

Требования по обеспечению информационной безопасности применяются в случае проведения Проектно-исследовательских работ на предмет модернизации, реконструкции, создания системы АСУ ТП (ТМ), СДТУ, МП РЗА, АСМД и дистанционного управления КА.

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».

Обеспечить создание подсистемы информационной безопасности, а также обеспечить выполнение:

- требований 187-ФЗ от 26.07.2017г. «О безопасности критической информационной инфраструктуры Российской Федерации» и подзаконных актов;

- 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» от 01.04.2016 № 140 «Об утверждении минимальных требований к информационной безопасности АСТУ» (в редакции распоряжения ПАО «Россети» от 27.04.2016 № 178р и распоряжения ПАО «Россети» от 08.02.2019 г. № 70р);

- 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);

В случае модернизации, реконструкции или создания автоматизированной системы мониторинга и диагностики энергетического оборудования, обеспечить выполнение требований Приказа Министерства энергетики РФ от 06.11.2018 №1015 «Об утверждении требований в отношении базовых (обязательных) функций и информационной безопасности объектов электроэнергетики при создании и последующей эксплуатации на территории Российской Федерации систем удаленного мониторинга и диагностики энергетического оборудования».

В случае организации дистанционного управления оборудованием, обеспечить выполнение требований Приказа Минэнерго России от 26.12.2023 № 1215 "Об утверждении дополнительных требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры, функционирующих в сфере электроэнергетики, при организации и осуществлении дистанционного управления технологическими режимами работы и эксплуатационным состоянием объектов электроэнергетики из диспетчерских центров субъекта оперативно-диспетчерского управления в электроэнергетике".

Применяемое оборудование должно быть включено в Реестр промышленной продукции, произведенной на территории Российской Федерации.

Применяемое программное обеспечение должно быть включено в Единый реестр российских программ для электронно-вычислительных машин и баз данных.

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».

При проектировании и выполнении работ, учесть мероприятия, выполняемые в рамках смежных проектов.

Тома проектной и рабочей документации в части информационной безопасности и тома в части защищаемых объектов информационной инфраструктуры (системы АСУ ТП, ТМ, СДТУ, АСМД, дистанционного управления КА и/или оборудования РЗА) согласовать со структурным подразделением информационной безопасности филиала, Департаментом информационной безопасности ИА Общества и филиалом АО «СО ЕЭС» - «Московское РДУ». (в случае организации обмена информацией с филиалом АО «СО ЕЭС» - «Московское РДУ»).

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:

- Лицензии ФСТЭК на деятельность по технической защите конфиденциальной информации согласно п. д) ст.4 Положения введенного Постановлением Правительства РФ 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».

Директор департамента
информационной безопасности



В.А. Краснокутский