

Дополнительные требования по обеспечению информационной безопасности

- 1.1. 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».
- 1.2. Обеспечить создание подсистемы информационной безопасности, а также обеспечить выполнение:
 - требований Приказа ФСТЭК от 14 марта 2014 г. № 31 - не ниже **3 класса** защищенности автоматизированной системы управления;
 - требований РД «Автоматизированные системы. Защита от несанкционированного доступа. Классификация автоматизированных систем и требования по защите информации» не ниже уровня 1 Г;
 - требований Распоряжения ПАО «Россети» «О единой технической политике в электросетевом комплексе»;
 - средства защиты информации должны соответствовать требованиям не ниже 6-го или более высокого уровня доверия («Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», утвержденные приказом ФСТЭК России от 02.06.2020 №76);
- 1.3. Применяемое оборудование должно быть включено в Реестр промышленной продукции, произведенной на территории Российской Федерации.
- 1.4. Применяемое программное обеспечение должно быть включено в Единый реестр российских программ для электронно-вычислительных машин и баз данных.
- 1.5. Применяемое оборудование и программное обеспечение средств информационной безопасности, сети передачи данных, АСУТП, ТМ должно быть сертифицированным ФСТЭК России и/или допущенным к применению на объектах ПАО "Россети", в соответствии с требованиями Приказа ПАО «Россети» от 26.07.2023 № 305 «Об утверждении документов в области проверки качества (аттестации) оборудования, материалов и систем» и прошедшим проверку в соответствии с требованиями приказа ПАО «Россети» от 28.08.2020 № 391 «Об утверждении Методики проведения проверки цифрового оборудования и систем на соответствие требованиям безопасности информации, в том числе проведения проверки качества технических средств защиты информации в электросетевом комплексе».
- 1.6. При проектировании и выполнении работ, учесть мероприятия, выполняемые в рамках смежных проектов.
- 1.7. Предусмотреть использование криптографической защиты для трафика обмена информацией между приборами учета / УСПД и ПТК АСТУ / ИВК «Пирамида-сети» / ПО «Альфа-Центр».
- 1.8. Предусмотреть использование средств межсетевого экранирования для фильтрации трафика взаимодействия с внешними сетями и трафика внутри туннеля (расшифрованного трафика).
- 1.8.1. Настройки средств межсетевого экранирования системы телемеханики и учёта ЭЭ должны предусматривать:
 - запрет любого трафика взаимодействий с внешними сетями, кроме шифрованного трафика взаимодействия с криптошлюзами верхнего уровня;
 - в части фильтрации трафика внутри туннеля (расшифрованного трафика), должны быть прописаны конкретные IP-адреса и TCP/UDP порты взаимодействия устройств верхнего

уровня: ПТК АСТУ / ИВК «Пирамида-сети» / ПО «Альфа-Центр», взаимодействие с которыми предусматривается проектом.

- обмен телеинформации с энергообъектом должен быть разрешен только с ПТК АСТУ филиала по протоколу МЭК-60870-104. Обмен телеинформацией с любыми другими устройствами, в том числе серверами АСКУЭ, должен быть запрещен.
- обмен информацией с энергообъектом об учете электроэнергии должен быть разрешен только с ИВК «Пирамида-сети» / ПО «Альфа-Центр» по протоколу DLMS/COSEM (информационная модель СПОДЭС). Обмен информацией об учете электроэнергии с любыми другими устройствами, в том числе серверами ПТК АСТУ, должен быть запрещен.

1.9. Предусмотреть использование брандмауэра уровня приложений с настройками разрешений сетевых взаимодействий (конкретные IP-адреса и TCP/UDP порты) для конкретных программных компонентов, присутствующих в белом списке программных компонентов.

1.10. Применяемые на энергообъекте устройства телемеханики и учёта ЭЭ должны исключать возможность взаимодействия подсистемы учета электроэнергии устройства с сегментом АСТУ верхнего уровня (ПТК АСТУ) и подсистемы телемеханики устройства с сегментом АСКУЭ верхнего уровня (ИВК «Пирамида-сети»), а также исключать возможность передачи любого, в том числе транзитного, трафика между сегментами АСТУ и АСКУЭ.

1.11. взаимодействие устройств верхнего уровня: ПТК АСТУ / ИВК «Пирамида-сети» с подсистемой телемеханики и подсистемой учета электроэнергии должно быть разделено таким образом, при котором исключается возможность доступа из ИВК «Пирамида-сети» к подсистеме телемеханики и из ПТК АСТУ к подсистеме учета электроэнергии.

1.12. Применяемые устройства телемеханики и учёта ЭЭ, содержащие средства криптографической защиты должны размещаться в запираемых металлических шкафах, исключающих доступ к системе телемеханики и учёта ЭЭ без открытия металлического шкафа.

1.13. Информация об открытии/вскрытии и закрытии металлического шкафа с размещенной в нем системой телемеханики и учёта ЭЭ, содержащей средства криптографической защиты, должна передаваться в составе передаваемой телеинформации на диспетчерский пункт.

1.14. В применяемых устройствах телемеханики и учёта ЭЭ, в том числе, должны быть реализованы следующие функции информационной безопасности:

- Идентификация и аутентификация пользователей при конфигурировании устройств;
- Управление доступом пользователей;
- Ограничение программной среды (установка и запуск программных компонентов должен осуществляться на основании белого списка);
- Регистрация событий безопасности и передача их в SIEM;
- Контроль целостности программного обеспечения с использованием криптостойких алгоритмов хеширования;
- Резервное копирование образа программного обеспечения и конфигураций;
- Управление обновлениями программного обеспечения (получение обновлений программного обеспечения только от доверенного источника, контроль целостности обновлений программного обеспечения с использованием криптостойких алгоритмов хеширования).

1.15. Перед проведением предварительных испытаний, выполнить процедуру контроля защищенности устройства телемеханики и учёта ЭЭ. Материалы с результатами контроля защищенности, совместно с протоколами и актами предварительных/приемочных испытаний, включить в комплект исполнительной документации.

1.16. В смете затрат учесть мероприятия по настройке централизованных подсистем обеспечения информационной безопасности.

1.17. В случае использования для передачи информации оперативно-технологического управления и информации учета электроэнергии, каналов операторов мобильной связи (с использованием сим-карт), к услугам, сервисам и настройкам, предъявляются следующие требования:

- Для передачи данных должны использоваться сим-карты с услугой выделенной APN (без доступа к сети Интернет и любым другим внешним сетям);
- Услуги и сервисы, не предназначенные для целей передачи данных с использованием выделенной APN, должны быть отключены и/или заблокированы;
- Для доступа к APN Общества должна применяться аутентификация с использованием логина и пароля. При этом логины и пароли должны быть уникальными для каждой сим-карты;
- Должна быть зафиксирована привязка сим-карты к IMEI оборудования с целью предотвращения их неправомерного использования в других устройствах в случае хищения;
- Любые сетевые соединения между узлами в сети APN (другими сим-картами в той же APN), за исключением серверов/устройств верхнего уровня в сети ПАО «Россети Московский регион», должны быть запрещены/заблокированы путем выполнения настроек на стороне оператора сотовой связи;
- Любые сетевые соединения между узлами в разных APN (сим-картами одной APN с сим-картами другой APN) должны быть запрещены/заблокированы.

Обязательные требования к Участнику:

Участник торгово-закупочных процедур или член коллективного участника, чьими силами планируется выполнение работ в части обеспечения информационной безопасности, на момент подачи заявки и выполнения работ должен отвечать следующим требованиям по наличию:

В случае выполнения ПИР:

– Лицензии ФСТЭК на деятельность по технической защите конфиденциальной информации согласно п.п. д) ст.4 Положения введенного Постановлением Правительства РФ 03.02.2012 года № 79;

Лицензии ФСБ на осуществлении работ по пунктам 2, 3 «Перечня выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств», утвержденного Постановлением Правительства РФ 16.04.2012 года № 313.

Директор департамента
информационной безопасности



В.А. Краснокутский

Поляков В.И.
15-91

77-10/04