9] МР 26.2.001—2022 Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколе обмена ключами в сети Интернет версии 2 (IKEv2)

[10] Р 1323565.1.035—2021 Информационная технология. Криптографическая защита информации. Использование российских криптографических алгоритмов в протоколе защиты информации ESP

[11] Р 1323565.1.024—2019 Информационная технология. Криптографическая защита информации. Параметры эллиптических кривых для криптографических алгоритмов и протоколов

[12] Р 1323565.1.023—2022 Информационная технология. Криптографическая защита информации. Использование алгоритмов ГОСТ Р 34.10—2012, ГОСТ Р 34.11—2012 в сертификате, списке аннулированных сертификатов (CRL) и запросе на сертификат PKCS #10 инфраструктуры открытых ключей X.509

[13] IETF RFC 2986 PKCS #10: формат запроса сертификата версии 1.7 (Certification Request Syntax Specification Version 1.7)

[14] Р 50.1.110—2016 Информационная технология. Криптографическая защита информации. Контейнер хранения ключей

УДК 621.311:006.354 ОКС 27.010

Ключевые слова: энергосистема, дистанционное управление, информационный обмен, информационная безопасность

Редактор *Н.В. Таланова*
Технический редактор *И.Е. Черепкова*
Корректор *М.И. Першина*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 00.00.2023. Подписано в печать 10.11.2023. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 1,86. Уч.-изд. л. 1,58.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении в ФГБУ «Институт стандартизации»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
www.gostinfo.ru info@gostinfo.ru