Приложение 5

к Техническому заданию

Требования по обеспечению безопасности информации

Порядок создания подсистемы информационной безопасности, построение этапов работ, а также разработка технической и рабочей документации должны соответствовать ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения».

При создании системы учета электроэнергии до ее ввода в опытную эксплуатацию должны быть реализованы мероприятия обеспечения информационной безопасности:

– разработка, выбор и применение мер и средств программно-технической защиты информационных ресурсов на этапах сбора, обработки и транспортировки информации с обеспечением степени ее защищенности, адекватной ценности и конфиденциальности содержания;

– оценка соответствия мер и средств программно-технической защиты информационных ресурсов на соответствие требованиям по безопасности информации в соответствии с действующим законодательством, а также ВНД и ОРД ПАО «Россети Московский регион» и ПАО «Россети»;

– обеспечить создание подсистемы информационной безопасности информационных ресурсов на этапах сбора, обработки и транспортировки информации (инфраструктуры системы учета электроэнергии нижнего уровня);

– обеспечить интеграцию создаваемой подсистемы информационной безопасности инфраструктуры системы учета электроэнергии нижнего уровня с подсистемой информационной безопасности информационно - вычислительного комплекса верхнего уровня автоматизированной системы учёта электроэнергии в распределительных сетях на базе ПО «Пирамида-Сети» (АСУЭ РЭС).

Участник торгово-закупочной процедуры или член коллективного участника должен отвечать следующим требованиям по наличию:

– Лицензии ФСТЭК на деятельность по технической защите конфиденциальной информации согласно пп. б), д), е) ст.4 Положения введенного Постановлением Правительства РФ 2012 года № 79;

– Лицензии ФСБ на осуществлении работ по пунктам 2, 3, 8, 9, 14, 23 «Перечня выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств».

Подрядчик должен обеспечить выполнение требований по обеспечению безопасности информации в соответствии со следующими требованиями.

№ п/п	Наименование требования	Примечание
1.	В интеллектуальной системе учета для пользователей интеллектуальной системы учета должны быть реализованы функции:	п. 9 1.6.1.Постановления Правительства РФ от 19.06.2020 N 890

№ п/п	Наименование требования	Примечание
1.1.	- передачи данных о параметрах настройки и событиях, зафиксированных прибором учета электрической энергии, присоединенным к интеллектуальной системе учета;	
1.2.	- оповещение о возможных недостоверных данных, поступающих с приборов учета в случае срабатывания индикаторов вскрытия электронных пломб на корпусе и клеммной крышке прибора учета, воздействия магнитным полем на элементы прибора учета, неработоспособности прибора учета вследствие аппаратного или программного сбоя, его отключения (после повторного включения), перезагрузки.	
2.	Данные об изменении параметров настройки и о событиях, зафиксированных компонентами интеллектуальной системы учета и прибором учета электрической энергии, должны содержать дату и время возникновения соответствующих изменений и (или) событий и (или) их окончания.	п. 25 Постановления Правительства РФ от 19.06.2020 N 890
3.	Принимаемые меры по защите интеллектуальной системы учета и содержащейся в ней информации должны в том числе обеспечивать:	п. 42 Постановления Правительства РФ от 19.06.2020 N 890
3.1.	- механизмы идентификации и аутентификации по логину и паролю в каждом из компонентов и элементов интеллектуальной системы учета с обязательной фиксацией в интеллектуальной системе учета информации о неверном вводе пароля	
3.2.	- предотвращение неправомерного доступа к информации, обрабатываемой и хранимой в интеллектуальной системе учета и приборах учета электрической энергии, уничтожения такой информации, ее модифицирования, блокирования, копирования, предоставления и распространения, а также иных неправомерных действий в отношении такой информации;	
3.3.	- недопущение воздействия на технические и программные средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование интеллектуальной системы учета	

№ п/п	Наименование требования	Примечание
4.	Идентификация ПУ проводиться по уникальным логическим именам, размером не более 16 байт (первые три символа которого, должны содержать 3-х байтовый код производителя, присваиваемый ассоциацией DLMS)	п. 6.2. СТО 34.01-5.1-006-2023
5.	Для типа соединения «*Публичный клиент*» должен использоваться идентификатор клиента равный 16. Для этого типа соединения разрешены только операции чтения. Криптографическая защита информации не применятся.. Уровень преобразования при установлении соединения с ПУ используется самый низкий.	п. 6.3.3. СТО 34.01-5.1-006-2023
6.	Для типа соединения «*Считыватель показаний*» должен использоваться идентификатор клиента равный 32. Для этого типа соединения разрешены операции чтения, селективной выборки, а также разрешено выполнение определенных действий. Применение криптографической защиты информации в соответствии с п. 10.3. Уровень преобразования при установлении соединения с ПУ используется низкий.	п. 6.3.4. СТО 34.01-5.1-006-2023
7.	Для типа соединения «Конфигуратор» должен использоваться идентификатор клиента равный 48. Для этого типа соединения разрешены операции записи, чтения, селективной выборки, а также разрешено выполнение действий. Применение криптографической защиты информации в соответствии с п. 10.3. Уровень преобразования при установлении соединения с ПУ используется высокий (п. 10.3.3).	п. 6.3.5. СТО 34.01-5.1-006-2023
8.	Изменение пароля или ключа шифрования.	п. 7.3.12. СТО 34.01-5.1-006-2023
9.	Настройки оптопорта [IEC Local Port Setup]	п. 7.3.14. СТО 34.01-5.1-006-2023
10.	Требования по управлению режимами отключения ПУ [Disconnect Control]	п. 7.3.19. СТО 34.01-5.1-006-2023

№ п/п	Наименование требования	Примечание
11.	Объекты класса «Настройки безопасности» предназначены для хранения параметров доступа к данным	п. 7.3.20. СТО 34.01-5.1-006-2023
12.	Низкий уровень безопасности - доступ к ПУ осуществляется через процедуру аутентификации доступа основанную на явной передаче пароля. Соединение с ПУ устанавливается только в случае верного пароля. Низкий уровень безопасности используется для соединения типа «Считыватель показаний». Смена пароля в ПУ осуществляется путем записи атрибута 7 объекта 0.0.40.0.0.255, ИК: 15 при соединении типа «Конфигуратор»	п. 10.3.2. СТО 34.01-5.1-006-2023
13.	Смена мастер ключа производится по объекту 0.0.43.0.2.255 метод 2	п. Д.5 Приложения Д СТО 34.01-5.1-006-2023
14.	Чтение параметров ПУ по безопасности информации в режиме "Считыватель" и "Конфигуратор"	Приложение И. СТО 34.01-5.1-006-2023
15.	Очистка журналов событий безопасности	Приложения Г и Д. СТО 34.01-5.1-006-2023
16.	При выборе средств защиты информации, в том числе сопутствующего встроенного программного обеспечения, должно учитываться возможное наличие ограничений со стороны разработчиков (производителей) или иных лиц на применение программных или программно-аппаратных средств на всей территории Российской Федерации	п.3.3. Типового технического задания на организацию системы учета электроэнергии
17.	Руководство пользователя должно содержать описание: – режимов работы программного обеспечения; – принципов безопасной работы; – функций и интерфейсов функций средства, доступных каждой роли пользователей; – параметров (настроек) безопасности, доступных каждой роли пользователей, и их безопасных значений; – типов событий безопасности, связанных с доступными пользователю	Требование ПАО «Россети»

№ п/п	Наименование требования	Примечание
	функциями; – действий после сбоев и ошибок эксплуатации.	
18.	Руководство администратора должно содержать описание: – действий по приемке поставленного оборудования; – действий по безопасной установке и настройке; – действий по реализации функций безопасности среды функционирования.	Требование ПАО «Россети»
19.	Не допускается влияние аппаратных устройств (микросхем) на выполнение функций безопасности и (или) на реализацию угроз безопасности информации	Требование ПАО «Россети»
20.	Аппаратная платформа программно-технического средства должна соответствовать структурной и функциональной схемам, а также сведениям, приведенным в технических условиях на оборудование	Требование ПАО «Россети»
21	Устранение разработчиком на безвозмездной основе недостатков ПО в течение срока, на который передается неисключительное право использования ПО	Требование ПАО «Россети»
22.	Направление информации о выявленной уязвимости в Банк данных угроз ФСТЭК России в течение 3 рабочих дней с даты выявления уязвимости в своем ПО или программно-аппаратном средстве в соответствии с положениями Методического документа «Регламент включения информации об уязвимостях программного обеспечения и программно-аппаратных средств в Банк данных угроз безопасности информации ФСТЭК России», утвержденного ФСТЭК России 26.06.2018 г.	Требование ПАО «Россети»
23.	Поиск в доступных источниках информации о недостатках средства, в том числе о недостатках в компонентах средства, заимствованных у сторонних изготовителей	Требование ПАО «Россети»

№ п/п	Наименование требования	Примечание
24.	ИВКЭ должен размещаться в металлическом шкафу оснащенным охранной сигнализацией. ИВКЭ должен регистрировать в электронном журнале дату и время срабатывания охранной сигнализации.	Требование ПАО «Россети»
25.	Разработчик ПО должен установить в отношении исходного кода\текста программы режим конфиденциальности.	Требование ПАО «Россети»
26.	Идентификация и аутентификация пользователя должна выполняться до выполнения любых действий по доступу в информационную систему или до выполнения действий администратором по управлению	Требование ПАО «Россети»
27.	Должна быть реализована политика дискреционного и (или) ролевого управления доступом	Требование ПАО «Россети»
28.	Установка ПО (компонентов ПО) должно проводиться только администратором	Требование ПАО «Россети»
29.	Реализация дискреционного и (или) ролевого управления доступом на основе списков управления доступом (матрицы управления доступом) и (или) ролей	Требование ПАО «Россети»
30.	Должна быть предусмотрена обязательная процедура изменения начальной аутентификационной информации администратора\пользователей информационной системы/ОС	Требование ПАО «Россети»
31.	Атрибутами безопасности, функциями безопасности, данными событий безопасности и параметрами функций безопасности информационной системы/ОС должен управлять только администратор	Требование ПАО «Россети»
32.	Аутентификационная информация и информация событий безопасности должны быть защищены от неправомерного доступа к ним и раскрытия	Требование ПАО «Россети»

№ п/п	Наименование требования	Примечание
33.	Должен осуществляться постоянный контроль и проверка правомочности обращений субъектов доступа к объектам доступа	Требование ПАО «Россети»
34.	Должна быть обеспечена блокировка доступа в случае превышения неудачных попыток аутентификации администратора\пользователя	Требование ПАО «Россети»
35.	Должна быть обеспечена надежность меток времени при регистрации событий безопасности	Требование ПАО «Россети»
36.	Администратору должна быть доступна\предоставлена вся информация событий безопасности	Требование ПАО «Россети»
37.	Должно быть обеспечено блокирование загрузки информационной системы\ОС при выявлении попыток загрузки нештатной операционной системы	Требование ПАО «Россети»
38.	Должно быть обеспечено выполнение перезагрузки информационной системы\ОС при выявлении попыток обхода средства доверенной загрузки	Требование ПАО «Россети»
39.	Тестирование (самотестирование) функций безопасности информационной системы\ОС, проверки целостности и целостности данных (параметров) информационной системы\ОС, в том числе метрологического ПО, должна проводиться при загрузке информационной системы\ОС и на периодической основе	Требование ПАО «Россети»
40.	Информация событий безопасности должна быть защищена от несанкционированного удаления или модифицирования	Требование ПАО «Россети»
41.	Регистрация событий безопасности должна проводится непрерывно	Требование ПАО «Россети»
42.	Выполнение управляющих команд должно регистрироваться	Требование ПАО «Россети»

№ п/п	Наименование требования	Примечание
43.	Должна быть обеспечена возможность передачи электронных журналов с событиями безопасности для внешнего хранения	Требование ПАО «Россети»
44.	Должна быть обеспечена идентификация и аутентификация субъектов межсетевого взаимодействия	Требование ПАО «Россети»
45.	Должно быть обеспечено блокирование сетевых запросов и трафика, несанкционированно исходящих из информационной системы и (или) входящих в информационную систему, путем фильтрации информационных потоков	Требование ПАО «Россети»
46.	Непосредственное взаимодействие пользователей прикладного программного обеспечения с ОС (в случае применения) должно быть исключено	Требование ПАО «Россети»
47.	Должен быть обеспечен автоматический запуск прикладного программного обеспечения при старте	Требование ПАО «Россети»
48.	Должно быть обеспечено восстановление штатного режима функционирования информационной системы/ОС без потери данных функций безопасности	Требование ПАО «Россети»
49.	Должно быть обеспечена информационное взаимодействие с между информационно-вычислительным комплексом и прибором учета электроэнергии по защищенным протоколам связи	Требование ПАО «Россети»
50.	Авторские права или права иного правообладателя не должны нарушаться в ДЗО ПАО «Россети» при использовании программного обеспечения и баз данных, входящее в состав комплекта поставки.	Требование ПАО «Россети»
51.	ДЗО ПАО «Россети» должны иметь возможность без согласия правообладателя и без выплаты дополнительного вознаграждения воспроизвести и преобразовать объектный код в исходный текст (декомпилировать программу для ЭВМ) или поручить иным лицам осуществить эти действия, если они необходимы для расследования компьютерных инцидентов	Требование ПАО «Россети»

№ п/п	Наименование требования	Примечание
52.	Направление обновлений ДЗО ПАО «Россети» (потребителям) с обеспечением подлинности и целостности обновлений ПО за счет применения электронной подписи	Требование ПАО «Россети»
53.	Самостоятельное тестирование (испытание) доработанного ПО или его отдельных компонентов на предмет устранения влияния обновлений ПО на его функции безопасности, подтверждение устранения уязвимостей, невнесения новых уязвимостей в ПО путем информирования Департамента обеспечения безопасности ПАО «Россети»	Требование ПАО «Россети»
54.	Разработка безопасного ПО должна проводиться в соответствии с Руководством по разработке безопасного ПО. Руководство по разработке безопасного ПО должно быть утверждено руководством организации, издано и доведено до сведения всех сотрудников организации, имеющих отношение к разработке безопасного ПО	Требование ПАО «Россети»