

Приложение 1
к приказу ПАО «Россети»
от 28.08.2020 № 391

МЕТОДИКА ПАО «РОССЕТИ»

проведения проверки цифрового оборудования и систем на соответствие требованиям безопасности информации, в том числе проведения проверки качества технических средств защиты информации в электросетевом комплексе

Москва
2020

1. ОБЩИЕ ПОЛОЖЕНИЯ.

1.1. Настоящая Методика проведения проверки цифрового оборудования и систем на соответствие требованиям безопасности информации в электросетевом комплексе, в том числе проверки качества технических средств защиты информации (далее - Методика) является внутренним документом ПАО «Россети» (далее - Общество).

1.2. Настоящая Методика определяет состав и функции участников проверки, правила и процедуру проверки цифрового оборудования и систем на соответствие требованиям безопасности информации в электросетевом комплексе, в том числе проверки технических средств защиты информации (далее – ТСЗИ) на совместимость с автоматизированными системами технологического управления (далее – АСТУ), и предназначенных для применения в составе объектов критической информационной инфраструктуры (далее - ОКИИ) дочерних обществ ПАО «Россети» (далее - ДЗО Общества), осуществляющих деятельность по передаче и распределению электрической энергии (в т.ч. передачу электроэнергии посредством использования объектов ЕНЭС), а также процедуру оценку производственных площадок.

1.3. В отношении ДЗО Общества настоящая Методика содержит положения рекомендательного характера с описанием процесса взаимодействия Общества и ДЗО при организации работы по вопросам проведения проверки цифрового оборудования и систем на соответствие требованиям безопасности информации в электросетевом комплексе, в том числе проверки ТСЗИ на совместимость с АСТУ на этапах приемки ОКИИ (подсистемы безопасности ОКИИ) в эксплуатацию.

1.4. Проверка цифрового оборудования и систем на соответствие требованиям безопасности информации в электросетевом комплексе, в том числе проверка ТСЗИ на совместимость с АСТУ, проводится в соответствии с Положением ПАО «Россети» о единой технической политике в электросетевом комплексе, утвержденным решением Совета директоров ПАО «Россети» (протокол от 07.10.2019 г. № 378), Методикой ПАО «Россети» проведения проверки качества (аттестации) оборудования, материалов и систем в электросетевом комплексе, утвержденной приказом ПАО «Россети» от 28.07.2020 №329.

1.5. Проверка направлена на повышение надежности и безопасности ОКИИ ДЗО Общества за счет поставки цифрового оборудования и систем обладающих минимальным набором встроенных функций безопасности, а также соответствующих по своим функциональным характеристикам требованиям НТД в области безопасности информации и условиям применения, в том числе совместимых с АСТУ.

1.6. Поставленные цели достигаются путем решения следующих основных задач:

- проведение оценки соответствия цифрового оборудования и систем на всех этапах жизненного цикла;
- проведение оценки процессов разработки программного обеспечения и производства цифрового оборудования и систем, процессов поддержки программного обеспечения;
- актуализация требований Положения ПАО «Россети» о единой технической политике в электросетевом комплексе по результатам опытно-промышленной эксплуатации цифрового оборудования и систем, ТСЗИ.

1.7. В рамках настоящей Методики проверка охватывает следующие формы

оценки соответствия:

- внутренние испытания;
- подтверждение соответствия в форме добровольной сертификации;
- подтверждение соответствия в форме обязательной сертификации ФСТЭК России;
- приемка перед вводом в эксплуатацию.

1.8. Объектами проверки являются:

- цифровое оборудование и системы, перечень которых приведен в приложении 1 к Методике.
- ТСЗИ, перечень которых приведен в приложении 2 к Методике.

Проверка может быть проведена по видам цифрового оборудования и систем, не включенного в приложение 1 к Методике, на основании заявки со стороны организации, предприятия-изготовителя, подрядчика, поставщика, официального представителя зарубежной фирмы в Российской Федерации, при условии одобрения со стороны Заказчика.

1.9. Проверка проводится:

- в отношении цифрового оборудования и систем, ранее не проходивших оценку соответствия и предлагаемого к применению в составе ОКИИ на объектах ДЗО Общества;

- в отношении цифрового оборудования и систем, в аппаратные и(или) программные компоненты которых были внесены конструктивные, функциональные и другие изменения, существенно влияющие на встроены функции безопасности информации;

- в отношении ТСЗИ предлагаемых к применению в составе подсистемы безопасности ОКИИ на объектах ДЗО Общества.

1.10. Цифровое оборудование и системы, ТСЗИ проходят оценку соответствия в форме обязательной сертификации в случаях, установленных законодательством Российской Федерации, в также в случае принятия соответствующего решения Обществом.

1.11. В иных случаях, проверка цифрового оборудования и систем, совместимости ТСЗИ проходит в форме внутренних испытаний (приемки), подтверждения соответствия в форме добровольной сертификации.

1.12. Требования по безопасности информации, оцениваемые в рамках проверки, изложены в приложении 3 настоящей Методики.

1.13. В порядке исключения решение о применении в составе ОКИИ на объектах ДЗО Общества не проверенного ранее цифрового оборудования и систем, ТСЗИ принимается на основании решения Комиссии по допуску оборудования, материалов и систем ДЗО, в том числе в случае применения инновационного оборудования в формате приемки перед вводом в эксплуатацию.

1.14. Испытания (приемка) цифрового оборудования и систем, ТСЗИ проводится Обществом (или уполномоченной организацией) самостоятельно или с привлечением организаций, имеющих в соответствии с законодательством Российской Федерации лицензии на деятельность в области защиты информации в порядке, предусмотренной настоящей Методикой.

1.15. При проведении проверки результаты оценки соответствия требованиям по безопасности информации в зарубежных системах сертификации могут быть приняты Обществом. Решение об их признании принимается на этапе анализа представленных документов (4-й этап Проверки настоящей Методики).

1.16. Настоящая Методика распространяется на всех участников процесса Проверки.

1.17. Ответственным за разработку и актуализацию настоящей Методики является Заместитель Генерального директора по безопасности ПАО «Россети».

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ.

Автоматизированная система технологического управления (АСТУ) – совокупность технических и программных средств, предназначенных для автоматизации управления технологическими процессами электросетевого комплекса.

Проверка - инструмент реализации Положения ПАО «Россети» о единой технической политике в электросетевом комплексе, основанный на оценке соответствия функциональных показателей предлагаемого к использованию на объектах электросетевого хозяйства ДЗО ПАО «Россети» цифрового оборудования, систем и ТСЗИ требованиям нормативно-технических документов и дополнительным требованиям электросетевого комплекса в области безопасности информации, отражающим условия применения и возможности использования на объектах ДЗО Общества.

Комиссия по проверке (Аттестационная комиссия) - группа работников, формируемая Исполнителем и утверждаемая Заказчиком. В состав аттестационной комиссии входят представители исполнительного аппарата Общества, ДЗО Общества, Исполнителя, представители научно-исследовательских, проектных институтов и других организаций и экспертов, привлеченных для проведения Проверки.

Депозитарий - организация, уполномоченная ПАО «Россети» для создания, ведения и актуализации (поддержания) архива документов аттестационных комиссий и Портала ПАО «Россети» по Проверке.

Заключение аттестационной комиссии (ЗАК) - документ, подтверждающий возможность применения цифрового оборудования и систем, в том числе ТСЗИ в составе АСТУ, на объектах ДЗО Общества в заданных условиях эксплуатации.

Заказчик - структурное подразделение исполнительного аппарата ПАО «Россети», осуществляющее общее руководство и контроль за проведением Проверки.

Заявитель – организация, зарегистрированная на территории РФ, (предприятие-изготовитель, подрядчик, поставщик, официальный представитель зарубежной фирмы в Российской Федерации), подавшая заявку в ПАО «Россети» на проведение проверки.

Исполнитель - экспертная организация, уполномоченная ПАО «Россети» на проведение внутренних испытаний.

Нормативно-техническая документация (НТД) - номенклатура государственных, межгосударственных и зарубежных стандартов, отраслевых стандартов и стандартов организации (СТО) и организационно-распорядительных документов Общества в области защиты информации обязательных для применения на объектах электросетевого хозяйства ДЗО Общества.

Перечень цифрового оборудования и систем, в том числе технических средств защиты информации совместимых с автоматизированными системами управления, рекомендованных к применению в составе ОКИИ на объектах

ДЗО Общества (далее - Перечень) - совокупность цифрового оборудования, систем и технических средств защиты информации, прошедших процедуру Проверки, и имеющих заключение аттестационной комиссии, срок действия которого не приостановлен (не прекращен), и рекомендованных к применению в составе ОКИИ на объектах электросетевого хозяйства ДЗО Общества. Перечень размещается на сайте ПАО «Россети» в разделе «ИНВЕСТИЦИИ И ИННОВАЦИИ → Единая техническая политика → АТТЕСТАЦИЯ».

Плановая инспекционная проверка состояния производства (ИПП) – проверка состояния производства цифрового оборудования, систем и технических средств защиты информации с участием представителей Исполнителя, представителей Общества и/или ДЗО, проводимая на периодической основе в целях подтверждения соответствия продукции требованиям по безопасности информации, отсутствия изменений ТУ, отсутствия технологических изменений процесса производства, отсутствия замены комплектующих аттестованной продукции и контроля проведения периодических испытаний.

Производитель цифрового оборудования, систем и технических средств защиты информации – предприятие, организация, компания, лицо, производящее, изготавливающее цифровое оборудование, системы и технические средства защиты информации на производственной площадке, принадлежащей этому лицу на любом законном основании.

Протокол предварительного рассмотрения документации - документ, оформляемый Исполнителем по результатам анализа комплектности представленных Заявителем на Проверку документов.

Протокол испытаний – документ с результатами оценки соответствия, проведенной в Обществе.

Принятие результатов оценки соответствия – использование результатов оценки соответствия цифрового оборудования и систем, проведенной сторонней организацией, в том числе зарубежными организациями, в которых правила и процедура оценки соответствия аналогична настоящей Методике.

Признание результатов оценки соответствия – признание достоверности результата оценки соответствия, проведенной в системе Сертификации ФСТЭК России, ФСБ России или в системе добровольной сертификации АО «НТЦ ФСК».

Стандарт организации (СТО) - внутренний нормативный документ Общества (ДЗО Общества) в сфере стандартизации, который регламентирует свод правил, требований и норм к объекту Проверки с учетом специфики применения цифрового оборудования, систем и технических средств защиты информации на объектах электросетевого хозяйства ДЗО Общества.

Технические условия (ТУ) – технический документ на продукцию, разрабатываемый разработчиком (изготовителем), и содержащий полный комплекс технических требований к продукции, ее изготовлению, контролю и приемке.

Технические требования (ТТ) - совокупность параметров и характеристик для определенного вида и типа цифрового оборудования, систем и ТСЗИ на соответствие которым проводится проверка цифрового оборудования и систем, в том числе проверка ТСЗИ на совместимость с АСТУ, с учетом требований государственных стандартов, отраслевых стандартов, стандартов организации в области защиты информации.

Типопредставитель – это представитель типа или серии конкретного вида оборудования, результаты испытаний которого могут быть распространены на

оборудование данного или другого типа (серии). Правила выбора типопредставителя указываются в соответствующих стандартах по видам оборудования на конкретные виды испытаний.

Экспертная организация - организация, привлекаемая Исполнителем для проведения внутренних испытаний.

Цифровое оборудование – аппаратно-программный комплекс, предназначенный для получения по цифровым интерфейсам информации и ее обработки в цифровой форме, используя цифровые технологии.

3. УЧАСТНИКИ ПРОВЕРКИ. ФУНКЦИИ И ОБЯЗАННОСТИ.

3.1. Участниками проверки являются:

- Заместитель Генерального директора по безопасности ПАО «Россети»;
- заказчик – Департамент обеспечения безопасности ПАО «Россети»;
- представители структурных подразделений исполнительного аппарата ПАО «Россети», ДЗО Общества, других организаций, осуществляющих деятельность в сфере электроэнергетики, привлекаемые к проведению Проверки;
- аттестационные комиссии;
- исполнитель;
- экспертные организации;
- заявитель;
- депозитарий.

3.2. Заместитель Генерального директора по безопасности ПАО «Россети»:

- осуществляет общее руководство Проверкой;
- согласовывает (утверждает) ОРД по Проверке и осуществляет общий контроль за его реализацией;
- утверждает требования Общества по безопасности информации к проверяемому цифровому оборудованию, системам и техническим средствам защиты информации;
- утверждает ЗАК и, при необходимости, согласовывает ТУ;
- прекращает (приостанавливает) срок действия ЗАК, при необходимости отзывает согласующую подпись с ТУ путем выпуска писем об отзыве, аннулировании или возобновлении действия ЗАК или ТУ.

3.3. Заказчик:

- осуществляет оперативное руководство Проверкой;
- принимает и рассматривает заявки на Проверку или на проведение ИПП, необходимости Проверки, выбора варианта Проверки, а также комплектности документов, предоставленных Заявителем для проведения Проверки;
- в случае нецелесообразности проведения Проверки направляет мотивированный отказ в адрес Заявителя;
- согласовывает и утверждает технические требования по безопасности информации к цифровому оборудованию и системам и программы (методики) испытаний;
- утверждает составы Аттестационных комиссий, учитывая требования, предъявляемые к квалификации членов Аттестационной комиссии, и полноту состава аттестационной комиссии для принятия объективных решений;
- согласовывает ЗАК, внесение дополнений и изменений к ЗАК по представлению Исполнителя;
- утверждает акт инспекционной проверки производства;

- направляет утвержденные ЗАК, Технические требования, дополнения и изменения к ЗАК в Депозитарий;
- по запросу представляет в ДЗО копию полнотекстового ЗАК;
- разрабатывает и представляет на утверждение Заместителю Генерального директора по безопасности ПАО «Россети» организационно-распорядительные документы и формы документов по Проверке и предложения по ее совершенствованию;
- осуществляет контроль соблюдения сроков и процедуры Проверки путем ведения специализированного файла учета цифрового оборудования, систем и технических средств защиты информации проходящего процедуру Проверки, в т.ч. с учетом необходимости продлений и внесения дополнений и изменений в ЗАК (при необходимости в ТУ), формируемого на основе информации, получаемой от Исполнителя;
- поддерживает в актуальном состоянии Перечень;
- осуществляет мониторинг работы цифрового оборудования, систем и технических средств защиты информации, при необходимости, готовит предложения об отзыве или приостановке действия ЗАК;
- рассматривает апелляции Заявителей;
- вырабатывает механизмы взаимодействия с Заявителями с целью обеспечения своевременного прохождения Проверки; осуществляет контроль исполнения обязательств Заявителей;
- разрабатывает мероприятия по повышению прозрачности системы Проверки;
- принимает участие (очно или заочно) в работе Аттестационной комиссии с правом блокирующего голоса.

Заказчик несет ответственность за:

- проведение Проверки в соответствии с действующими ОРД;
- совершенствование системы Проверки;
- оформление материалов работы АК.

3.4. Представители структурных подразделений Общества и ДЗО Общества:

- анализируют опыт эксплуатации цифрового оборудования и систем, в том числе ТСЗИ совместно с АСТУ, используемого в составе ОКИИ на объектах ДЗО Общества, и передают Заказчику данные о выявленных недостатках и дефектах;
- делегируют своих представителей для работы в составе АК.

Кроме того, профильные структурные подразделения Общества и ДЗО Общества, при необходимости:

- согласовывают ТТ к цифровому оборудованию и системам, в том числе к совместимости ТСЗИ с АСТУ и программы (методики) испытаний ;
- в случае необходимости направляют предложения по актуализации ТТ по видам цифрового оборудования и систем, в том числе по видам ТСЗИ в составе АСТУ.

Структурные подразделения Общества, структурные подразделения ДЗО Общества несут ответственность за:

- делегирование экспертов для участия в процедуре Проверки по видам цифрового оборудования, систем и технических средств защиты информации, в соответствии функциональным направлением привлекаемого структурного подразделения;
- качество экспертизы представленных материалов и качество проведенных

испытаний по утвержденной программе (методике) испытаний ДЗО Общества.

3.5. Исполнитель:

- направляет запросы Заявителю о подтверждении срока и готовности прохождения Проверки;
- готовит, корректирует и направляет утвержденный протокол предварительного рассмотрения документации Заявителю;
- подготавливает и направляет на утверждение Заказчику составы аттестационных комиссий по проверке требований безопасности информации по всем видам цифрового оборудования и систем, в том числе по видам ТСЗИ, применяемых в составе ОКИИ на объектах электросетевого комплекса;
- формирует ТТ к цифровому оборудованию и системам, в том числе к ТСЗИ, в рамках каждой Проверки;
- в отдельных случаях разрабатывает совместно с Заявителем и согласовывает с представителями ДЗО Общества программу (методику) испытаний по проверке требований безопасности информации цифрового оборудования и систем, в том числе по проверке ТСЗИ на совместимость с АСТУ, представленного на Проверку;
- в отдельных случаях организует проведение испытаний по проверке требований безопасности информации цифрового оборудования и систем в лабораториях (собственных, либо в аккредитованных в системе сертификации ФСТЭК России, ФСБ России) с обязательным участием представителей Общества;
- организует проведение испытаний с участием членов АК на стенде Заявителя или предприятия-изготовителя ;
- проводит проверку комплектности материалов, представленных на Проверку;
- организует работу АК;
- организует экспертизу АК материалов Заявителя;
- вносит в повестку заседания АК вопрос о необходимости проведения анализа состояния производства на соответствие ГОСТ Р 56939-2016 «Национальный стандарт Российской Федерации. Защита информации. Разработка безопасного программного обеспечения. Общие требования» (утв. и введен в действие Приказом Росстандарта от 01.06.2016 № 458-ст) и ГОСТ Р ИСО/МЭК 27001-2006 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности» (утв. и введен в действие Приказом Ростехрегулирования от 27.12.2006 № 375-ст);
- организует инспекционную проверку производства (при первичной Проверке);
- организует плановую инспекционную проверку состояния производства продукции (ИПП);
- разрабатывает проекты документов ЗАК, дополнений (изменений) в ЗАК и организует их согласование (утверждение);
- готовит акт плановой инспекционной проверки состояния производства;
- готовит проекты протоколов заседаний АК;
- обеспечивает сопровождение всех материалов работы АК до утверждения ЗАК;
- обеспечивает работников Общества, ответственных за Проверку, доступом к информации, размещенной в Депозитарии;

- ежемесячно готовит и передает Заказчику отчет о ходе проведения Проверки.

Исполнитель несет ответственность за:

- сроки проведения Проверки;
- объективную оценку представленных материалов;
- оформление материалов работы АК;
- организацию плановых инспекционных проверок производства и оформление соответствующих актов.

Исполнитель вправе привлекать для проведения Проверки и инспекционных проверок экспертные организации и экспертов на договорной основе.

3.6. Заявитель:

- подает заявку с перечнем документов для проведения Проверки в соответствии с п. 4. настоящей Методики;
- представляет дополнительную информацию, запрашиваемую АК в рамках проводимой Проверки;
- проводит корректировку технической документации по требованию АК;
- проводит дополнительные испытания оборудования по решению АК;
- организует работу членов АК при проведении испытаний с участием членов АК и оценке производства.

Заявитель несет ответственность за:

- полноту, качество и достоверность материалов на цифровое оборудование, системы и технические средства защиты информации, своевременность их представления;
- своевременное проведение плановых инспекционных проверок производства (ИПП).

3.7. Депозитарий организует хранение информации и актуализацию информации на Портале. Отношения с Депозитарием и порядок взаимодействия с ним оформляются договором и определены положениями Методики ПАО «Россети» проведения проверки качества (аттестации) оборудования, материалов и систем в электросетевом комплексе, утвержденной приказом ПАО «Россети» от 28.07.2020 №329.

3.8. Аттестационные комиссии.

АК формируются Исполнителем при первичной Проверке и при последующих Проверках. Заседания АК могут проводиться очно и заочно.

Решение АК считается правомочным, если на ее очном заседании присутствуют не менее половины членов комиссии, а также если в заочном голосовании принимают участие не менее половины членов комиссии. Решения принимаются большинством голосов от числа присутствующих на заседании. При равенстве голосов голос Председателя аттестационной комиссии является решающим.

3.9.1. *Председатель АК* - назначается Заместителем Генерального директора по безопасности ПАО «Россети».

Председатель АК координирует и контролирует работу членов АК.

Председатель АК несет ответственность за своевременное рассмотрение представленных Заявителем документов и правильность принятых решений АК.

3.10.2. *Члены АК*:

- рассматривают материалы, представленные Заявителем и Исполнителем;
- участвуют в испытаниях представленного на Проверку цифрового

оборудования, систем и ТСЗИ по утвержденной программе;

- проводят оценку производства;
- рассматривают проект и подписывают заключение АК.

Члены АК несут дисциплинарную и материальную ответственность за:

- результаты экспертизы материалов Проверки и испытаний цифрового оборудования и систем, в том числе испытаний ТСЗИ на совместимость с АСТУ;
- объективность выводов о целесообразности допуска цифрового оборудования и систем, в том числе ТСЗИ, к применению в проектных решениях вновь сооружаемых, реконструируемых, модернизируемых и ремонтируемых объектов ДЗО Общества;

- нарушение процедуры организации системы Проверки;
- разглашение сведений, определенных ОРД Общества (приказ от 30.01.2020 № 37 «Об организации работ по защите информации, составляющей коммерческую тайну ПАО «Россети») как конфиденциальная информация и коммерческая тайна.

3.10.3. Требования к квалификации работников, входящих в состав аттестационных комиссий:

- высшее профильное образование и наличие необходимых квалификационных аттестатов в области электроэнергетики, в области защиты информации;

- опыт работы по специальности не менее 5 лет;

- знание организационно-распорядительных документов Общества по процедуре Проверки;

- знание объекта Проверки и НТД по направлению.

Исполнитель обязан вести реестр высококвалифицированных работников, входящих в состав аттестационных комиссий, для которых не является обязательным требованием предоставление документов, подтверждающих их квалификацию.

3.10.4. АК дает обоснованные предложения по сроку действия ЗАК с целью снижения возможных последствий применения образцов цифрового оборудования и систем, а также по причине отсутствия положительного опыта эксплуатации цифрового оборудования, систем и технических средств защиты информации в области электроэнергетики на объектах электросетевого комплекса ДЗО Общества.

4. ДОКУМЕНТАЦИЯ, ПОДАВАЕМАЯ С ЗАЯВКОЙ НА ПРОВЕРКУ.

4.1. Для участия в Проверке Заявителем должны быть представлены пакеты документации, включающие:

- сведения о Заявителе и предприятии-изготовителе;

- техническую (эксплуатационную) документацию на цифровое оборудование и системы, ТСЗИ;

- описание состава программного обеспечения и баз данных входящего в состав цифрового оборудования и систем, ТСЗИ;

- сведения о правах интеллектуальной собственности на программное обеспечение и базы данных;

- копии имеющихся российских и международных сертификатов в области безопасности информации на продукцию, сертификатов и заключений по ранее проведенным испытаниям;

- декларацию об отсутствии в программном обеспечении ошибок и общеизвестных уязвимостей, сведения о которых опубликованы в базах данных

информационных ресурсов сети Интернет (ресурсы ФСТЭК России, <https://cve.mitre.org/> и другие).

4.2. Пакет технической документации является основной информационной базой для составления ЗАК. Вся техническая документация должна быть составлена с учетом требований НТД и представлена на русском языке.

4.3. Подробный перечень документации представлен в приложениях 4 и 5 к Методике.

5. ПРОВЕДЕНИЕ ПРОЦЕДУРЫ ПРОВЕРКИ.

5.1. ПОДГОТОВКА ЗАК .

5.1.1. Подготовка ЗАК осуществляется в результате проведения:

- экспертизы документации, представленных Заявителем на Проверку;
- оценки состояния производства;
- испытаний цифрового оборудования и систем, в том числе ТСЗИ на совместимость с АСТУ .

5.1.1.1. Оценка состояния производства проводится в случаях:

- первичной Проверки;
- при модернизации выпускаемой продукции и (или) технологий производства, внесении изменений в технологию производства, которые могут повлиять на соответствие цифрового оборудования и систем, в том числе на совместимость ТСЗИ с АСТУ, техническим требованиям Заказчика по безопасности информации;
- по результатам анализа технологических нарушений цифрового оборудования и систем, в том числе вызванных не совместимостью ТСЗИ с АСТУ, на объектах ДЗО Общества на основании актов расследования технологических нарушений.

По результатам оценки состояния производства составляется акт по форме Приложения 13 настоящей Методики, свидетельствующий о наличии у производителя необходимых условий производства для обеспечения соответствия выпускаемой продукции установленным государственным и отраслевым требованиям по безопасности информации.

5.1.1.2. Дополнительные испытания назначаются если:

- Исполнителем при предварительном рассмотрении представленной Заявителем документации выявлено отсутствие определенного вида испытаний на соответствие техническим требованиям Заказчика;
- членами Аттестационной комиссии выявлено несоответствие проведенных Заявителем испытаний методике, установленной в НТД, либо недостаточность подтверждения технических параметров.

5.1.2. Результатом работы АК является ЗАК (положительное или отрицательное):

- при положительном ЗАК цифровое оборудование и системы, ТСЗИ, рекомендуется для применения в составе ОКИИ на объектах ДЗО Общества без ограничений, либо в ЗАК указываются ограничения применения по условиям эксплуатации, сроку действия ЗАК;

- при отрицательном ЗАК цифровое оборудование и системы, ТСЗИ, не прошедшее Проверку, не рекомендуются для применения в составе ОКИИ на объектах ДЗО Общества, а Заявитель, после устранения несоответствий техническим требованиям, выявленных в процессе Проверки, имеет право на

повторную Проверку.

5.2. ВНЕСЕНИЕ ИЗМЕНЕНИЙ, ДОПОЛНЕНИЙ В ЗАК.

5.2.1. Изменения и дополнения в ЗАК вносятся при проведении повторной Проверки.

5.2.2. Дополнительная Проверка цифрового оборудования, систем и ТСЗИ, проводится в следующих случаях:

- изменения НТД;
- по результатам анализа технологических нарушений цифрового оборудования и систем, в том числе нарушений совместимости ТСЗИ с АСТУ, на объектах ДЗО Общества на основании актов расследования технологических нарушений и дефектов, связанных как с конструктивными недоработками, так и с качеством производства;
- внесение конструктивных, функциональных и других изменений в цифровое оборудование, системы и ТСЗИ, существенно влияющие на состояние безопасности;
- при отрицательном акте плановой инспекционной проверки состояния производства.

5.2.3. В случае изменений в НТД и ТТ Заказчик обязан разместить информацию на соответствующем корпоративном сайте.

5.2.4. По результатам анализа технологических нарушений цифрового оборудования и систем, в том числе нарушений совместимости ТСЗИ с АСТУ, эксплуатируемых в составе ОКИИ на объектах ДЗО Общества, и выявления дефектов, связанных как с конструктивными недоработками, так и с качеством изготовления, или при отрицательном акте плановой инспекционной проверки состояния производства Заказчик обязан:

- разместить информацию на соответствующем корпоративном сайте;
- создать рабочую группу для анализа причин произошедших отказов;
- известить Заявителя официальным письмом о выявленных конструктивных дефектах и направлении рабочей группы.

При этом, Заявитель обязан дать заключение о причинах технологических нарушений, известить о характере конструктивных, технологических доработок, представить программу испытаний и протоколы испытаний. Если характер изменений и доработок требует проведения значительного объема типовых испытаний, должна быть назначена повторная Проверка данного оборудования.

5.2.5. В случае инициативного внесения изменений в конструкцию, технологию, программное обеспечение цифрового оборудования и систем, в том числе в ТСЗИ Заявитель в течении трех месяцев с момента внесения изменений направляет заявку на внесение изменений/дополнений в адрес Заказчика с указанием изменений, внесенных в цифровое оборудование и системы, в том числе в ТСЗИ и в техническую документацию, отражающую эти изменения. Заявитель декларативно подтверждает успешное выполнение повторных испытаний в объеме ранее выполненной проверке.

5.2.6. Рассмотрение изменений, внесенных в цифровое оборудование и систему, включая в ТСЗИ в составе АСТУ, осуществляется Исполнителем с привлечением, при необходимости, других участников Проверки и с последующим согласованием и утверждением ЗАК с изменениями, дополнениями.

5.2.7. В зависимости от характера внесенных изменений могут быть приняты

следующие решения:

- оформлено новое ЗАК и на его основании, согласовано извещение об изменении ТУ;
- оформлено дополнение к ЗАК и на его основании, согласовано извещение об изменении ТУ (при условии ранее согласованных ТУ);
- оформлено дополнение к ЗАК и на его основании, согласовано скорректированное извещение об изменении ТУ (при условии ранее согласованных ТУ) с изменением условий эксплуатации;
- отказ от внесения дополнений к ЗАК и на его основании отказ согласования извещения об изменении ТУ в связи с несоответствием ТТ;
- отказ от внесения дополнений к утвержденному ЗАК и на его основании отказ согласования извещения об изменении ТУ с предложением пройти процедуру повторной Проверки.

Дополнения к ЗАК оформлено только после представления протоколов типовых испытаний, технической документации и других необходимых материалов.

5.2.8. Решение о дополнении к заключению или отказе внесения дополнений в ЗАК формулируется Исполнителем, согласовывается и утверждается Заказчиком и направляется в адрес Заявителя и Депозитарий вместе с соответствующей документацией.

5.3. ПЛАНОВАЯ ИНСПЕКЦИОННАЯ ПРОВЕРКА СОСТОЯНИЯ ПРОИЗВОДСТВА ПРОДУКЦИИ (ИПП) ПРОШЕДШЕЙ ПРОВЕРКУ

5.3.1. ИПП должна проводиться в срок не реже 1 раза в 5 лет, если иное не оговорено в ЗАК на основании решения аттестационной комиссии (но не более 5 лет). Срок исчисляется с момента выдачи ЗАК или с даты утверждения предыдущего акта ИПП.

5.3.2. Проведение ИПП осуществляется Исполнителем, проводившим первичную Проверку данного цифрового оборудования и систем.

5.3.3. Проведение ИПП осуществляется за счет Заявителя и оформляется соответствующим договором между Заявителем и Исполнителем. Затраты на переезд и проживание членов инспекционной комиссии (не более 3х человек) оплачиваются Заявителем.

5.3.4. Проведения ИПП оформляется соответствующим актом (приложение 13 настоящей Методики), подготовленным Исполнителем и согласовывается/утверждается Заказчиком.

5.3.5. Заявка на проведение ИПП подается Заявителем за 3 (три) месяца до очередного срока в адрес Заказчика в свободной форме на бланке письма Заявителя с указанием номера ЗАК, наименования аттестованного цифрового оборудования и систем, ТСЗИ и адреса производства.

5.3.6. Исполнитель по согласованию с Заявителем и Заказчиком определяет возможные сроки проведения ИПП, при этом ИПП должна быть проведена в срок не позднее 3х месяцев с момента поступления заявки на ИПП от Заявителя.

5.3.7. По согласованию с Заказчиком допускается одновременное проведение ИПП на несколько видов продукции, имеющих отдельные ЗАК.

5.3.8. По согласованию с Заказчиком допускается проведение ИПП в удаленном режиме с использованием современных средств и приложений видеосвязи.

5.3.9. Отсутствие акта плановой проверки состояния производства,

отрицательный акт ИПП или отказ Заявителя в проведении ИПП является основанием для прекращения действия ЗАК.

5.3.10. Ответственность за своевременную организацию проведения плановой инспекционной проверки производства несет Заявитель.

5.4. ПРОДЛЕНИЕ СРОКА ДЕЙСТВИЯ ЗАКЛЮЧЕНИЯ АТТЕСТАЦИОННОЙ КОМИССИИ.

5.4.1. Продление срока действия заключения аттестационной комиссии проводится на основании заявки и документов, представленных Заявителем в Общество.

5.4.2. Рассмотрение заявок на продление срока действия ЗАК осуществляется Исполнителем по представлению Заказчика с привлечением, при необходимости, других участников Проверки.

5.4.3. Решение о продлении оформляется на основе анализа представленной документации и опыта эксплуатации в соответствии с Методикой. Результатом является выдача протокола продления и, при необходимости, на его основании проводится согласование извещения об изменении ТУ.

5.4.4. Решение о продлении срока действия ЗАК принимает Заказчик. Решение направляется в Депозитарий с соответствующими документами, информация о новом сроке действия ЗАК размещается на сайте Общества.

5.4.5. Заявитель направляет в Общество заявку на продление срока действия ЗАК за 3 месяца до указанного в ЗАК срока.

5.4.6. Срок действия протокола продления не ограничивается. При наличии рекомендаций АК о проведении дополнительных испытаний срок действия устанавливается до проведения соответствующих испытаний.

5.5. ПРЕКРАЩЕНИЕ ДЕЙСТВИЯ ЗАК.

5.5.1. Решение о прекращении действия ЗАК принимается Заказчиком в следующих случаях:

- по выявленным в процессе эксплуатации конструктивным и технологическим недостаткам;
- при нарушении технологии производства, исключения функций безопасности из конструкции, технологии, программного обеспечения цифрового оборудования, систем и ТСЗИ без официального уведомления Заявителем или производителем проверенного ранее цифрового оборудования и систем, ТСЗИ;
- при отсутствии сервисного обслуживания программного обеспечения цифрового оборудования, систем и ТСЗИ, которое должно выполняться по условиям его эксплуатации;
- при переносе производственной площадки за пределы территории Российской Федерации;
- при прекращении производства цифрового оборудования, систем и ТСЗИ;
- в случае инициативного обращения заявителя (производителя);
- при отрицательном акте плановой проверки состояния производства;
- при отказе Заявителя на проведение плановой проверки состояния производства.

5.5.2. Уведомление о досрочном прекращении действия ЗАК с подписью Заместителя Генерального директора по безопасности ПАО «Россети» направляется в адрес Заявителя или производителя, в Депозитарий, а также другим

заинтересованным организациям.

5.5.3. При принятии решения о прекращении действия ЗАК, либо по окончании срока действия ЗАК, наименование типа цифрового оборудования, систем и ТСЗИ исключается Заказчиком из Перечня, рекомендованного к применению на объектах ДЗО Общества цифрового оборудования, систем и ТСЗИ, и размещенного на сайте Общества.

6. СРОК ДЕЙСТВИЯ ЗАКЛЮЧЕНИЯ АТТЕСТАЦИОННОЙ КОМИССИИ.

6.1. Срок действия ЗАК не ограничивается. При наличии рекомендаций АК о проведении дополнительных испытаний срок действия может быть ограничен до проведения соответствующих испытаний. При наличии обоснованных предложений членов АК срок действия может быть выбран из ряда от одного до пяти лет. Для продления срока действия ЗАК должна быть проведена процедура продления срока действия ЗАК согласно п.9.5. настоящей Методики.

7. ПОРЯДОК ПОДАЧИ И РАССМОТРЕНИЯ АПЕЛЛЯЦИЙ.

7.1. Апелляция на действия АК и Исполнителя процедуры проверки направляется Заявителем на имя Заместителя Генерального директора по безопасности ПАО «Россети».

7.2. В течение 15 рабочих дней Заказчик рассматривает поданную апелляцию и официально извещает о принятом решении сторону, подавшую заявку на апелляцию.

8. ПОРЯДОК РАЗМЕЩЕНИЯ ИНФОРМАЦИИ НА САЙТЕ ОБЩЕСТВА.

Размещение информации на сайте Общества регулируется положениями Методики ПАО «Россети» проведения проверки качества (аттестации) оборудования, материалов и систем в электросетевом комплексе, утвержденной приказом ПАО «Россети» от 28.07.2020 № 329.

9. ПОРЯДОК ПРОВЕДЕНИЯ ПРОВЕРКИ.

9.1. Проверка выполняется в 5 этапов:

1 этап. Подача заявки.

2 этап. Актуализация перечня Проверки, где указывается информация о текущем состоянии рассмотрения заявок на Проверку, о представленных документах, сроках, а также иная информация, связанная с прохождением Проверки.

3 этап. Разработка технических требований (при необходимости, если отсутствует нормативно-технические документы и требования электросетевого комплекса в области безопасности информации), предварительное рассмотрение документации, представленных для Проверки, и в случае необходимости, программы и методики испытаний.

4 этап. Анализ представленных документов, при необходимости - подготовка и проведение испытаний. Подготовка и утверждение ЗАК, подтверждающего (или не подтверждающего) возможность применения цифрового оборудования и систем, ТСЗИ, в составе ОКИИ на объектах ДЗО Обществ.

5 этап. Формирование и актуализация Перечня цифрового оборудования и систем, в том числе ТСЗИ, рекомендованных к применению в составе ОКИИ на объектах ДЗО Общества.

9.2. ПОДАЧА ЗАЯВКИ.

Порядок подачи заявки на Проверку и сроки актуализации перечня Проверки приведены в таблице 1.

Корректировка перечня Проверки проводится Исполнителем по согласованию с Заказчиком.

При выдаче Исполнителем отрицательного протокола комплектности или отрицательного ЗАК, перечень Проверки корректируется, а процедура Проверки возобновляется без учета предыдущих планируемых сроков проведения Проверки.

Предложения Исполнителя по корректировке перечня Проверки направляются Заказчику не реже одного раза в месяц.

Если через 3 месяца после направления Исполнителем запросов Заявителю о подтверждении срока и готовности к прохождению Проверки ответа от Заявителя не последовало, то Заявка на Проверку аннулируется, о чем Исполнитель письменно информирует Заявителя.

Таблица 1

№ п/п	Содержание работы	Ответственный участник	Срок выполнения
1.	Направление в ПАО «Россети» Заявки по форме приложения 6 к настоящей Методике с пакетом документов (приложение 7 к настоящей Методике при продлении и приложение 8 к настоящей Методике при внесении изменений (дополнений))	Заявители	постоянно, за 30 рабочих дней до планируемого срока начала Проверки
2.	Рассмотрение Заявки на предмет: - необходимости его Проверки (проверка включения данного вида продукции в перечень оборудования, подлежащего Проверки); - наличие документов, предоставляемых Заявителем для проведения Проверки	Заказчик	2 рабочих дня с даты поступления Заявки
3.	Принятие решения о целесообразности / нецелесообразности проведения Проверки	Заказчик	2 рабочих дня с даты принятия решения о целесообразности / нецелесообразности проведения Проверки
3.1	В случае нецелесообразности проведения Проверки направление мотивированного отказа в адрес Заявителя		
3.2	В случае целесообразности проведения Проверки направление письма-поручения (резолуции в АСУД) о проведении Проверки Исполнителю		
4.	Направление запросов Заявителю о подтверждении срока и готовности к	Исполнитель	2 рабочих дня с даты получения поручения от Заказчика

№ п/п	Содержание работы	Ответственный участник	Срок выполнения
	прохождению Проверки ¹		
5.	Направление предложений Заказчику об изменении Перечня	Исполнитель	Ежемесячно, до 10 числа следующего месяца

9.3. РАССМОТРЕНИЕ ЗАЯВКИ.

Порядок и сроки рассмотрения материалов для проведения Проверки (этап 3) указаны в таблице 2.

Таблица 2

№ п/п	Содержание работы	Ответственный участник процедуры	Срок
1.	Заключение договора на организацию Проверки ² .	Исполнитель, Заявитель	
2.	Проведение анализа представленных Заявителем документов на предмет комплектности и актуальности. Подготовка Протокола предварительного рассмотрения документации (приложение 12 к настоящей Методике).	Исполнитель	15 рабочих дней с даты начала действия договора (в зависимости от сложности оборудования срок может быть увеличен, но не более чем на 10 рабочих дней)
3.	Согласование актуальности и комплектности предоставленных Заявителем документов, утверждение Протокола предварительного рассмотрения документации.	Исполнитель	2 рабочих дня с даты разработки Протокола предварительного рассмотрения документации
4.	Направление утвержденного Протокола предварительного рассмотрения документации Заявителю в соответствии с условиями договора и Заказчику ³ .	Исполнитель	2 рабочих дня с даты получения утвержденного Протокола предварительного рассмотрения документации
5.	При отсутствии общих технических требований по виду цифрового оборудования и систем, включая ТСЗИ, разработка проекта ТТ.	Исполнитель	15 рабочих дней с даты начала действия договора (в зависимости от сложности оборудования срок может быть увеличен)
6.	Согласование, подписание проекта ТТ и направление Заказчику посредством АСУД с приложением сканированной копии и на бумажном носителе.	Исполнитель	3 рабочих дня с даты разработки проекта ТТ
7.	Согласование проекта ТТ Заказчиком на предмет соответствия государственным и отраслевым требованиям и дополнительным требованиям Обществ.	Исполнитель	5 рабочих дней с даты получения проекта ТТ
8.	Доработка проекта ТТ по замечаниям Заказчика.	Исполнитель	3 рабочих дня с даты получения замечаний и предложений

¹ в случае отсутствия подтверждения от Заявителя в течение 30 календарных дней с даты направления Исполнителем запроса о готовности к прохождению Проверки, заявка на проведение Проверки исключается из перечня Проверки.

² Если договор на Проверку не заключается Заявителем более 30 календарных дней, то заявка исключается, о чем Исполнитель уведомляет Заявителя письменно.

³ В случае положительного Протокола предварительного рассмотрения документации проводится следующий этап, подготовка и утверждение ЗАК.

№ п/п	Содержание работы	Ответственный участник процедуры	Срок
9.	Утверждение ТТ и направление в Депозитарий.	Заместитель Генерального директора по безопасности ПАО «Россети», Заказчик	7 рабочих дней с даты получения согласованных ТТ
10.	Предоставление Исполнителю недостающей документации.	Заявитель	10 рабочих дней с даты получения утвержденного отрицательного Протокола предварительного рассмотрения документации
11.	Корректировка Протокола предварительного рассмотрения документации с учетом предоставленной Заявителем документации, согласование и утверждение.	Исполнитель	10 рабочих дней с даты получения недостающей документации
12.	Направление скорректированного утвержденного Протокола предварительного рассмотрения документации Заявителю в соответствии с условиями договора и Заказчику.	Исполнитель	2 рабочих дня с даты получения утвержденного Протокола предварительного рассмотрения документации

9.4. ПОДГОТОВКА И УТВЕРЖДЕНИЕ ЗАКЛЮЧЕНИЯ АТТЕСТАЦИОННОЙ КОМИССИИ.

Порядок и сроки подготовки и утверждения заключения аттестационной комиссии (этап 4) указаны в таблице 3.

Таблица 3

№ п/п	Содержание работы	Ответственный участник процедуры	Срок
1.	Формирование состава комиссии и направление на согласование Заказчику	Исполнитель	5 рабочих дней с даты утверждения положительного Протокола предварительного рассмотрения документации
2.	Утверждение состава аттестационной комиссии. (по форме Приложения 9 к настоящей Методике)	Заместитель Генерального директора по безопасности ПАО «Россети», Заказчик	2 рабочих дня с даты формирования состава комиссии
3.	Направление комплекта документации членам аттестационной комиссии для подготовки отчета	Исполнитель	5 рабочих дней с даты утверждения состава аттестационной комиссии
4.	Подготовка отчета по представленной документации и направление Исполнителю	Члены Аттестационной комиссии	10 рабочих дней с даты получения документации
5.	Подготовка и передача Заявителю обобщенных замечаний членов аттестационной комиссии по документации	Исполнитель	7 рабочих дней с даты получения замечаний от членов аттестационной комиссии

№ п/п	Содержание работы	Ответственный участник процедуры	Срок
6.	Предоставление Исполнителю уточнений (документов) по полученным замечаниям	Заявитель	15 рабочих дней с даты получения перечня замечаний членов аттестационной комиссии
7.	Подготовка проекта заключения (приложение 11 к настоящей Методике) с учетом полученных от Заявителя уточнений (документов), либо, в случае непредоставления в указанный срок, на основе имеющихся документов и его рассылка членам аттестационной комиссии	Исполнитель	15 рабочих дней с даты получения отчетов от аттестационной комиссии и предоставления ответов Заявителем
8.	Направление членам аттестационной комиссии, официального письма о проведении заседания аттестационной комиссии в очной форме. Письмо направляется посредством АСУД, электронной почты, факсимильной связи.	Исполнитель	2 рабочих дня с даты подготовки проекта ЗАК
9.	<p>Рассмотрение проекта ЗАК, направление замечаний и предложений по его корректировке Исполнителю</p> <p>Оценка необходимости проведения анализа состояния производства. Согласование с Заказчиком необходимости проведения очной проверки технологий производства.</p>	Аттестационная комиссия	5 рабочих дней с даты получения проекта ЗАК
10	В случае принятия решения о необходимости проведения очного анализа состояния производства - согласование и формирование состава рабочей группы, формируемой из представителей Заказчика и Исполнителя, учитывая требования к квалификации членов рабочей группы	Исполнитель Заказчик	3 рабочих дня с даты принятия решения о необходимости проведения анализа состояния производства
11	Направление официального письма о направлении рабочей группы Исполнителю и Заявителю посредством электронной почты, факсимильной связи.	Заместитель Генерального директора по безопасности ПАО «Россети», Заказчик	4 рабочих дня с даты формирования состава рабочей группы

№ п/п	Содержание работы	Ответственный участник процедуры	Срок
12	Анализ состояния производства на соответствие ГОСТ Р 56939-2016 «Национальный стандарт Российской Федерации. Защита информации. Разработка безопасного программного обеспечения. Общие требования» (утв. и введен в действие Приказом Росстандарта от 01.06.2016 № 458-ст) и ГОСТ Р ИСО/МЭК 27001-2006 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности» (утв. и введен в действие Приказом Ростехрегулирования от 27.12.2006 № 375-ст) (при необходимости)	Рабочая группа	5 рабочих дней с даты направления решения о создании рабочей группы
13	Оформление Акта инспекционной проверки состояния производства (Приложение 13 к Методике) и подписание членами рабочей группы	Рабочая группа	2 рабочих дня с даты проведения анализ состояния производства
14	Корректировка проекта заключения по замечаниям членов аттестационной комиссии и, в случае наличия уточняющих запросов, направление Заявителю	Исполнитель	5 рабочих дней с даты получения замечаний и предложений
15.	Предоставление Исполнителю уточнений (документов) по полученным запросам	Заявитель	5 рабочих дней с даты получения запроса от Исполнителя
16.	Корректировка проекта заключения по полученным ответам от Заявителя и подписание членами аттестационной комиссии. В случае несогласия одного из членов комиссии с выводами ЗАК он имеет право подписать документ с «особым мнением». Об особом мнении члена комиссии информируется Заместитель Генерального директора по безопасности при утверждении ЗАК.	Исполнитель	5 рабочих дней с даты получения ответа от Заявителя
17.	Рассмотрение и подписание заключения аттестационной комиссией	Председатель аттестационной комиссии	5 рабочих дней с даты получения проекта ЗАК
18.	Направление подписанного членами аттестационной комиссии и согласованного Исполнителем ЗАК на согласование Заказчику	Исполнитель	2 рабочих дня с даты подписания ЗАК

№ п/п	Содержание работы	Ответственный участник процедуры	Срок
19.	Согласование ЗАК Заказчиком на предмет соответствия цифрового оборудования и систем, в том числе на предмет совместимости ТСЗИ с АСТУ, НТД и дополнительным требованиям Заказчика	Заказчик	5 рабочих дней с даты получения ЗАК на бумажном носителе
20.	Доработка проекта заключения аттестационной комиссии по замечаниям Заказчика	Исполнитель	5 рабочих дней с даты получения замечаний и предложений
21.	Утверждение заключения аттестационной комиссии в ПАО «Россети» (в соответствии с условиями) и, на основании положительного ЗАК	Заместитель Генерального директора по безопасности ПАО «Россети», Заказчик	4 рабочих дня
22.	Внесение изменений в Перечень цифрового оборудования и систем рекомендованного к применению в составе ОКИИ на объектах ПАО «Россети»	Заказчик	5 рабочих дней с даты утверждения ЗАК
23.	Размещение на сайте ПАО «Россети» актуального Перечня цифрового оборудования и систем рекомендованного к применению в составе ОКИИ на объектах ПАО «Россети»	Департамент по связям с общественностью и СМИ ПАО «Россети»	5 рабочих дней с даты утверждения ЗАК
24.	Направление утвержденного ЗАК в Депозитарий	Заказчик	5 рабочих дней с даты утверждения ЗАК
25.	Направление утвержденного ЗАК Заявителю в соответствии с условиями договора	Исполнитель	2 рабочих дня с даты получения утвержденного ЗАК и согласованных ТУ

При выявлении замечаний по несоответствию ТТ, по качеству документации и замечаний по протоколам испытаний, АК предлагает Заявителю провести испытания для подтверждения параметров цифрового оборудования и систем, в том числе совместимости ТСЗИ с АСТУ, при этом необходимо в Протоколе заседания АК записать (форма приведена в приложении 10 к настоящему Порядку): «Приостановить Проверку до представления документов и исключить заявку из перечня Проверки».

Заявитель готовит программу испытаний и, в случае необходимости, согласовывает ее с Исполнителем и Заказчиком.

Результаты испытаний оформляются протоколом испытаний и представляются Заявителем Исполнителю.

Максимальный срок представления протоколов по проводимым испытаниям - не более 2 месяцев. Если Заявитель не представит протоколы испытаний в течение указанной в протоколе даты, то Проверку считать завершенной с отрицательным результатом.

9.5. ПРОДЛЕНИЕ СРОКА ДЕЙСТВИЯ, ВНЕСЕНИЕ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ В ЗАКЛЮЧЕНИЯ АТТЕСТАЦИОННОЙ КОМИССИИ.

Порядок продления срока действия, внесения дополнений и изменений в ЗАК и извещений об изменении ТУ указаны в таблице 4.

Таблица 4

№ п/п	Содержание работы	Исполнитель	Срок
1.	Направление Заявки по форме приложения 7 к настоящей Методике с пакетом документов (приложение 5 к настоящей Методике) в ПАО «Россети»	Заявители	Постоянно, за 90 рабочих дней до планируемого срока начала Проверки
2.	Рассмотрение Заявки на предмет: - необходимости применения данного типа цифрового оборудования, систем и ТСЗИ в составе ОКИИ на объектах электросетевого комплекса; - наличия документов, предоставляемых Заявителем для продления срока действия, внесения дополнений и изменений в ЗАК	Заказчик	5 рабочих дней с даты поступления Заявки
3.	Подписание письма-поручения и направление Исполнителю	Заказчик	2 рабочих дня с даты согласования Заявки
4.	Заключение договора на проведение продления, внесения изменений в ЗАК	Исполнитель, Заявитель	В соответствии с планом-графиком Проверки
5.	Анализ представленной Заявителем документации на предмет соответствия государственным и отраслевым требованиям и дополнительным требованиям Обществ, с учетом анализа отзывов эксплуатирующих организаций и возможности продления. Оформление проекта решения по форме приложения 15 к настоящему Методике о продлении (или отказе в продлении) срока действия, дополнений и изменений к заключению аттестационной комиссии.	Исполнитель, при необходимости с привлечением экспертных организаций (экспертов)	30 рабочих дней с даты начала действия договора
6.	Согласование проекта решения о продлении (или отказе в продлении) срока действия, дополнений и изменений к ЗАК на предмет актуальности и комплектности предоставленных Заявителем документов.	Исполнитель	5 рабочих дней с даты получения проекта решения
7.	Направление Исполнителем проекта Решения на согласование Заказчику с приложением сканированной копии	Исполнитель	2 рабочих дня с даты получения согласованного с Заказчиком проекта Решения
8.	Согласование проекта решения Заказчиком на предмет соответствия государственным и отраслевым требованиям и дополнительным требованиям Обществ с проверкой отсутствия замечаний от эксплуатирующих организаций	Заказчик	5 рабочих дней с даты получения проекта Решения

№ п/п	Содержание работы	Исполнитель	Срок
9.	Доработка проекта Решения по замечаниям Заказчика	Исполнитель	5 рабочих дней с даты получения замечаний и предложений
10.	Утверждение Решения о продлении (или отказе в продлении) срока действия дополнений и изменений к заключению аттестационной комиссии и направление в Депозитарий (по форме Приложения 15 к настоящей Методике)	Заместитель Генерального директора по безопасности ПАО «Россети», Заказчик	4 рабочих дня с даты получения проекта Решения
11.	Внесение в Перечень рекомендованных к применению в составе ОКИИ на объектах Обществ, нового срока действия ЗАК или внесенных изменений и дополнений к ЗАК	Заказчик	5 рабочих дней с даты утверждения решения
12.	Размещение на сайте ПАО «Россети» Перечня	Заказчик, Департамент по связям с общественностью и СМИ ПАО «Россети»	5 рабочих дней с даты утверждения решения

9.6. ПЛАНОВАЯ ИНСПЕКЦИОННАЯ ПРОВЕРКА СОСТОЯНИЯ ПРОИЗВОДСТВА АТТЕСТОВАННОЙ ПРОДУКЦИИ

Порядок организации плановой инспекционной проверки состояния производства указан в таблице 6.

Таблица 6

№ п/п	Содержание работы	Исполнитель	Срок
1.	Направление Заявки на проведение ИПП по свободной форме в адрес Заказчика с приложением документации согласно Приложения 16 к Методике	Заявитель	Не менее чем за 3 месяца до истечения срока действия ЗАК или предыдущего акта ИПП
2.	Рассмотрение Заявки на предмет: - необходимости проведения ИПП; - своевременности подачи заявки на ИПП; - наличия документов, предоставляемых Заявителем для проведения ИПП	Заказчик	5 рабочих дней с даты поступления Заявки
3.	Оформление поручения в адрес Исполнителя на проведение ИПП	Заказчик	2 рабочих дня с даты согласования Заявки
4.	Заключение договора на проведение ИПП между Исполнителем и Заявителем	Исполнитель, Заявитель	В течении 10 рабочих дней
5.	Оплата Заявителем услуг по договору	Заявитель	В течении 3 рабочих дней
6.	Рассмотрение полноты и достоверности представленной Заявителем документации	Исполнитель	В течении 10 рабочих дней

№ п/п	Содержание работы	Исполнитель	Срок
7.	Устранение замечаний по полноте и достоверности представленной документации	Заявитель	В течении 5 рабочих дней
8.	Согласование сроков выезда инспекционной комиссии для проведения ИПП	Исполнитель, Заявитель Заказчик	В течении 10 рабочих дней с даты оплаты по договору
9.	Выезд на производство. Проведение инспекционной проверки состояния производства	Исполнитель, Заявитель	5 рабочих дней (день туда, день обратно, 3 дня на производстве)
10.	Подготовка акта выполнения ИПП	Исполнитель	5 рабочих дней с даты завершения инспекционной проверки
11.	Согласование акта ИПП с Заявителем. Устранение замечаний. Направление акта ИПП на утверждение Заказчику	Исполнитель, Заявитель	5 рабочих дней
12.	Согласование и утверждение акта ИПП	Заказчик	5 рабочих дней

ПЕРЕЧЕНЬ
цифрового оборудования и систем,
подлежащих Проверке в ПАО «Россети»

№ п/п	Наименование группы оборудования	Наименование вида оборудования
1.	Устройства релейной защиты и автоматики*	Устройства релейной защиты, электроавтоматики, сигнализации, противоаварийной автоматики
		Регистраторы аварийных событий (РАС)
		Приборы определения места повреждения на линии (ОМП)
		Программные продукты для мониторинга и обслуживания РЗА, определения мест повреждения на ВЛ. Аппаратура для испытания и проверки устройств РЗА.
2.	Средства связи*	Системы и оборудование высокочастотной связи
		Высокочастотные заградители
		Фильтры присоединения
		Разделительные фильтры
		Системы/оборудование передачи информации (по металлическим и волоконно-оптическим кабелям)
		Радиорелейные системы передачи
		Системы/оборудование спутниковой и радиосвязи
		Беспроводные оптические системы передачи
		Системы/оборудование телефонной связи
		Системы радиопоисковой громкоговорящей радиосвязи
3.	Средства контроля, измерений и системы мониторинга*	Системы и аппаратура диагностики состояния оборудования
		Система мониторинга основного оборудования
		Аппаратура контроля изоляции, кроме СОИТ
		Датчики и преобразователи электрических величин
		Датчики и преобразователи для специальных измерений (вибрации, состава газов и т.п.)
		Вторичная аппаратура КИП и А
		Электросчетчики
		Электрические измерительные приборы
		Системы централизованного контроля технологических параметров
		Щиты, панели
		Поверочная и измерительная аппаратура
		Автоматизированные информационно-измерительные системы контроля гололедной нагрузки (АИИСКГН)
		Индикаторы повреждения ВЛ
4.	Автоматизированные и автоматические системы*	Автоматизированные системы диспетчерско-технологического управления (АСДТУ)
		Серверы приемо-передачи и обработки данных, центральные приемо-передающие станции
		Автоматизированные системы управления технологическими процессами (АСТУ) - комплексы в целом и компоненты, входящие в состав комплекса
		Телемеханические комплексы и устройства телемеханики

*Аппаратно-программные комплексы, предназначенный для получения по цифровым интерфейсам информации и ее обработки в цифровой форме, используя цифровые технологии.

№ п/п	Наименование группы оборудования	Наименование вида оборудования
		МП измерительные и Управляющие контроллеры
		Устройства связи с объектом
		Средства представления информации
		Средства сбора информации
		Оборудование информационно-вычислительных сетей
		Программные продукты информационных и управляющих комплексов
		Системы автоматического пожаротушения (порошкового, аэрозольного, тонкораспыленной водой, газового пожаротушения)
		Системы пожарной сигнализации

Примечание:

Перечень цифрового оборудования и систем составлен в соответствии с приложением 1 к Порядку проведения проверки качества (аттестации) оборудования, материалов и систем в электросетевом комплексе на электросетевых объектах ДЗО ПАО «Россети» (утвержден Приказом ПАО «Россети» от 28.07.2020 № 329).

ПЕРЕЧЕНЬ
технических средств защиты информации,
подлежащих проверке на совместимость с АСТУВ ПАО «Россети»

1. средства защиты информации от несанкционированного доступа к АРМ, Ноутбукам, Серверам (включая DLP, а также встроенные в общесистемное, прикладное программное обеспечение функции защиты информации от НСД);
2. средства защиты информации от несанкционированного доступа к информации, обрабатываемой на смартфонах, планшетах;
3. межсетевые экраны уровня сети, уровня логических границ сети;
4. межсетевые экраны уровня промышленной сети;
5. средства обнаружения (предотвращения) вторжений (компьютерных атак) уровня сети;
6. межсетевые экраны уровня веб-сервера;
7. средства однонаправленной передачи данных (Дата-диод);
8. средствами обнаружения (предотвращения) вторжений (компьютерных атак) уровня узла;
9. средства антивирусной защиты общего назначения;
10. средства антивирусной защиты АРМ производственного персонала, промышленных серверов;
11. средства антивирусной защиты уровня сети, веб-сервера;
12. средства (системы) контроля (анализа) защищенности;
13. средства мониторинга и корреляции событий безопасности;
14. средства управления инцидентами;
15. средства предупреждения компьютерных атак;
16. средства защиты каналов передачи данных;
17. средства защищенного удаленного доступа в ЛВС, в том числе средства терминального доступа, двухфакторной аутентификации;
18. средства резервного копирования, в том числе средства создания и хранения резервных копий;
19. средства управления ключевой информацией.

Примечание:

Перечень технических средств защиты информации составлен в соответствии с Положением ПАО «Россети» о единой технической политике в электросетевом комплексе, утвержденным решением Совета директоров ПАО «Россети» (протокол от 07.10.2019 г. № 378).

ТРЕБОВАНИЯ ПО БЕЗОПАСНОСТИ ИНФОРМАЦИИ, ОЦЕНИВАЕМЫЕ В РАМКАХ ПРОВЕРКИ

1. ОБЩИЕ ТРЕБОВАНИЯ

В рамках проверки предлагаемого к использованию на объектах электросетевого хозяйства ДЗО ПАО «Россети» программного обеспечения и баз данных в составе цифрового оборудования, систем и ТСЗИ оценке подлежат:

- состав микропроцессорного, общесистемного, прикладного и специализированного программного обеспечения и баз данных на отсутствие нарушений авторских прав, отсутствие ошибок и общеизвестных уязвимостей в программном обеспечении и системах управления базами данных;
- встроенные функции безопасности информации;
- порядок поставки, первоначальной установки, конфигурирования микропроцессорного, общесистемного, прикладного и специализированного программного обеспечения и баз данных;
- полнота технической (эксплуатационной) документации;
- устойчивость программного обеспечения и баз данных в режиме повышенной информационной нагрузки;
- отсутствие не декларируемых возможностей программного обеспечения и баз данных;
- корректность встраивания средств криптографической защиты информации (при наличии);
- процессы разработки программного обеспечения и производства цифрового оборудования и систем, процессы поддержки программного обеспечения на всех этапах жизненного цикла.

Оценка функции безопасности ТСЗИ производится в соответствии с профилями защиты соответствующих СТЗИ, размещенными на сайте ФСТЭК России (при наличии профиля защиты).

2. БАЗОВЫЕ УГРОЗЫ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Базовые угрозы безопасности информации, которым должны противостоять цифровое оборудование и системы:

- Злоумышленник получает доступ к управлению цифровым оборудованием и системами без авторизации пользователей;
- Злоумышленник реализует атаку, направленную на получение аутентификационной информации пользователей путем ее подбора (перебора);
- Злоумышленник реализует атаку, направленную на получение идентификационной и/или аутентификационной информации пользователей путем организации внешнего наблюдения;

- Злоумышленник реализует атаку, обеспечивающую нарушение целостности встроенного программного обеспечения и баз данных;
- Злоумышленник реализует атаку, направленную на нарушение функционирования или прекращение функционирования цифрового оборудования и систем за счет создания повышенной информационной нагрузки на него;
- События и инциденты безопасности не регистрируются вследствие переполнения области хранения данных журналов регистрации событий безопасности.

3. ТРЕБОВАНИЯ К МЕРАМ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

В цифровом оборудовании, системах должен быть реализован минимальный набор мер по обеспечению безопасности информации:

- Идентификация и аутентификация пользователей и иницируемых ими процессов;
- Идентификация и аутентификация устройств;
- Защита аутентификационной информации при передаче;
- Управление учетными записями пользователей;
- Доверенная загрузка;
- Разделение полномочий (ролей) пользователей;
- Ограничение неуспешных попыток доступа в информационную (автоматизированную) систему;
- Ограничение числа параллельных сеансов доступа;
- Контроль использования интерфейсов ввода (вывода) информации на съемные машинные носители информации;
- Генерирование временных меток и (или) синхронизация системного времени;
- Регистрация событий безопасности;
- Защита информации о событиях безопасности;
- Контроль целостности программного обеспечения;
- Обеспечение возможности восстановления Информации;
- Обеспечение возможности восстановления программного обеспечения при нештатных ситуациях;
- Разделение функций по управлению (администрированию) информационной (автоматизированной) системой с иными функциями;
- Защита от угроз отказа в обслуживании;
- Установка (инсталляция) только разрешенного к использованию программного обеспечения;
- Контроль действий по внесению изменений;
- Получение обновлений программного обеспечения от доверенного источника;
- Контроль целостности обновлений программного обеспечения;
- Установка обновлений программного обеспечения.

В программу (методику) испытаний включаются мероприятия по проверке выполнения указанных мер.

4. ТРЕБОВАНИЯ К БЕЗОПАСНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Полнота технической (эксплуатационной) документации проверяется на предмет наличия описания следующих правил и процедур (при наличии) в отношении программного обеспечения и баз данных предлагаемого к использованию на объектах электросетевого хозяйства ДЗО ПАО «Россети» цифрового оборудования, систем и ТСЗИ:

- Регламентация правил и процедур идентификации и аутентификации;
- Регламентация правил и процедур управления доступом;
- Регламентация правил и процедур ограничения программной среды;
- Регламентация правил и процедур аудита безопасности;
- Регламентация правил и процедур защиты машинных носителей информации;
- Регламентация правил и процедур антивирусной защиты;
- Регламентация правил и процедур обеспечения целостности;
- Регламентация правил и процедур обеспечения доступности;
- Регламентация правил и процедур защиты технических средств и систем;
- Регламентация правил и процедур защиты информационной (автоматизированной) системы и ее компонентов;
- Регламентация правил и процедур управления обновлениями программного обеспечения;
- Регламентация правил и процедур обеспечения действий в нештатных ситуациях;
- Регламентация правил и процедур управления конфигурацией информационной (автоматизированной) системы.

Процессы разработки программного обеспечения и производства цифрового оборудования и систем, процессы поддержки программного обеспечения на всех этапах жизненного цикла проверяются на предмет:

- Наличия правил и процедур планирования мероприятий по обеспечению безопасности информации в цифровом оборудовании и системах;
- Наличия правил и процедур отслеживания и исправления ошибок и уязвимостей в программном обеспечении;
- Наличия правил и процедур анализа возникших ошибок в программном обеспечении и принятия мер по недопущению их повторного возникновения;
- Наличия правил и процедур информирования конечных пользователей об угрозах безопасности информации и о правилах безопасной работы с цифровым оборудованием и системами.

В качестве подтверждения реализации мер направленных на безопасную разработку программного обеспечения предприятие-изготовитель (или уполномоченный заявитель) могут быть представлены копии имеющихся российских и международных сертификатов, подтверждающих наличие у производителя необходимых условий для обеспечения безопасности информации на

соответствие ГОСТ Р 56939-2016 «Национальный стандарт Российской Федерации. Защита информации. Разработка безопасного программного обеспечения. Общие требования» (утв. и введен в действие Приказом Росстандарта от 01.06.2016 № 458-ст) и ГОСТ Р ИСО/МЭК 27001-2006 «Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности» (утв. и введен в действие Приказом Ростехрегулирования от 27.12.2006 № 375-ст).

ПЕРЕЧЕНЬ
документов, представляемых Заявителем
для проведения Проверки

1. Сведения о предприятии-изготовителе цифрового оборудования, системы и ТСЗИ.

2. Сведения об организации, представляющей цифровое оборудование, системы и ТСЗИ на проверку с приложением поручения от предприятия-изготовителя на представление своих интересов при проведении проверки.

3. Технические условия (спецификация) применения цифрового оборудования, систем и ТСЗИ, указания по безопасной установке, обновлению и выбору параметров настройки и алгоритмов функционирования,

4. Техническая (эксплуатационная) документация.

5. Описание состава программного обеспечения и баз данных в составе цифрового оборудования и систем, ТСЗИ (включая протоколы обмена информацией, прикладное программное обеспечение и т.д.);

6. Сведения об объеме прав интеллектуальной собственности Заявителя (предприятия-изготовителя) на программное обеспечение и базы данных, входящие в состав цифрового оборудования и систем, ТСЗИ (включая, указание правообладателя, формы, срока действия права, разрешенной территории использования), а также сведения об объеме прав, передаваемых конечному пользователю (Обществу или ДЗО).

7. Сведения о гарантийных обязательствах Заявителя (предприятия-изготовителя) в отношении программного обеспечения и баз данных, входящих в состав цифрового оборудования и систем, ТСЗИ (включая порядок и частоту выпуска обновлений, сроки и условия прекращения поддержки).

8. Копии имеющихся российских и международных сертификатов в области безопасности информации на программное обеспечение и базы данных, входящие в состав цифрового оборудования и систем, ТСЗИ (при наличии).

9. Копии имеющихся заключений о проведенных испытаниях программного обеспечения и баз данных, входящих в состав цифрового оборудования и систем, ТСЗИ в режиме повышенной информационной нагрузки (при наличии).

10. Копии имеющихся российских и международных сертификатов, подтверждающих наличие у производителя необходимых условий производства для обеспечения безопасности информации в выпускаемой продукции (при наличии).

11. Декларация о выполнении мероприятий по отслеживанию и устранению ошибок и общеизвестных уязвимостей в программном обеспечении и системах управления базами данных, входящих в состав цифрового оборудования и систем, ТСЗИ с приложением перечня выпущенных обновлений.

12. Декларация о выполнении мероприятий по устранению ошибок и уязвимостей в программном обеспечении и системах управления базами данных, выявленных в ходе эксплуатации (предоставляется при повторной проверке или после отзыва заключения аттестационной комиссии).

13. Справка о выполненных внедрениях, отзывы эксплуатирующих предприятий.

Примечания:

1. К заявке на Проверку должны быть приложены документы:

- по пунктам 1,2 - на бумажном носителе (1 экз.);*
- по пунктам 3-13 - на электронном носителе (CD).*

2. Исполнителю предоставляется полный комплект документов на бумажном и электронном носителях в формате pdf и MS Office.

3. Все документы (за исключением копий) должны представляться на русском языке. При необходимости Исполнитель может потребовать от Заявителя предоставления переводов документации на русский язык.

4. ПАО «Россети» и Исполнитель обеспечивают конфиденциальность использования представленных документов.

ПЕРЕЧЕНЬ
документов, представляемых Заявителем
для проведения дополнительной Проверки с целью внесения изменений или
дополнений в заключение аттестационной комиссии

1. Документы, перечисленные в Приложении 4 к настоящей Методике.
2. Акт (справка, извещение) предприятия-изготовителя об изменениях в конструкции, технологии изготовления, программном обеспечении или отсутствии таковых.

Форма заявки для первичной Проверки*[На бланке организации (предприятия) Заявителя]*Руководителю Департамента
обеспечения безопасности
ПАО «Россети»
_____**ЗАЯВКА**

на проведение Проверки *[указать наименование и обозначение типа (модели, марки) цифрового оборудования, системы, технического средства защиты информации подлежащего проверке на совместимость с АСТУ],* изготавливаемого *[указать производителя оборудования].* (Заявка подается отдельно на каждый тип и вид цифрового оборудования и системы, объединение заявок возможно в соответствии с принципом выбора типопредставителя).

В целях проведения Проверки *[Заявитель]* добровольно принимает на себя обязанности соблюдения Методики, утвержденной приказом ПАО «Россети» от _____ № _____).

Приложения: *[перечислить прилагаемые к заявке документы]*

*[Должность руководителя]**[Ф.И.О.]*

М.П.

*Исполнитель
контактный телефон
E-mail*

Форма заявки для продления срока действия ЗАК*[На бланке организации (предприятия) Заявителя]*Директору Департамента
обеспечения безопасности
ПАО «Россети»
_____**ЗАЯВКА**

на продление срока действия ЗАК от ___ № ___) *[указать наименование и обозначение типа (модели, марки) цифрового оборудования и системы], изготавливаемого [указать производителя]. (Заявка подается отдельно на каждый тип и вид цифрового оборудования и системы, объединение заявок возможно в соответствии с принципом выбора типопредставителя).*

В целях проведения Проверки (продления срока действия Заключения аттестационной комиссии) *[Заявитель]* добровольно принимает на себя обязанности соблюдения Методики, утвержденной приказом ПАО «Россети» от _____ № _____).

Приложения: *[перечислить прилагаемые к заявке документы]**[Должность руководителя]**[Ф.И.О.]*

М.П.

*Исполнитель
контактный телефон
E-mail*

Форма заявки для проведения работ по внесению изменений (дополнений) в действующее ЗАК

[На бланке организации (предприятия) Заявителя]

Директору Департамента
обеспечения безопасности
ПАО «Россети»

ЗАЯВКА

на внесение изменений (дополнений) в действующее ЗАК от _____ № _____
[указать наименование и обозначение типа (модели, марки) цифрового оборудования и системы], изготавливаемого [указать производителя оборудования] в связи с [указать причину внесения изменений (дополнений)].

В целях проведения Проверки *[Заявитель]* добровольно принимает на себя обязанности соблюдения Методики, утвержденной приказом ПАО «Россети» от _____ № _____).

Приложения: *[перечислить прилагаемые к заявке документы, в соответствии с приложением 5 к Методике]*

[Должность руководителя]

[Ф.И.О.]

М.П.

*Исполнитель
контактный телефон
E-mail*

Форма письма о составе аттестационной комиссии

*[Заявителю
Генеральному директору
Организация]*

Ф.И.О.

О составе комиссии по приемке

Уважаемый !

В соответствии с Методикой проверки цифрового оборудования и систем на соответствие требованиям безопасности информации, в том числе проверки технических средств защиты информации на совместимость с АСТУ в электросетевом комплексе для проведения Проверки (аттестации) _____, изготавливаемого _____ (г. _____, Страна) на соответствие техническим требованиям ПАО «Россети», утверждена комиссия в следующем составе:

Председатель комиссии:

Представитель ПАО «Россети» или Исполнителя (должность, место работы, ученая степень, Ф.И.О.).

Члены комиссии:

Представитель организации (должность, место работы, ученая степень, Ф.И.О.).

Директор Департамента

Ф.И.О.

Исп.

Тел. исп.

РЕКОМЕНДУЕМАЯ ФОРМА**ПРОТОКОЛ**
заседания аттестационной комиссии
Место проведения

_____ (Дата)

№ _____

ПРИСУТСТВОВАЛИ:

Состав аттестационной комиссии.

РАССМОТРЕЛИ И ОТМЕТИЛИ:

Объем материалов, представленных аттестационной комиссии для рассмотрения и анализа с указанием разработчика, поставщика (изготовителя) оборудования, наименования (тип, марка) оборудования).

- перечень конструкторской документации,
- перечень технологической документации,
- перечень протоколов испытаний,
- перечень эксплуатационной документации и т.д.

РЕШИЛИ:

Выводы комиссии:

- о комплектности и качестве представленных материалов;
- о полноте, качестве и достоверности результатов испытаний и проверок.

Подписи председателя и членов аттестационной комиссии.

РЕКОМЕНДУЕМАЯ ФОРМА

УТВЕРЖДАЮ
Заместитель Генерального директора
по безопасности
ПАО «Россети»

_____ Ф.И.О.
«___» _____ 20 г.

**Заключение
аттестационной комиссии
№ _____**

Срок действия с _____ г
Дата очередной плановой проверки производства _____ г

ОБОРУДОВАНИЕ

(Наименование и обозначение оборудования, обозначение ТУ или технической спецификации)

ЗАЯВИТЕЛЬ

(Полное и сокращенное наименование предприятия изготовителя, почтовый и фактический адрес на территории РФ)

ИЗГОТОВИТЕЛЬ

(Полное и сокращенное наименование предприятия изготовителя, почтовый адрес и фактический адрес)

Соответствует

техническим требованиям ПАО «Россети» по безопасности информации

РЕКОМЕНДУЕТСЯ

для применения на объектах ПАО «Россети»

(Указать область применения и ограничения и обязательства при применении)

Запрещается передача и перепечатка и публикация материалов настоящего заключения
без разрешения ПАО «Россети»

**ЛИСТ СОГЛАСОВАНИЯ
заключения аттестационной комиссии**

Наименование должности, структурного подразделения, Ф.И.О. согласующего лица	Согласование или замечания	Подпись должностного лица

1. Состав аттестационной комиссии и кем образована

Председатель комиссии - должность, место работы, ученая степень, Ф.И.О.

Члены комиссии - должность, место работы, ученая степень, Ф.И.О.

2. Исполнитель

Полное название и адрес организации, которой поручено координация и организация работы.

3. Производитель-изготовитель.

Полное название и адрес предприятия-изготовителя и сервисных центров цифрового оборудования и систем, ТСЗИ, представленного для проверки. Краткая характеристика предприятия-изготовителя.

Полное название и адрес поставщика оборудования.

4. Объем материалов, представленных для проверки

Указать полный перечень материалов (включая образцы оборудования), представленных Заявителем для проверки.

5. Общие технические характеристики и функциональные показатели оборудования, представленного на проверку.

6. Перечень стандартов и отраслевых документов, содержащих требования по безопасности информации, условиям его применения и дополнительные требования, на соответствие которым проводится экспертиза

7. Краткое описание методов и оборудования, использованных при проведении проверки.

Заключение составляется на основании анализа протоколов испытаний и анализа системы безопасности. Оцениваются технологии производства и меры, принимаемые для разработки безопасного программного обеспечения.

При анализе протоколов испытаний необходимо указать номер и дату выдачи аттестата аккредитации испытательных лабораторий (при наличии).

При распространении результатов испытаний одного типоразмера

оборудования на всю серию, если это технологически возможно, учитывается правило прототипов.

8. Результаты проверки соответствия оборудования утвержденным техническим требованиям

Технические требования ПАО «Россети»	Требуемое значение	Значения функциональных показателей, подтвержденных протоколами испытаний	Заключение о соответствии
1	2	3	4

9. Описание испытаний, проведенных в присутствии членов аттестационной комиссии.

Результаты испытаний приводятся в таблице:

Вид испытаний	Требуемые значения функциональных показателей, указанных в НД	№ протокола, дата проведения испытаний, значения функциональных показателей	Заключение о соответствии
1	2	3	4

Выводы аттестационной комиссии по результатам испытаний

10. Предложения аттестационной комиссии о целесообразности организации опытно-промышленной эксплуатации аттестуемого оборудования.

11. Выводы о соответствии цифрового оборудования, систем и ТСЗИ утвержденным техническим требованиям.

Дается общая оценка соответствия принимаемого оборудования требованиям и условиям эксплуатации.

Указывается срок действия ЗАК и очередная дата ИПП

Председатель комиссии _____ Ф.И.О.

Члены комиссии: _____

РЕКОМЕНДУЕМАЯ ФОРМА

УТВЕРЖДАЮ
*Должность руководителя
Исполнителя*

_____ Ф.И.О.

«__» _____ 201 г.

**Протокол предварительного рассмотрения документации
по проверке (аттестации) _____**

СОГЛАСОВАНО
*Технический представитель
Исполнителя*

_____ Ф.И.О.
«__» _____ 201 г.

1. ОСНОВАНИЕ

Договор на оказание услуг по проведению проверки (аттестации)
_____ (указать реквизиты договора)

2. ОБЪЕКТ ПРОВЕРКИ

2.1. Наименование продукции

3. ИЗГОТОВИТЕЛЬ (полный адрес)

4. ОБЪЕМ ДОКУМЕНТАЦИИ ПРЕДСТАВЛЕННОЙ НА ПРОВЕРКУ

5. РЕЗУЛЬТАТЫ ОЦЕНКИ КОМПЛЕКТНОСТИ

5.1. Результаты предварительного рассмотрения документации.

6. ЗАКЛЮЧЕНИЕ

Представленная Заявителем документация на _____
НЕ/удовлетворяет требованию в части комплектности.

*Технический специалист
Исполнителя*

Ф.И.О.

АКТ
о результатах анализа состояния производства
(оформляется при первичной аттестации)
«.....» (указать производителя)
по выпуску (указать продукцию)

Место: г. _____

дата

1. ЦЕЛЬ АНАЛИЗА проверка наличия необходимых условий на заводе «.....» для производства ...

2. ОСНОВАНИЕ поручение ПАО «Россети» от xx.xx.201x №... по заявке на проверку (аттестацию).

3. МЕСТО И ВРЕМЯ ПРОВЕДЕНИЯ – xx.xx.201x.

**4. ЭКСПЕРТЫ, ПРОВОДИВШИЕ АНАЛИЗ
ПРОИЗВОДСТВА**

1. ФИО - должность.
2. ФИО - должность.

5. БАЗА АНАЛИЗА ПРОИЗВОДСТВА

6. ОБЩАЯ ИНФОРМАЦИЯ О ПРОИЗВОДСТВЕ

Основание производства: собственная разработка, лицензионная сборка (степень локализации).

7. РЕЗУЛЬТАТЫ ПРОВЕРКИ ПРОИЗВОДСТВА

7.1. Технологические процессы обеспечения безопасной разработки программного обеспечения

7.2. Документация безопасной разработки ПО

7.3. Средства защиты информации для обеспечения разработки безопасного ПО

7.4. Методики испытаний (тестирования) программного обеспечения

7.5. Входной контроль

7.6. Приемочный контроль

7.7. Периодические испытания

7.8. Испытания, проведенные в присутствии экспертов

8.РЕКЛАМАЦИИ ПОТРЕБИТЕЛЯ

9. ВЫВОДЫ

10. Подписи ЭКСПЕРТОВ

ФИО _____ (подпись)
ФИО _____ (подпись)
ФИО _____ (подпись)

С АКТОМ ОЗНАКОМЛЕН

ФИО - генеральный директор Заявителя/производителя-изготовителя.

РЕКОМЕНДУЕМАЯ ФОРМА

УТВЕРЖДАЮ
Заместитель Генерального директора
по безопасности
ПАО «Россети»

_____ Ф.И.О.
«___» _____ 20 г.

АКТ
ПЛАНОВОЙ ИНСПЕКЦИОННОЙ ПРОВЕРКИ ПРОИЗВОДСТВА
№ _____

Срок действия с __ . __ . 20 г. по __ . __ . 20 г.

ОБОРУДОВАНИЕ

(Наименование и обозначение оборудования, обозначение ТУ или технической спецификации)

ЗАЯВИТЕЛЬ

(Полное и сокращенное наименование предприятия изготовителя, почтовый и фактический адрес на территории РФ)

ИЗГОТОВИТЕЛЬ

(Полное и сокращенное наименование предприятия изготовителя, почтовый адрес и фактический адрес)

СООТВЕТСТВУЕТ

техническим требованиям ПАО «Россети» по безопасности информации

РЕКОМЕНДУЕТСЯ

для применения на объектах ПАО «Россети»

(Указать область применения и ограничения и обязательства при применении)

1. ЦЕЛЬ АНАЛИЗА проверка наличия необходимых условий на заводе «.....» для производства ...

2. ОСНОВАНИЕ поручение ПАО «Россети» от хх.хх.201х №... по проверке (аттестации).

3. МЕСТО И ВРЕМЯ ПРОВЕДЕНИЯ – хх.хх.201х.

4. ЭКСПЕРТЫ, ПРОВОДИВШИЕ АНАЛИЗ ПРОИЗВОДСТВА

ФИО - должность.

ФИО - должность.

ФИО – должность

5. БАЗА АНАЛИЗА ПРОИЗВОДСТВА

Анализ проводился в соответствии с ГОСТ Р 50.3.004-99 «Анализ состояния производства при сертификации продукции».

6. ОБЩАЯ ИНФОРМАЦИЯ О ПРОИЗВОДСТВЕ

Основание производства: собственная разработка, лицензионная сборка (степень локализации).

7. РЕЗУЛЬТАТЫ ПРОВЕРКИ ПРОИЗВОДСТВА

7.1. Технологические процессы обеспечения безопасной разработки программного обеспечения

7.2. Документация безопасной разработки ПО

7.3. Средства защиты информации для обеспечения разработки безопасного ПО

7.4. Методики испытаний (тестирования) программного обеспечения

7.5. Входной контроль

7.6. Приемочный контроль

7.7. Периодические испытания

7.8. Испытания проведенные в присутствии экспертов

8. РЕКЛАМАЦИИ ПОТРЕБИТЕЛЕЙ**9. ОБЪЕМ ДОКУМЕНТАЦИИ ПРЕДСТАВЛЕННОЙ НА ПРОВЕРКУ****10. РЕЗУЛЬТАТЫ РАССМОТРЕНИЯ ДОКУМЕНТАЦИИ**

Наименование функциональных показателей	Требования нормативных документов	Результаты испытаний и проверок	Заключение
1	2	3	4

11. ВЫВОДЫ**12. ПОДПИСЬ ЭКСПЕРТОВ**

ФИО _____ подпись
ФИО _____ подпись
ФИО _____ подпись

РЕКОМЕНДУЕМАЯ ФОРМА

РАЗРАБОТАНО

*Должность руководителя
Исполнителя*

_____ Ф.И.О.

«__» _____ 201 г.

УТВЕРЖДАЮ

Заместитель Генерального
директора по безопасности
ПАО «Россети»

_____ Ф.И.О.

«__» _____ 201 г.

ПРОТОКОЛ № _____ от __. __. 201 г.по продлению срока действия Заключения аттестационной комиссии
№ _____ от __. __. 20 г.

Срок действия с __. __. 20 г. по __. __. 20 г.

ОБОРУДОВАНИЕ**ИЗГОТОВИТЕЛЬ****СООТВЕТСТВУЕТ**

техническим требованиям ПАО «Россети» по безопасности информации

РЕКОМЕНДУЕТСЯ

для применения на объектах ПАО «Россети»

Запрещается передача и перепечатка и публикация материалов настоящего заключения
без разрешения ПАО «Россети»

1. ОСНОВАНИЕ

Заявка от производителя, на продление срока действия Заключения аттестационной комиссии.

2. ОБЪЕКТ ПРОВЕРКИ

3. ИЗГОТОВИТЕЛЬ/ПОСТАВЩИК

Адреса

4. ОБЪЕМ ДОКУМЕНТАЦИИ ПРЕДСТАВЛЕННОЙ НА ПРОВЕРКУ

5. РЕЗУЛЬТАТЫ РАССМОТРЕНИЯ ДОКУМЕНТАЦИИ

Наименование функциональных показателей	Требования нормативных документов	Результаты испытаний и проверок	Заключение
1	2	3	4

6. ЗАКЛЮЧЕНИЕ

На основании результатов рассмотрения представленной документации продлить срок действия заключения аттестационной комиссии на _____, производства _____ по ТУ (номер ТУ если есть)

Срок действия заключения аттестационной комиссии - _____ лет с даты утверждения настоящего протокола.

Технический эксперт
Исполнителя Ф.И.О.

ПЕРЕЧЕНЬ
документов, представляемых Заявителем
для проведения плановой инспекционной проверки производства

1. Сведения о предприятии (организации), представляющей оборудование на аттестацию, с доверенностью от предприятия-изготовителя оборудования.
2. Документ (Акт, Экспертное Заключение и т.д.) подтверждающий прохождение проверки (аттестации) в ПАО «Россети».
3. Технические условия (обязательно для отечественного оборудования, в том числе, локализованного).
4. Техническая спецификация (для импортного оборудования).
5. Руководство (инструкция) по монтажу, настройке и вводу в эксплуатацию.
6. Паспорт или иной документ, удостоверяющий гарантийные обязательства предприятия-изготовителя.
7. Копии протоколов периодических испытаний
8. Перечень протоколов с указанием номера протокола испытаний, даты утверждения, наименования испытательной лаборатории, вида испытаний, объекта испытаний в области защиты информации
9. Акт (справка, извещение) предприятия-изготовителя об изменениях в конструкции, технологии изготовления, программном обеспечении или отсутствии таковых.
10. Справка о внедрении, отзывы эксплуатирующих предприятий.
11. Копии действующих российских и международных сертификатов в области защиты информации.
12. Копии документов, подтверждающих право передачи ДЗО Общества неисключительных прав на программное обеспечение.
13. Копии договоров об оказании услуг технической поддержки программного обеспечения (при отсутствии исключительных прав на программное обеспечение).