

ДОГОВОР № _____

на оказание услуг по техническому обслуживанию и сопровождению
системы коллективного отображения информации ДП ЦУС АО «Тюменьэнерго»

г. Сургут

« ____ » _____ 2018 г.

Акционерное общество энергетики и электрификации «Тюменьэнерго» (АО «Тюменьэнерго»), именуемое в дальнейшем «Заказчик», в лице _____, действующего на основании _____ с одной стороны, и _____, именуемое в дальнейшем «Исполнитель», в лице _____, действующего на основании _____ с другой стороны, именуемые «Стороны», по результатам _____ (закупка осуществлялась при участии всех субъектов предпринимательства), объявленного на официальном сайте РФ www.zakupki.gov.ru (извещение № _____ от _____), на корпоративном сайте www.te.ru (извещение № _____ от _____), проведенного в _____ по адресу _____ (№ _____), на основании протокола № _____ от _____, заключили настоящий Договор о нижеследующем:

1. ПРЕДМЕТ ДОГОВОРА

1.1. Исполнитель обязуется оказывать услуги по техническому обслуживанию и сопровождению системы коллективного отображения информации Диспетчерского пункта ЦУС АО «Тюменьэнерго» (далее – «Система»), принадлежащей Заказчику (далее по тексту – «Услуги»), в соответствии с Техническим заданием (Приложение № 1 к настоящему Договору).

1.2. Заказчик обязуется оплачивать Исполнителю оказываемые им Услуги на условиях настоящего Договора.

2. СТОИМОСТЬ УСЛУГ ПО ДОГОВОРУ

2.1. Общая стоимость услуг по Договору включает в себя стоимость технического обслуживания Системы и стоимость сопровождения Системы и определена по результатам _____ на основании протокола № _____ от _____ и составляет _____ (_____) рублей _____ копеек в год, кроме того НДС по ставке 20%- _____ (_____) рублей _____ копеек. Итого в год с учетом НДС (20%) _____ (_____) рублей _____ копеек.

2.1.1. Стоимость услуг по сопровождению Системы составляет _____ (сумма прописью) рублей _____ копеек. Кроме того, НДС-20% - _____ (сумма прописью) рублей _____ копеек. Итого с НДС 20% - _____ (сумма прописью) рублей _____ копеек.

2.1.2. Стоимость услуг по техническому обслуживанию Системы составляет _____ (сумма прописью) рублей _____ копеек. Кроме того, НДС- 20% - _____ (сумма прописью) рублей _____ копеек. Итого с НДС 20% - _____ (сумма прописью) рублей _____ копеек.

2.2. Общая стоимость услуг по Договору включает в себя все затраты Исполнителя, связанные с исполнением обязательств по настоящему Договору, включая командировочные расходы, затраты на непредвиденные и неотложные услуги.

3. УСЛОВИЯ ПЛАТЕЖЕЙ И ПОРЯДОК РАСЧЕТОВ

3.1. Оплата услуг по сопровождению Системы производится Заказчиком ежеквартально, после подписания обеими сторонами Актов сдачи-приемки оказанных услуг, в течение 30 календарных дней с момента предоставления Исполнителем счета-фактуры.

Если договор заключается с субъектом малого и среднего предпринимательства, п.3.1. Договора изложить в следующей редакции:

«Оплата услуг по сопровождению Системы производится Заказчиком ежеквартально, за фактически оказанные услуги, в течение 30 (тридцати) календарных дней после подписания Заказчиком Акта сдачи-приемки оказанных услуг (по форме, установленной Приложением № 2 к настоящему Договору)».

3.2. Оплата услуг по техническому обслуживанию производится Заказчиком один раз в полугодие после подписания обеими сторонами Актов сдачи-приемки оказанных услуг, в течение 30 календарных дней с момента предоставления Исполнителем счета-фактуры.

Если договор заключается с субъектом малого и среднего предпринимательства, п.3.2. Договора изложить в следующей редакции:

«Оплата услуг по техническому обслуживанию производится Заказчиком один раз в полугодие»

Согласовано: Секретарь закупочной комиссии
АО «Тюменьэнерго» Дудасова Н.И.

Согласовано: Департамент правового обеспечения
АО «Тюменьэнерго»

после подписания Заказчиком Акта сдачи-приемки оказанных услуг, в срок не более 30 календарных дней.

3.3. Стоимость услуг по сопровождению Системы в квартал составляет _____ (сумма прописью) рублей __ копеек. Кроме того, НДС- 20% - _____ (сумма прописью) рублей __ копеек. Итого с НДС 20% - _____ (сумма прописью) рублей __ копеек.

3.4. Стоимость услуг технического обслуживания Системы в полугодие составляет _____ (сумма прописью) рублей __ копеек. Кроме того, НДС- 20% - _____ (сумма прописью) рублей __ копеек. Итого с НДС 20% - _____ (сумма прописью) рублей __ копеек.

3.5. Исполнитель обязан выставлять Заказчику счета-фактуры, соответствующие положениям ст.169 НК РФ, не позднее 5 числа первого календарного месяца, следующего за отчетным периодом (отчетным периодом по сопровождению Системы является календарный квартал; отчетным периодом по техническому обслуживанию Системы является полугодие). В случае если Исполнитель не выставил в срок счет-фактуру, либо выставил счет-фактуру, содержание которого не соответствует ст.169 НК РФ, Заказчик вправе взыскать с Исполнителя неустойку в сумме налога на добавленную стоимость, которая могла бы быть предъявлена Заказчиком к вычету или возмещению из бюджета, при условии надлежащего оформления и предоставления счета-фактуры. Для целей применения настоящего пункта стороны признают, что понятие «выставил» означает изготовление и передачу Заказчику оригинала счета-фактуры. Стороны также признают, что для взыскания неустойки, предусмотренной настоящим пунктом, Заказчик не обязан доказывать факт отказа налоговых органов в предоставлении указанных выше вычетов или возмещения Заказчику из бюджета, указанных выше.

3.6. Все расчеты по настоящему Договору осуществляются банковским переводом в рублях. Обязательства Заказчика по оплате считаются исполненными на дату списания денежных средств с расчетного счета Заказчика (по реквизитам, указанным в разделе 14 настоящего Договора).

4. ПОРЯДОК СДАЧИ И ПРИЕМКИ УСЛУГ

4.1. Датой сдачи-приемки оказанных услуг по сопровождению Системы является последний день календарного месяца отчетного квартала; по техническому обслуживанию Системы - согласно Графику оказания услуг (последний день календарного месяца 2 квартала и последний день календарного месяца 4 квартала). Приемка услуг по техническому обслуживанию Системы оформляется Актом сдачи-приемки оказанных услуг (по форме, установленной Приложением № 2 к настоящему Договору); по сопровождению Системы - Актом сдачи-приемки оказанных услуг (по форме, установленной Приложением № 2 к настоящему Договору), с обязательным приложением к нему журнала обращений Заказчика и отчета (по форме, установленной Приложением № 3 к настоящему Договору). Акты сдачи-приемки оказанных услуг должны соответствовать требованиям п.2 ст.9 Федерального закона №402-ФЗ «О бухгалтерском учете». Указанные Акты предоставляются Исполнителем Заказчику не позднее 5-ого числа первого календарного месяца, следующего за отчетным периодом (отчетным периодом по сопровождению Системы является календарный квартал; отчетным периодом по техническому обслуживанию Системы является полугодие)..

4.2. Заказчик в течение 10 (десяти) календарных дней с даты получения Актов сдачи-приемки оказанных услуг, указанных в пункте 4.1 настоящего договора, обязан подписать Акты и направить их Исполнителю или предоставить Исполнителю в тот же срок письменный мотивированный отказ от подписания Акта.

4.3. Услуги считаются принятыми с момента подписания сторонами Акта сдачи-приемки оказанных услуг в порядке, установленном в разделе 4 настоящего Договора.

5. ОТВЕТСТВЕННОСТЬ СТОРОН

5.1. В случае нарушения Исполнителем сроков оказания услуг по техническому обслуживанию и сопровождению Системы, определенных в Техническом задании (Приложение №1 к настоящему Договору), Заказчик вправе взыскать с Исполнителя неустойку в размере 0,1 % от стоимости услуг за отчетный период (отчетным периодом по сопровождению Системы является календарный квартал; отчетным периодом по техническому обслуживанию Системы является полугодие), за каждый день просрочки, но не более 10% от стоимости услуг за отчетный период.

5.2. Заказчик вправе в одностороннем внесудебном порядке отказаться от исполнения договора (в т.ч. при неисполнении/ненадлежащем исполнении Исполнителем обязательств по Договору). При этом договор считается расторгнутым с даты получения Исполнителем уведомления об отказе от исполнения договора, если иной более поздний срок не указан в уведомлении. При неполучении Исполнителем уведомления по причинам, связанным с отсутствием у Заказчика информации о фактическом месте нахождения Исполнителя, с изменением наименования, реорганизацией последнего, договор считается расторгнутым с даты получения Заказчиком уведомления об отсутствии Исполнителя по последнему известному Заказчику адресу, либо уведомления об истечении срока хранения корреспонденции органами связи и т.п.

5.3. При неисполнении/ненадлежащем исполнении Исполнителем обязательств по Договору, в

Согласовано: _____
секретарь конкурсной комиссии
АО «Тюменьэнерго» Дурасова Н.И.

Согласовано: Департамент правового обеспечения
АО «Тюменьэнерго»

том числе, при расторжении договора в связи с невыполнением/ненадлежащим выполнением обязательств Исполнителем, Заказчик вправе взыскать с Исполнителя штраф в размере 10% от суммы, указанной в п.3.3. (по сопровождению Системы) или п.3.4. (по техническому обслуживанию Системы) настоящего Договора. При этом Заказчик вправе удержать сумму штрафа из стоимости надлежаще оказанных Исполнителем и принятых Заказчиком услуг, подлежащих оплате.

5.4. Исполнитель несет ответственность за причиненный по его вине ущерб Заказчику согласно действующему законодательству Российской Федерации.

6. ОБЯЗАННОСТИ СТОРОН

6.1. При исполнении Договора Исполнитель обязан:

6.1.1. Обеспечить своевременное и качественное оказание услуг в соответствии с Техническим заданием (Приложение №1 к настоящему Договору).

6.1.2. В связи с внедрением в АО «Тюменьэнерго» интегрированной системы менеджмента Исполнитель обязан ознакомить свой персонал, а также свои подрядные организации с «Памяткой для ознакомления с системой экологических аспектов, рисков в области охраны здоровья и обеспечения безопасности труда, энергетического менеджмента в АО «Тюменьэнерго» персонала Общества, подрядных и других организаций, при выполнении работ на оборудовании Общества, в том числе с привлечением механизмов (Приложение №7 к настоящему Договору).

6.1.3. Соблюдать требования стандарта организации АО «Тюменьэнерго» СТО 05770629.29.240.013-2008 «Организация производственно-технологических процессов. Общие положения».

6.1.4. Соблюдать требования Регламента допуска подрядных и субподрядных организаций для работы на объектах АО «Тюменьэнерго», размещенного по адресу: http://www.te.ru/zakupki/vzaimodeistvie_s_podryadnymi_organizatsiyami/.

6.1.5. Обеспечить соблюдение персоналом подрядных и субподрядных организаций:

- правил внутреннего трудового распорядка, установленных Заказчиком;

- нормативных требований по охране труда, промышленной и пожарной безопасности, Правил технической эксплуатации электрических сетей, Правил по охране труда при эксплуатации электроустановок, и другой нормативно-технической документации, действующей на территории Российской Федерации.

6.1.6. Исполнитель несет ответственность перед Заказчиком за нарушение на объектах Заказчика работниками Исполнителя, работниками субподрядной организации, привлеченной Исполнителем для выполнения работ по договору, Правил технической эксплуатации электрических сетей, Правил по охране труда при эксплуатации электроустановок, и другой нормативно-технической документации, действующей на территории Российской Федерации. В случае выявления факта нарушения Заказчик вправе взыскать с Исполнителя штраф в размере 50 000 (пятьдесят) тысяч рублей за каждое нарушение. Факт нарушения подтверждается протоколом, согласно Положению АО «Тюменьэнерго» о проведении проверок по соблюдению правил охраны труда на рабочих местах, составленным и подписанным представителями Заказчика и Исполнителя. Исполнитель уплачивает Заказчику штраф, установленный в настоящем пункте в течение 5 (пяти) дней с даты получения соответствующего требования Заказчика.

6.1.7. В случае невыполнения графика оказания услуг по причине нарушения требований действующих правил, норм, инструкций, стандартов, регламентов по охране труда, промышленной и пожарной безопасности, Правил технической эксплуатации электрических сетей, Правил по охране труда при эксплуатации электроустановок, и другой нормативно-технической документации, действующей на территории Российской Федерации со стороны Исполнителя (субподрядчика) скорректировать график выполнения работ, компенсировать издержки или убытки, понесенные Заказчиком.

6.1.8. Не допускать своими действиями нарушений нормальной работы Системы.

6.1.9. В течение 10 календарных дней после подписания настоящего Договора, назначить приказом своего Представителя, уполномоченного выступать от имени Исполнителя по вопросам, касающимся исполнения настоящего Договора. Исполнитель имеет право заменить своего Представителя, направив письменное уведомление Заказчику не позднее 20 календарных дней до указанной замены.

6.1.10. Обеспечить решение возникающих в ходе оказания услуг технических и организационных вопросов совместно с Представителем Заказчика.

6.1.11. Немедленно известить Представителя Заказчика о независимых от Исполнителя обстоятельствах, угрожающих надежности и качеству результатов оказания услуг, либо создающих невозможность завершения их в срок, а также приостановить оказание услуг, до получения от него письменных указаний.

Согласовано:
секретарь конкурсной комиссии
АО «Тюменьэнерго» Дипасова Н.И.

Согласовано: Департамент правового обеспечения
АО «Тюменьэнерго»

6.1.12. Соблюдать Инструкцию по соблюдению правил информационной безопасности, которая находится по адресу http://www.te.ru/suppliers/vzaimodeystvie_s_podryadnymi_organizatsiyami/vypiska_instr_ib.docx «Выписка из инструкции по соблюдению правил информационной безопасности в АО «Тюменьэнерго» для работников подрядных организаций». В случае нарушения Исполнителем требований Инструкции по соблюдению правил информационной безопасности Заказчик вправе взыскать штраф в размере 10% от стоимости услуг за отчетный период (квартал/полугодие) оказания услуг по договору за каждый выявленный случай нарушения.

6.1.13. В день подписания договора со стороны Исполнителя, Исполнитель обязан направить Заказчику на электронный адрес Petrov-ea@te.ru в формате файла *.pdf **скан-копию подписанного договора** (со всеми приложениями к нему), с последующим направлением оригинала договора.

6.1.14. Исполнитель обязуется предоставлять Заказчику информацию: а) об изменении состава собственников Исполнителя (включая конечных бенефициаров), а также состава исполнительных органов Исполнителя; б) информацию об изменении состава собственников (включая конечных бенефициаров) привлекаемых субподрядчиков/соисполнителей Исполнителя, а также состава исполнительных органов привлекаемых субподрядчиков/соисполнителей. В целях раскрытия вышеуказанной информации не позднее 5 (пяти) рабочих дней с даты наступления соответствующего события (юридического факта) предоставляются сканированные документы, подтверждающие произошедшие изменения, а также оригинал согласия на обработку персональных данных физических лиц (руководителей, учредителей, участников, акционеров и т.д.) с подписью субъекта персональных данных по форме, утвержденной Заказчиком.

6.1.15. Исполнитель обязан согласовывать с Заказчиком привлечение третьих лиц и информировать его о заключении договоров с Субподрядчиками.

6.1.16. Исполнитель предоставляет Заказчику информацию об отнесении привлекаемых третьих лиц к субъектам малого и среднего предпринимательства до заключения договора (дополнительного соглашения о привлечении/замене третьих лиц).

В случае непредставления Исполнителем информации об отнесении привлекаемых третьих лиц к субъектам малого и среднего предпринимательства, Исполнитель уплачивает Заказчику штраф в размере 0,1% от стоимости договора.

В случае неисполнения Исполнителем обязательств по привлечению к исполнению договора третьих лиц (соисполнителей, субподрядчиков) из числа субъектов малого и среднего предпринимательства, Исполнитель уплачивает Заказчику штраф в размере 0,1% от стоимости договора *(абзац включается в текст договора только в случае наличия в конкурсной/закупочной документации требования о привлечении субъектов малого и среднего предпринимательства на оказание услуг, а также в случае наличия соответствующих обязательств по оферте Исполнителя, поданной на участие в закупочной процедуре).*

6.1.17. Исполнять требования 187-ФЗ от 26.07.2017 «О БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ».

6.1.18. Соблюдать Требования к встроенным средствам защиты информации автоматизированных систем технологического управления электросетевого комплекса группы компаний «Россети» (Приложение № 8 к настоящему Договору).

6.1.18. Выполнять иные обязанности, предусмотренные настоящим Договором.

6.2. Заказчик обязан:

6.2.1. Контролировать оказание услуг по Договору.

6.2.2. Контролировать соблюдение требований охраны труда, промышленной и пожарной безопасности, Правил технической эксплуатации электрических сетей, Правил по охране труда при эксплуатации электроустановок, и другой нормативно-технической документации, действующей на территории Российской Федерации персоналом Исполнителя (субподрядчика) и принимать действенные меры к нарушителям вплоть до отстранения от оказания услуг.

6.2.3. Обеспечить оплату и приемку надлежащим образом оказанных услуг.

6.2.4. Назначить технически квалифицированного Представителя, ответственного за подачу заявки, который должен располагать достаточными техническими знаниями, чтобы поддерживать эффективную связь со специалистом Исполнителя.

6.2.5. Предоставить Исполнителю всю необходимую и имеющуюся диагностическую информацию в отношении проблем, по которым запрашивается помощь.

6.2.6. Предоставлять Исполнителю необходимый дистанционный доступ к Системе Заказчика, чтобы помочь определить причину проблемы. Заказчик отвечает за необходимую защиту Системы Заказчика и всех, содержащихся в ней данных, в то время, когда Исполнитель с разрешения Заказчика осуществляет дистанционный вход в нее.

Согласовано:
секретарь закупочной комиссии

Согласовано: Департамент правового обеспечения
АО «Тюменьэнерго» Зубов В. В.

6.2.7. Обеспечить допуск Исполнителя для исполнения обязательств, принятых по настоящему Договору, на рабочие места в соответствии с «Правилами по охране труда при эксплуатации электроустановок» утвержденных Приказом Минтруда №328н от 24.07.2013г.

6.2.8. Использовать информацию, полученную при оказании Услуги, только для поддержки требований обработки информации внутри предприятия Заказчика.

6.2.9. Выполнять иные обязанности, предусмотренные настоящим Договором.

6.3. Заказчик вправе:

- при нарушении работниками Исполнителя, работниками третьих лиц, привлеченных Исполнителем для оказания услуг по Договору, требований действующих нормативных документов по охране труда, промышленной и пожарной безопасности, Правил технической эксплуатации электрических сетей, Правил по охране труда при эксплуатации электроустановок, и другой нормативно-технической документации, действующей на территории Российской Федерации отказаться от их дальнейшего допуска на объекты Заказчика.

7. ОБСТОЯТЕЛЬСТВА НЕПРЕОДОЛИМОЙ СИЛЫ (ФОРС-МАЖОР)

7.1. Стороны освобождаются от ответственности за частичное или полное неисполнение обязательств по настоящему Договору, если это неисполнение явилось следствием обстоятельств непреодолимой силы, возникших после заключения договора в результате событий чрезвычайного характера, которые Сторона не могла ни предвидеть, ни предотвратить разумными мерами (форс-мажор) и непосредственно повлиявших на исполнение обязательств по Договору.

7.2. К событиям чрезвычайного характера в контексте настоящего договора относятся: наводнение, землетрясение, шторм, эпидемии или иные проявления сил природы, а также война или военные действия.

7.3. При наступлении указанных в пункте 7.2 Договора обстоятельств, Сторона, для которой создавалась невозможность исполнения своих обязательств, должна немедленно известить об этом другую Сторону, приложив к извещению справку компетентного государственного органа.

7.4. При отсутствии своевременного извещения, предусмотренного в п.7.3. Договора, виновная Сторона обязана возместить другой Стороне убытки, причиненные не извещением или несвоевременным извещением.

7.5. Наступление обстоятельств, вызванных действием непреодолимой силы, влечет увеличение срока исполнения Договора на период действия указанных обстоятельств, если они действуют не более 1 месяцев. В случае действия этих обстоятельств более 1 месяцев любая из сторон вправе расторгнуть Договор в одностороннем внесудебном порядке, при этом стороны обязаны провести взаимные расчеты в течение 15 дней с момента расторжения Договора. При этом упущенная выгода не возмещается.

8. РАССМОТРЕНИЕ СПОРОВ

8.1. Все споры, разногласия или требования, возникшие из настоящего Договора или в связи с ним, в том числе касающиеся его заключения, изменения, исполнения, нарушения, расторжения, прекращения или недействительности, подлежат разрешению в арбитражном суде ХМАО-Югры в соответствии с действующим законодательством РФ. Досудебный порядок урегулирования спора обязателен. Срок ответа на претензию - 15 календарных дней со дня ее получения.

(если Подрядчик является дочерним хозяйственным обществом ПАО «Россети» или обществом, являющимся дочерним по отношению к дочернему хозяйственному обществу ПАО «Россети») Все споры, разногласия и требования, возникающие из настоящего договора (соглашения) или в связи с ним, в том числе связанные с его заключением, действием, изменением, исполнением, нарушением, расторжением, прекращением и действительностью, подлежат разрешению путем переговоров.

В случае невозможности урегулировать возникший спор путем переговоров, до обращения в суд он подлежит разрешению путем применения альтернативной процедуры урегулирования споров (медиации), на условиях и в порядке, установленном законодательством и Регламентом рассмотрения и урегулирования споров и конфликтов интересов в Группе компаний ПАО «Россети», утвержденным решением Совета директоров АО «Тюменьэнерго» (протокол № 24/15 от 29.12.2015).

Согласовано:
секретарь конкурсной комиссии
АО «Тюменьэнерго»

Согласовано: Департамент правового обеспечения
АО «Тюменьэнерго» Зубов В. В.

При не достижении сторонами соглашения об урегулировании спора путем медиации, он подлежит разрешению в порядке арбитража (третейского разбирательства), администрируемого Арбитражным центром при Российском союзе промышленников и предпринимателей (место нахождения – г. Москва) в соответствии с его правилами, действующими на дату подачи искового заявления.

Решения третейского суда являются обязательными, окончательными и оспариванию не подлежат.

9. КОНФИДЕНЦИАЛЬНОСТЬ

9.1. Стороны обязуются без взаимного предварительного письменного согласования не разглашать третьим лицам информацию, составляющую коммерческую тайну: информацию, полученную в ходе заключения настоящего Договора; информацию, относящуюся к предмету и условиям настоящего Договора (содержащуюся в тексте настоящего Договора, а также в документах, являющихся неотъемлемой частью настоящего Договора); информацию, полученную в ходе исполнения Сторонами обязательств по настоящему Договору (далее – конфиденциальная информация)¹. Срок неразглашения конфиденциальной информации устанавливается Сторонами в течение всего срока действия Договора, а также в течение трех лет после прекращения данного срока.

9.2. Каждая из Сторон обязуется предпринять все разумные меры, необходимые и целесообразные для предотвращения несанкционированного раскрытия конфиденциальной информации.

9.3. Стороны обязуются не использовать незаконно конфиденциальную информацию, а также обязуются незамедлительно информировать друг друга о ставших им известными угрозе разглашения, разглашении или ином незаконном использовании конфиденциальной информации, о случаях запросов конфиденциальной информации третьими лицами, в том числе органами государственной власти, иными государственными органами, органами местного самоуправления.

9.4. За разглашение или незаконное использование конфиденциальной информации Сторона, нарушившая обязательства, предусмотренные данным разделом настоящего Договора, обязана возместить потерпевшей Стороне причиненные убытки.

10. АНТИКОРРУПЦИОННАЯ ПОЛИТИКА

10.1. Исполнителю известно о том, что АО «Тюменьэнерго» реализует требования статьи 13.3 Федерального закона от 25.12.2008 № 273-ФЗ «О противодействии коррупции», принимает меры по предупреждению коррупции, присоединилось к Антикоррупционной хартии российского бизнеса (свидетельство от 01.07.2015 № 414), ведет Антикоррупционную политику и развивает не допускающую коррупционных проявлений культуру, поддерживает деловые отношения с контрагентами, которые гарантируют добросовестность своих партнеров и поддерживают антикоррупционные стандарты ведения бизнеса.

10.2. Исполнитель настоящим подтверждает, что он ознакомился с Антикоррупционной хартией российского бизнеса и Антикоррупционной политикой ПАО «Россети» и ДЗО ПАО «Россети», представленных в разделе «Антикоррупционная политика» на официальном сайте АО «Тюменьэнерго» по адресу: http://www.te.ru/about/anticorruptionnaya_politika/, -полностью принимает положения Антикоррупционной политики ПАО «Россети» и ДЗО ПАО «Россети» и обязуется обеспечивать соблюдение ее требований как со своей стороны, так и со стороны аффилированных с ним физических и юридических лиц, действующих по настоящему Договору, включая собственников, должностных лиц, работников и/или посредников.

10.3. При исполнении своих обязательств по настоящему Договору Стороны, их аффилированные лица, работники или посредники не выплачивают, не предлагают выплатить и не разрешают выплату каких-либо денежных средств или ценностей, прямо или косвенно, любым лицам для оказания влияния на действия или решения этих лиц с целью получить какие-либо неправомерные преимущества или достичь иные неправомерные цели.

Стороны отказываются от стимулирования каким-либо образом работников друг друга, в том числе путем предоставления денежных сумм, подарков, безвозмездного выполнения в их адрес работ (услуг) и другими, не поименованными здесь способами, ставящими работника в определенную

¹ За исключением информации, являющейся общедоступной; информации, в отношении которой в соответствии с действующим законодательством РФ не может быть установлен режим коммерческой тайны; информации, подлежащей раскрытию в соответствии с действующим законодательством РФ.

зависимость и направленным на обеспечение выполнения этим работником каких-либо действий в пользу стимулирующей его стороны (Исполнителя и АО «Тюменьэнерго»).

10.4. В случае возникновения у одной из Сторон подозрений, что произошло или может произойти нарушение каких-либо положений пунктов 10.1 – 10.3, указанная Сторона обязуется уведомить другую Сторону в письменной форме. После письменного уведомления Сторона имеет право приостановить исполнение настоящего Договора до получения подтверждения, что нарушения не произошло или не произойдет. Это подтверждение должно быть направлено в течение десяти рабочих дней с даты направления письменного уведомления.

В письменном уведомлении Сторона обязана сослаться на факты и/или предоставить материалы, достоверно подтверждающие или дающие основание предполагать, что произошло или может произойти нарушение каких-либо положений пунктов 10.1, 10.2 любой из Сторон, аффилированными лицами, работниками или посредниками.

10.5. В случае нарушения одной из Сторон обязательств по соблюдению требований Антикоррупционной политики, предусмотренных пунктами 10.1, 10.2, и обязательств воздерживаться от запрещенных в пункте 10.3 настоящего раздела действий и/или неполучения другой стороной в установленный срок подтверждения, что нарушения не произошло или не произойдет, Исполнитель или Заказчик имеет право расторгнуть настоящий Договор в одностороннем порядке, полностью или в части, направив письменное уведомление о расторжении. Сторона, по чьей инициативе был расторгнут настоящий Договор, в соответствии с положениями настоящего пункта, вправе требовать возмещения реального ущерба, возникшего в результате такого расторжения.

11. ПРОЧИЕ УСЛОВИЯ

11.1. Переход возникших из настоящего договора прав требований к Заказчику, зачет взаимных требований без письменного согласия Заказчика не допускается. Уступка прав требований к Заказчику оформляется трехсторонним договором.

Если договор заключается с субъектом малого и среднего предпринимательства, договор должен содержать следующее условие:

«Подрядчик вправе переуступить право требования оплаты по выполненным договорным обязательствам в пользу иного лица (финансового агента). При этом Подрядчик направляет Заказчику (уполномоченному представителю Заказчика оригинал письменного уведомления об уступке денежного требования в течение 2 (двух) рабочих дней со дня осуществления уступки. В уведомлении об уступке денежного требования должно быть определено подлежащее исполнению денежное требование, а также указан финансовый агент, которому должен быть произведен платеж. День осуществления уступки – дата подписания Соглашения о переуступке прав требований между Подрядчиком и Фактором.

Соглашение между Финансовым агентом (Фактором) и Подрядчиком по переуступке права денежного требования по договору с Заказчиком должно содержать обязательство исполнения Подрядчиком регрессных требований Фактора (факторинг с правом регресса).

В случае переуступки Подрядчиком права денежного требования по договору с Заказчиком с нарушением условий, указанных в пункте 1 и / или 2, Подрядчик уплачивает Заказчику штраф за каждое нарушение в размере 1% от стоимости заключенного договора.»

11.2. Все изменения и дополнения к настоящему Договору действительны, если они совершены в форме дополнительного соглашения к Договору, подписаны и скреплены печатями обеих Сторон.

11.3. Все документы и иные сообщения, которые должны или могут направляться в соответствии с настоящим Договором, переданные по электронной почте либо факсимильной связью, принимаются к исполнению. Одновременно, заказным почтовым отправлением с уведомлением о вручении или курьером должны быть направлены оригиналы данных документов на бумажном носителе.

11.4. В случае изменения почтового адреса, телефонов, банковских реквизитов, полномочий должностных лиц и выданных им доверенностей Стороны обязаны уведомить об этом друг друга в течение 3 (трех) дней со дня наступления изменений. Для Сторон такие изменения становятся обязательными к исполнению со дня их получения. Оформление дополнительного соглашения к настоящему Договору при этом не требуется. При невыполнении данных требований, расчеты, а также иная информация, переданная по ранее действовавшим реквизитам, будет считаться полученной.

Согласовано:
секретарь конкурсной комиссии
АО «Тюменьэнерго» Давыдова И.И.

Согласовано: Департамент правового обеспечения
АО «Тюменьэнерго» Зубов В. В.

11.5. В соответствии со ст.431.2 ГК РФ Исполнитель заверяет Заказчика о следующих обстоятельствах, имеющих значение для заключения, исполнения настоящего Договора:

- Исполнитель надлежащим образом учрежден, действует и отвечает всем требованиям законодательства РФ;

- лицо, подписывающее договор, дополнительные и иные соглашения к Договору, первичные учетные документы от имени и по поручению Исполнителя на день подписания (заключения) имеет все необходимые для такого подписания полномочия;

- Исполнитель имеет все необходимые разрешения/одобрения компетентного органа Исполнителя на заключение и/или исполнение Договора, полученные с соблюдением всех корпоративных и иных процедур, требований действующего законодательства РФ и учредительных документов Исполнителя;

- Исполнитель имеет право осуществлять виды деятельности, предусмотренные настоящим Договором получены все необходимые разрешения, сертификаты, лицензии и прочие документы,

На основании ст. 406.1 ГК РФ Стороны договорились, что Исполнитель обязуется по письменному требованию Заказчика возместить в полном объеме все имущественные потери (упущенную выгоду и реальный ущерб) Заказчика, возникшие вследствие недостоверности вышеуказанных заверений, в том числе имущественные потери, возникшие в связи с предъявлением к Заказчику претензий, санкций и прочих требований третьих лиц, возникновением возможных споров (в т.ч. судебных), как влекущих за собой расторжение Договора либо признание его недействительным, так и не влекущих расторжение/признание недействительным Договора.

Заказчик вправе потребовать, а Исполнитель обязуется вместо возмещения Заказчику вышеуказанных имущественных потерь оплатить неустойку в размере 10% от цены Договора за каждый случай недостоверности вышеуказанных заверений.

11.6. Настоящий Договор подписан в двух подлинных экземплярах, имеющих одинаковую юридическую силу, по одному экземпляру для каждой из Сторон.

11.7. Во всем остальном, что прямо не предусмотрено условиями настоящего Договора, Стороны руководствуются действующим законодательством РФ.

11.8. Все Приложения к Договору являются его неотъемлемой частью.

12. СРОК ДЕЙСТВИЯ ДОГОВОРА. СРОКИ ОКАЗАНИЯ УСЛУГ

12.1. Договор вступает в силу с даты его заключения и действует до полного исполнения сторонами своих обязательств по нему.

12.2. Срок оказания услуг: 12 календарных месяцев с даты заключения настоящего Договора

12.3. Услуги по техническому обслуживанию Системы оказываются согласно Графику оказания услуг (Приложение № 4 к настоящему Договору). Услуги по сопровождению Системы – постоянно в течение срока действия Договора.

13. ПРИЛОЖЕНИЯ К ДОГОВОРУ

13.1. Приложение № 1 - Техническое задание

13.2. Приложение № 2 - Акты сдачи-приемки оказанных услуг (Форма)

13.3. Приложение № 3 - Журнал обращений Заказчика, отчет (Форма)

13.4. Приложение № 4 - График оказания услуг

13.5. Приложение № 5 – Сводный сметный расчет на оказание услуг

13.6. Приложение № 6 – Копия протокола по выбору Победителя

13.7. Приложение № 7 - Копия «Памятки для ознакомления с системой экологических аспектов, рисков в области охраны здоровья и обеспечения безопасности труда, энергетического менеджмента в АО «Тюменьэнерго» персонала Общества, подрядных и других организаций, при выполнении работ на оборудовании Общества, в том числе с привлечением механизмов»

13.8. Приложение № 8 – Требования к встроенным средствам защиты информации автоматизированных систем технологического управления электросетевого комплекса группы компаний «Россети».

14. АДРЕСА, РЕКВИЗИТЫ И ПОДПИСИ СТОРОН:

Исполнитель:

Заказчик:

Согласовано:
секретарь конкурсной комиссии
АО «Тюменьэнерго» Давыдов Н.И.

Согласовано: Департамент правового обеспечения
АО «Тюменьэнерго» Зубов В. В.

АО «Тюменьэнерго»

Место нахождения (почтовый адрес):
Россия, г. Сургут, Ханты-Мансийский
автономный округ – Югра,
ул. Университетская, 4.

Банковские реквизиты:

Р/с 40702810267170101719

в ПАО Сбербанк г. Тюмень

К/с 30101810800000000651

в ПАО Сбербанк г. Тюмень

ИНН 8602060185

КПП 997650001

ОКПО 05770629

БИК 047102651

ОГРН 1028600587399

_____/_____
МП

_____/_____
МП

Согласовано:
секретарь конкурсной комиссии
АО «Тюменьэнерго» *Деласова Н.И.*

Согласовано: Департамент правового обеспечения
АО «Тюменьэнерго» *Зубов В. В.*

ФОРМЫ

-----начало форм-----

АКТ № _____

сдачи-приемки оказанных услуг за _____ полугодие 201_ года
по техническому обслуживанию системы коллективного
отображения информации ДП ЦУС АО «Тюменьэнерго»

г. _____

«___» _____ 20_ г.

Мы, нижеподписавшиеся, Заказчик, в лице _____, действующего на основании _____, с одной стороны и Исполнитель, в лице _____, действующего на основании _____ с другой стороны, составили настоящий Акт о том, что согласно Договору № _____ от «___» _____ 20_ г. оказаны услуги по техническому обслуживанию системы коллективного отображения информации ДП ЦУС АО «Тюменьэнерго», на сумму _____ рублей, в том числе НДС (20%) _____ рублей:

№ п/п	Наименование вида (перечень) услуг и оборудования, в отношении которого оказывались услуги	Ед. изм.	Кол-во	Стоимость единицы, руб.	Общая стоимость, руб.
	Итого по акту:				
	НДС 20%:				
	Всего по акту с учетом НДС:				

Сведения о наличии/отсутствии у Заказчика претензий к оказанным услугам (качеству, срокам, объемам) _____

Настоящий акт является основанием для расчетов между Сторонами по договору.

ИСПОЛНИТЕЛЬ:

ЗАКАЗЧИК:
АО «Тюменьэнерго»

_____ (наименование должности)

_____ (наименование должности)

_____/_____/_____
(подпись) (Ф.И.О.)

МП

_____/_____/_____
(подпись) (Ф.И.О.)

МП

Согласовано:
секретарь конкурсной комиссии
АО «Тюменьэнерго» Зиндурская Н. И.

Согласовано: Департамент правового обеспечения
АО «Тюменьэнерго» Зубов В. В.

Акт сдачи-приемки оказанных услуг №

по договору № _____ от _____ 201_ г.

г. Сургут

« _____ » _____ 201_ г.

Мы, нижеподписавшиеся, Заказчик АО «Тюменьэнерго», в лице _____, действующего на основании _____, с одной стороны, и Исполнитель _____ в лице _____, действующего на основании _____, с другой стороны, составили настоящий Акт о том, что Исполнитель оказал услуги по сопровождению системы коллективного отображения информации ДП ЦУС АО «Тюменьэнерго» в _____ квартале 201_ г.

№ п/п	Наименование услуг	Ед. изм.	Кол-во	Стоимость единицы, руб.	Общая стоимость, руб.
1					
	Итого по акту:				
	НДС 20%:				
	Всего по акту с учетом НДС:				

Сведения о наличии/отсутствии у Заказчика претензий к оказанным услугам (качеству, срокам, объемам) _____

Настоящий акт является основанием для расчетов между Сторонами по договору.

ИСПОЛНИТЕЛЬ:

ЗАКАЗЧИК:
АО «Тюменьэнерго»

_____ (наименование должности)

_____ (наименование должности)

_____/_____
(подпись) (Ф.И.О.)

МП

_____/_____
(подпись) (Ф.И.О.)

МП

-----конец форм-----

Формы Актов сдачи-приемки оказанных услуг согласовали

ИСПОЛНИТЕЛЬ:

ЗАКАЗЧИК:
АО «Тюменьэнерго»

_____/_____
МП

_____/_____
МП

Согласовано:
секретарь конкурсной комиссии
АО «Тюменьэнерго» Дугарова Н. И.

Согласовано: Департамент правового обеспечения
АО «Тюменьэнерго» Зубов В. В.

ОТЧЕТ
по оказанию услуг по сопровождению системы
коллективного отображения информации ДП ЦУС

Принято в обработку запросов (заявок) - _____, в том числе: (заполняется при наличии)

По запросам Заказчика инициировано дополнительных услуг (заданий) - _____, в том числе:
(заполняется при наличии)

Представитель _____ /Ф.И.О./
подпись

Согласовано:
секретарь конкурсной комиссии
АО «Тюменьэнерго» *Дурасова Н.П.*

Согласовано: Департамент правового обеспечения
АО «Тюменьэнерго» *Зубов В. В.*

Журнал обращений заказчика

№	Дата	Время обращения	Дата исполнения	Филиал	ФИО обратившегося	Объект	Причина обращения	Примечания

ИСПОЛНИТЕЛЬ:

ЗАКАЗЧИК:
АО «Тюменьэнерго»

_____/_____/_____
МП

_____/_____/_____
МП

Согласовано:
секретарь конкурсной комиссии
АО «Тюменьэнерго» *Давыдова Н.Н.*

Согласовано: Департамент правового обеспечения
АО «Тюменьэнерго» *Зубов В. В.*

График оказания услуг
по техническому обслуживанию системы коллективного
отображения информации ДП ЦУС АО «Тюменьэнерго»

№ п/п	Наименование	График оказания услуг (календарный месяц) 2019 г.											
		1	2	3	4	5	6	7	8	9	10	11	12
1.	Система коллективного отображения информации ДП ЦУС												

Примечание: ■ - календарный месяц оказания услуг по техническому обслуживанию системы

ИСПОЛНИТЕЛЬ:

ЗАКАЗЧИК:
АО «Тюменьэнерго»

МП

МП

Согласовано:
секретарь конкурсной комиссии
АО «Тюменьэнерго» *Дурасова Н.И.*

Согласовано: Департамент правового обеспечения
АО «Тюменьэнерго» *Зубов В. В.*

Сводный сметный расчет стоимости

№ п/п	Наименование работ	Номер сметы (расчета)	Стоимость услуги в текущих ценах, руб. без НДС	НДС 20%, руб.	Стоимость услуги, руб. с НДС
1	2	3	4	5	6
1	Сопровождение системы коллективного отображения информации ДП ЦУС				
2	Техническое обслуживание системы коллективного отображения информации ДП ЦУС				
	Итого:				

Исполнитель

_____ (наименование должности)

_____/_____
(Ф.И.О.)

МП

Заказчик

АО "Тюменьэнерго"

_____ (наименование должности)

_____/_____
(Ф.И.О.)

МП

Согласовано:
секретарь конкурсной комиссии
АО «Тюменьэнерго» Дурасова В.И.

Согласовано: Департамент правового обеспечения
АО «Тюменьэнерго» Зубов В. В.

УТВЕРЖДАЮ

И.о. первого заместителя
генерального директора –
главного инженера
АО «Тюменьэнерго»

 Боровицкий В.Г.

«03» 09 2015 г.

ПАМЯТКА


Для ознакомления с системой экологических аспектов, рисков в области охраны здоровья и обеспечения безопасности труда, энергетического менеджмента в АО «Тюменьэнерго» персонала Общества, подрядных и других организаций, при выполнении работ на оборудовании Общества, в том числе с привлечением механизмов.

1. В АО «Тюменьэнерго» разработана, внедрена, функционирует и поддерживается в рабочем состоянии интегрированная система менеджмента (ИСМ), соответствующая требованиям международных стандартов:
 - 1.1. ISO 9001 «Системы менеджмента качества».
 - 1.2. ISO 14001 «Системы управления окружающей средой. Требования и руководство по применению».
 - 1.3. ISO 18001 «Системы менеджмента охраны здоровья и обеспечения безопасности труда. Требования».
 - 1.4. ISO 50001 «Система энергетического менеджмента. Требования и руководство по применению».
2. Персонал, выполняющий работы на оборудовании АО «Тюменьэнерго», обязан соблюдать следующие правила:
 - 2.1. Знать требования Политики ИСМ и способствовать их выполнению.
 - 2.2. Все работы производить в строгом соответствии с действующими процедурами, инструкциями, правилами и нормами, а также предупреждать возможные последствия отклонения от установленных процедур.
 - 2.3. Осуществлять сбор и размещение отходов и мусора в специально отведенных для этого местах и контейнерах.
 - 2.4. Не допускать разлива, утечек и протечек нефтепродуктов, лакокрасочных, горюче-смазочных и иных вредных химических веществ, в случае разлива немедленно произвести очистку.
 - 2.5. Использовать автотранспорт и строительно-дорожную технику, прошедшие контроль содержания вредных веществ отработанных газов, согласно установленному порядку.
 - 2.6. Не допускать попадания отходов и мусора на почву, в ливневые стоки, на тропинки, тротуары и дороги - проводить немедленную их очистку.
 - 2.7. Самостоятельно проводить уборку рабочих мест и территории после окончания работы, обеспечить содержание земельного участка в надлежащем виде.
 - 2.8. Нести ответственность за нарушение почвенно-растительного слоя вне границ земельного отвода и загрязнение территории производственными и бытовыми отходами, нефтепродуктами.
 - 2.9. Ознакомиться с Реестром экологических аспектов деятельности АО «Тюменьэнерго», правилами безопасного обращения с отходами: «Правила обращения с отходами производства и потребления в ОАО «Тюменьэнерго» ПР 05770629.23.001-2009, «Инструкцией по практическому ведению работ с отходами 1-3 классов опасности» ИН 05770629-07-23-002-2009.
 - 2.10. Работники обязаны соблюдать правила промышленной и пожарной безопасности, выполнять требования охраны труда, установленные правилами и инструкциями по охране труда.



Система управления АО «Тюменьэнерго» работает в соответствии с требованиями международных стандартов ISO 9001, ISO 14001, ISO 18001, GHSAS 18001

Согласовано:
секретарь конкурсной комиссии
АО «Тюменьэнерго» 

Согласовано: Департамент правового обеспечения
АО «Тюменьэнерго» 

- 2.11. Не допускать к выполнению работ в электроустановках работников, не ознакомившихся с перечнем потенциальных опасностей при выполнении работ на объектах АО «Тюменьэнерго», не прошедших обучение, инструктаж, стажировку, проверку знаний, обязательные медицинские осмотры.
- 2.12. Перед началом работы персонал должен быть обеспечен всеми необходимыми сертифицированными средствами индивидуальной и коллективной защиты, обучен правилам применения средств защиты и обязан пользоваться ими для обеспечения безопасности труда.
- 2.13. Весь персонал должен быть обучен безопасным методам и приемам выполнения работ, и оказанию первой помощи при несчастных случаях на производстве, должен быть обеспечен инструкциями по охране труда по профессиям и видам выполняемых работ.
- 2.14. Исполнитель (подрядчик) обязан соблюдать действующие стандарты и требования АО «Тюменьэнерго» установленные в области охраны окружающей среды и в области охраны здоровья и обеспечения безопасности труда.
- 2.15. Исполнитель (подрядчик) в ходе работы не в праве выполнять указания АО «Тюменьэнерго», если это может привести к нарушению требований, обязательных для сторон по охране окружающей среды и охраны здоровья и обеспечения безопасности труда.
- 2.16. Работники должны быть осведомлены о существующем или потенциальном влиянии своей деятельности на потребление энергоресурсов и потери электроэнергии на объектах АО «Тюменьэнерго».
- 2.17. Обеспечивать рациональное и экономное использование всех энергоресурсов, получаемых от АО «Тюменьэнерго», а также принимать все необходимые меры по минимизации потерь этих энергоресурсов.
- 2.18. Не допускать работу осветительных приборов в дневное время, если уровень естественной освещенности соответствует требованиям охраны труда и технике безопасности.
- 2.19. Рационально и экономно использовать нагревательные приборы и другое энергопотребляющее оборудование.
- 2.20. Планировать и реализовывать мероприятия по энергосбережению.
- 2.21. Обеспечивать учёт потребляемых энергоресурсов.
- 2.22. Отдавать предпочтение применению энергосберегающего оборудования.
- 2.23. Понимать важность энергосбережения и его экономические выгоды.
- 2.24. Поддерживать состояние используемого энергопотребляющего оборудования в соответствии с нормативными документами.
3. Персонал АО «Тюменьэнерго», подрядных и других организаций, которые выполняют работы на оборудовании АО «Тюменьэнерго», несет ответственность за выполнение перечисленных выше правил.



Система сертификации АО «Тюменьэнерго» работает в соответствии с требованиями международных стандартов ISO 9001, ISO 14001, ISO 50001, GRISSAS 18001

Согласовано:
секретарь конкурсной комиссии
АО «Тюменьэнерго» Давыдов Н.И.

Согласовано: Департамент правового обеспечения
АО «Тюменьэнерго» Зубов В. В.

Приложение 8
к Договору № _____
от «__» _____ 201_ г.

**ТРЕБОВАНИЯ
К ВСТРОЕННЫМ СРЕДСТВАМ ЗАЩИТЫ ИНФОРМАЦИИ
АВТОМАТИЗИРОВАННЫХ СИСТЕМ
ТЕХНОЛОГИЧЕСКОГО УПРАВЛЕНИЯ
ЭЛЕКТРОСЕТЕВОГО КОМПЛЕКСА
ГРУППЫ КОМПАНИЙ «РОССЕТИ»**

Москва
2018

Согласовано:
секретарь конкурсной комиссии
АО «Тюменьэнерго» *Зубов В. В.*

Согласовано: Департамент правового обеспечения
АО «Тюменьэнерго» Зубов В. В.

ОГЛАВЛЕНИЕ

1 ОБЩИЕ СВЕДЕНИЯ.....	5
1.1 Цель разработки документа.....	5
1.2 Основание для разработки.....	5
1.3 Область применения.....	5
1.4 Целевой пользователь документа.....	6
1.5 Нормативные ссылки.....	6
2 ОБЩИЕ ПОЛОЖЕНИЯ	7
3 ОПИСАНИЕ ОО	9
3.1 Описание ОО.....	9
3.2 Границы ОО	9
4 ОПРЕДЕЛЕНИЕ ПРОБЛЕМЫ БЕЗОПАСНОСТИ.....	9
4.1 Активы	9
4.2 Угрозы безопасности для объекта оценки	10
4.3 Угрозы безопасности для среды функционирования	11
4.4 Политики безопасности группы компаний.....	11
4.5 Предположения безопасности.....	12
5 ЦЕЛИ БЕЗОПАСНОСТИ	13
5.1 Цели безопасности для ОО.....	13
5.2 Цели безопасности для среды функционирования	14
5.3 Обоснование целей безопасности.....	15
6 ТРЕБОВАНИЯ БЕЗОПАСНОСТИ.....	16
6.1 Функциональные требования безопасности.....	16
6.2 Требования доверия к безопасности.....	22
6.3 Обоснование требований безопасности.....	32
7 ОТВЕТСТВЕННОСТЬ	33

Согласовано:
секретарь конкурсной комиссии
АО «Тюменьэнерго» *Зубов В.В.*

Согласовано: Департамент правового обеспечения
АО «Тюменьэнерго» Зубов В. В.

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Термин	Определение
Автоматизированная система	Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций (в соответствии с ГОСТ 34.003-90 Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения)
Доверие	Основание для уверенности в том, что изделие отвечает целям безопасности
Задание безопасности по	Совокупность требований безопасности и спецификаций, предназначенная для использования в качестве основы для оценки безопасности конкретного изделия
Информационные технологии	Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов (в соответствии с Федеральным законом Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»)
Объект оценки	Подлежащие оценке продукт или система; в контексте настоящих Требований - устройство, оборудование или АСТУ и ее подсистемы
Подразделение ИБ	Подразделение ПАО «Россети», на которое возложены функции планирования, организации, реализации и контроля мероприятий по обеспечению информационной безопасности
Политика безопасности организации	Совокупность руководящих принципов, правил, процедур и практических приемов в области безопасности, которыми руководствуется организация в своей деятельности
Предположения	Условия, которые должны быть обеспечены в среде, чтобы изделие ИТ могло рассматриваться как безопасное. Условия, которые должны быть обеспечены в среде, при которых может рассматриваться как безопасное
Профиль защиты	Независимая от реализации совокупность требований безопасности для некоторой категории изделий, отвечающая специфическим запросам потребителя
Среда безопасности	Область среды, в пределах которой предусматривается обеспечение необходимых условий для поддержания требуемого режима безопасности изделия
Угроза	Совокупность условий и факторов, определяющих потенциальную или реально существующую опасность возникновения инцидента, который может привести к нанесению ущерба изделию или его владельцу
Функция безопасности	Функциональные возможности части или частей изделия ИТ, обеспечивающие выполнение подмножества взаимосвязанных требований безопасности
Цель безопасности	Сформулированное намерение противостоять установленным угрозам и/или удовлетворять установленной политике безопасности организации и предположениям

Согласовано:
секретарь конкурсной комиссии
АО «Тюменьэнерго» Дудасова И. И.

Согласовано: Департамент правового обеспечения
АО «Тюменьэнерго» Зубов В. В.

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

Сокращение	Полная форма
АРМ	Автоматизированное рабочее место
АИИС КУЭ	Автоматизированные информационно-измерительные системы коммерческого учета электроэнергии
АСТУ	Автоматизированные системы технологического управления
АСОТСУ	Автоматизированные системы оперативно-технологического и ситуационного управления
АСУ ТП	Автоматизированные системы управления технологическими процессами
ВСЗИ	Встроенные средства защиты информации АСТУ
ЗБ	Задание по безопасности
ИБ	Информационная безопасность
ИТ	Информационные технологии
ЛВС	Локальная вычислительная сеть
ОМП	Системы определения места повреждения
ОО	Объект оценки
ОРД	Организационно-распорядительный документ
ПА	Системы противоаварийной автоматики
ПЗ	Профиль защиты
ПО	Программное обеспечение
РАСП	Системы регистрации аварийных событий и процессов
РЗА	Системы релейной защиты и автоматики
СВТ	Средства вычислительной техники
СМНР	Системы мониторинга переходных режимов
ТДБ	Требование доверия безопасности
ФБО	Функции безопасности ОО
ФТБ	Функциональное требование безопасности

Согласовано:
секретарь закупочной комиссии
АО «Тюменьэнерго» Давыдова Н. И.

Согласовано: Департамент правового обеспечения
АО «Тюменьэнерго» Зубов В. В.

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Цель разработки документа

Целью разработки требований к встроенным средствам защиты информации автоматизированных систем технологического управления электросетевого комплекса Группы компаний «Россети» (далее - Требования) является обеспечение условий, при которых создание, модернизация и применение на объектах электросетевого комплекса Группы компаний «Россети» автоматизированных систем технологического управления и оборудования, являющегося частью указанных систем, не ведет к возникновению угроз информационной безопасности и/или снижению уровня защищенности объектов электросетевого комплекса от деструктивных воздействий извне, а, напротив, значительно увеличивает способность противостоять им с одновременным сокращением финансовых, материальных и трудовых ресурсов, затрачиваемых на обеспечение информационной безопасности электросетевого комплекса, посредством реализации в составе АСТУ и/или оборудования функций и механизмов безопасности.

Указанные цели достигаются за счет установления единых и прозрачных критериев оценки возможности применения на объектах электросетевого комплекса Группы компаний «Россети» тех или иных автоматизированных систем технологического управления и их подсистем, включая оборудование, с позиции обеспечения информационной безопасности.

1.2 Основание для разработки

Настоящий нормативный документ разработан и утвержден в соответствии с «Программой создания комплексной системы информационной безопасности электросетевого комплекса группы компаний ПАО «Россети» на 2016-2020 годы, утвержденной решением Правления ПАО «Россети» (протокол от 22.09.2015 № 382пр) на основании «Концепции обеспечения информационной безопасности ПАО «Россети», утвержденной распоряжением Общества от 17.06.2014 № 249р, во исполнение пункта 1 статьи 11 Федерального закона Российской Федерации от 21.07.2011 № 256 «О безопасности объектов топливно-энергетического комплекса» и положений приказа ФСТЭК России от 14.03.2014 № 31 «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

Требования опираются на положения Методики и Порядка проведения аттестации оборудования, материалов и систем в электросетевом комплексе, утвержденных решением Правления ОАО «Россети» (протокол от 31.01.2014 № 225пр) и Положения ПАО «Россети» о единой технической политике в электросетевом комплексе, утвержденного Советом директоров ПАО «Россети» (протокол от 20.02.2017 № 252).

1.3 Область применения

Требования настоящего документа должны применяться при выполнении работ по защите, созданию, модернизации и эксплуатации, приемке (включая процесс аттестации оборудования, материалов и систем в электросетевом комплексе ПАО «Россети») и испытаний систем, входящих в состав автоматизированных систем технологического управления ПАО «Россети» и его дочерних и зависимых обществ (ДЗО), а также при проведении оценки соответствия в форме сертификации компонентов АСТУ и оборудования в системе сертификации ФСТЭК России (включая связанный с процедурой сертификации процесс разработки заданий по безопасности, профилей защиты и протоколов испытаний в соответствии с ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий»).

Городишанов:

Согласовано: Департамент правового обеспечения
АО «Тюменьэнерго» Зубов В. В.

Настоящие требования распространяются на аппаратно-программное обеспечение, применяемое в составе систем АСТУ, в том числе предназначенное для управления и встроенное в оборудование соответствующих подсистем.

Автоматизированная система технологического управления включает в себя (в соответствии с СТО ОАО «Россети» 34.01-6.2-001-2014):

- автоматизированные системы оперативно-технологического и ситуационного управления;

- автоматизированные системы объектового уровня;
- системы технологической связи.

Автоматизированные системы объектового уровня включают в себя:

- автоматизированные системы управления технологическими процессами;
- системы телемеханики;
- системы определения места повреждения;
- автоматизированные информационно-измерительные системы коммерческого учета электроэнергии;
- системы релейной защиты и автоматики;
- системы противоаварийной автоматики;
- системы регистрации аварийных событий и процессов;
- системы мониторинга переходных режимов;
- автоматизированные системы мониторинга и диагностики оборудования;
- системы сигнализации состояния вспомогательных и инженерных систем подстанций (видеонаблюдение, пожаротушение).

1.4 Целевой пользователь документа

Настоящий документ предназначен для работников структурных подразделений ПАО «Россети» и ДЗО ПАО «Россети», задействованных в реализации проектов по защите, созданию, модернизации и эксплуатации, приемке и испытаниям систем, входящих в состав автоматизированных систем технологического управления ПАО «Россети» и ДЗО, структурных подразделений, обеспечивающих деятельность по аттестации систем, оборудования и материалов для применения на объектах Группы компаний «Россети», а также производителей программного обеспечения подсистем, входящих в состав АСТУ и встроенного в оборудование, организаций, осуществляющих в соответствии с законодательством Российской Федерации работы по созданию средств защиты информации и заявителей на осуществление сертификации продукции в системе сертификации ФСТЭК России для нужд Группы компаний «Россети» и испытательных лабораторий.

1.5 Нормативные ссылки

Требования разработаны с использованием следующих национальных стандартов Российской Федерации и стандартов Группы компаний «Россети»:

- СТО 34.01-6.2-001-2014 «Автоматизированные системы оперативно-технологического и ситуационного управления типовые функциональные требования»;
- ГОСТ Р ИСО/МЭК 15408 (-1-2012, -2-2013, -3-2013) «Информационная технология. Методы и средства обеспечения безопасности Критерии оценки безопасности информационных технологий»;
- ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования»;
- ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»;
- ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения»;
- ГОСТ Р 51583-2014 «Защита информации. Порядок создания автоматизированных систем. Общие положения»;

Согласовано
секретарь конкурсной комиссии
АО «Тюменьэнерго» Дудасов И. И.

Согласовано: Департамент правового обеспечения
АО «Тюменьэнерго» Зубов В. В.

- ГОСТ Р 52069.0-2013 «Защита информации. Система стандартов. Основные положения»;
- ГОСТ Р 52447-2005 «Защита информации. Техника защиты информации. Номенклатура показателей качества»;
- ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения»;
- ГОСТ Р 53115-2008 «Защита информации. Испытание технических средств обработки информации на соответствие требованиям защищенности от несанкционированного доступа. Методы и средства»;
- ГОСТ Р 53131-2008 «Защита информации. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. Общие положения»;
- ГОСТ Р 54581-2011 «Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий»;
- ГОСТ Р ИСО 7498-1-99 «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель»;
- ГОСТ Р ИСО 7498-2-99 «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации»;
- ГОСТ Р ИСО/МЭК ТО 15446-2008 «Информационная технология. Методы и средства обеспечения безопасности. Руководство по разработке профилей защиты и заданий по безопасности»;
- ГОСТ Р ИСО/МЭК 18045-2013 «Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий»;
- ГОСТ Р ИСО/МЭК ТО 19791-2008 «Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем»;
- ГОСТ Р ИСО/МЭК 21827-2010 «Информационная технология. Методы и средства обеспечения безопасности. Проектирование систем безопасности. Модель зрелости процесса»;
- ГОСТ Р ИСО/МЭК 27034-1-2014 «Информационная технология. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 1. Обзор и общие понятия».

2 ОБЩИЕ ПОЛОЖЕНИЯ

Принципом формирования настоящих Требований являются главенство интересов Российской Федерации и Группы компаний «Россети».

Компоненты АСТУ, поставляемые и эксплуатируемые на объектах электросетевого комплекса Группы компаний «Россети», должны обладать ВСЗИ. Изготовитель АСТУ и/или электрооборудования обязан подтвердить соответствие ВСЗИ настоящим Требованиям в форме сертификации указанного оборудования и/или программного обеспечения в системе сертификации ФСТЭК России на соответствие:

- ЗБ, разработанному с учетом Требований настоящего документа (с предоставлением, при необходимости, Обоснования соответствия – см. ниже);
- требованиям руководящего документа Гостехкомиссии России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей» по 4 уровню контроля.

Настоящие требования по структуре, составу и форме представления приближены к ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности Критерии оценки безопасности информационных технологий» с целью повышения эффективности взаимодействия всех участников процесса оценки соответствия и обеспечения возможности разработки ЗБ/ПЗ на основании настоящих Требований.

Согласовано:
секретарь конкурсной комиссии
АО «Тюменьэнерго»

Согласовано: Департамент правового обеспечения
АО «Тюменьэнерго» Зубов В. В.

При разработке ЗБ/ПЗ для компонентов АСТУ/типов компонентов АСТУ допускается сокращение или дополнение множеств угроз/целей безопасности/ФТБ, обеспечивающих достижение целей безопасности относительно приведенного в настоящем документе, с сохранением связности отображения множеств угроз/целей безопасности/ФТБ. В этом случае для демонстрации соответствия компонента АСТУ требованиям настоящего документа составляется Обоснование соответствия, в котором обосновывается неактуальность (или, напротив, возможность реализации) определенных угроз для компонента АСТУ с исключением соответствующих целей безопасности/ФТБ.

ТДБ, приведенные в настоящем документе, сокращению при разработке ЗБ не подлежат. При разработке ЗБ/ПЗ допускается введение дополнительных ТДБ (включая сформулированные в явном виде) с соответствующим обоснованием.

Подтверждение реализации настоящих Требований представляет собой многоэтапный процесс:

- в соответствии с установленными в Группе компаний «Россети» «Методикой проведения аттестации оборудования, материалов и систем в электросетевом комплексе» и «Порядком проведения аттестации оборудования материалов и систем в электросетевом комплексе» получение заявки от изготовителя на допуск оборудования и систем для применения на объектах электросетевого комплекса Группы компаний «Россети»;

- принятие решения о необходимости прохождения процедуры оценки соответствия настоящим Требованиям, с оформлением решения в подразделении ИБ;

- изготовитель самостоятельно или с привлечением специализированной организации, разрабатывает задание по безопасности для объекта оценки и согласует его с Подразделением ИБ (при необходимости предоставляя Обоснование соответствия);

- прохождение процедуры сертификации в соответствии с Постановлением Правительства РФ от 26.06.1995 № 608 «О сертификации средств защиты информации» на соответствие требованиям ЗБ;

- изготовитель обязан направить в Подразделение ИБ протоколы сертификационных испытаний встроенных средств защиты информации (отчет по результатам сертификационных испытаний), проведенных испытательными лабораториями;

При выборе объекта оценки или АСТУ и оборудования, представляемого к допуску для применения в электросетевом комплексе, не должна быть утрачена общая оценка функционирования совокупности взаимодействующих элементов АСТУ, подсистем и оборудования, а также среды функционирования с связи с возможным сокрытием негативного синергетического эффекта, при котором совокупность не несущих угроз элементов приводит к появлению угроз информационной безопасности для всей АСТУ. Примером указанного случая является электрооборудование с внешней системой управления и конфигурации.

Учитывая сложность и временные рамки работ по реализации настоящих Требований и процедуры оценки соответствия при согласии изготовителя и подтверждении его намерений по реализации Требований в определенный согласованный со стороны подразделения ИБ срок, возможно осуществление временного допуска заявленных изготовителем компонентов АСТУ к применению в электросетевом комплексе ПАО «Россети». Для получения указанного временного допуска изготовитель предоставляет Утверждение о соответствии компонентов АСТУ настоящим Требованиям в части выполнения ФТБ с приведением отображения множества ФБО компонента АСТУ на множество ФТБ, определяемое настоящими Требованиями. Допускается предоставление проекта ЗБ и обоснования соответствия вместо упомянутого Утверждения о соответствии.

Указанный временный допуск оформляется в форме заключения аттестационной комиссии ПАО «Россети» с условием ограничения о допуске сроком на 1 год.

При этом подтверждением намерений изготовителя по реализации Требований может являться (в зависимости от этапа их реализации): заключение договора с органом по сертификации средств защиты информации и/или испытательной лабораторией,

Согласовано:
секретарь конкурсной комиссии
АО «Тиманьэнерго» Липовая Н.И.

Согласовано: Департамент правового обеспечения
АО «Тиманьэнерго» Зубов В.В.

включенными в соответствующие реестры ФСТЭК России, или организацией, обладающей действующей лицензией ФСТЭК России на проведение работ по технической защите информации, при этом предметом договора должны являться работы по реализации настоящих Требований или их этапы.

В случае поставки компонентов АСТУ на объекты электросетевого комплекса в течение действия временного допуска для указанных компонентов АСТУ, и при выявлении в ходе дальнейших сертификационных испытаний несоответствия компонентов АСТУ настоящим требованиям, изготовитель, по результатам реализации Требований, должен за свой счет произвести модернизацию и/или замену аппаратного и/или программного обеспечения поставленных ранее компонентов АСТУ, включая сопутствующие работы.

Временный допуск может быть оформлен изготовителю не более 2-х раз.

По результатам рассмотрения Утверждения о соответствии при оформлении временного допуска компоненты АСТУ могут допускаться к применению на электросетевом комплексе ПАО «Россети» с ограничениями применения, нейтрализующими потенциальные угрозы информационной безопасности, при этом реализация указанных ограничений может быть реализована технически или организационно.

3 ОПИСАНИЕ ОО

3.1 Описание ОО

Под ОО в настоящих требованиях подразумеваются ВСЗИ компонентов АСТУ, реализованные как программно (в большинстве случаев), так и аппаратно.

3.2 Границы ОО

3.2.1 Физические границы ОО

Физические границы ОО определяются физическими границами блоков, реализующих ФБО, или являющихся средой функционирования программных модулей ОО, реализующих ФБО. Каналы связи, за редким исключением, не входят в состав ОО и не подлежат оценке.

3.2.2 Логические границы ОО

Логические границы ОО определяются ФБО, реализуемыми ОО.

3.2.3 Среда функционирования

Средой функционирования ОО служат аппаратные средства, обеспечивающие функционирование программных модулей ОО, реализующих ФБО, или функционирование аппаратных модулей ОО (в случае аппаратной реализации ФБО), а также программные средства, являющиеся платформой для функционирования программных модулей ОО. Средой функционирования ОО могут являться (включая, но не ограничиваясь):

- Сервер общего назначения под управлением ОС семейства Windows;
- Сервер общего назначения под управлением ОС семейства Linux;
- Микропроцессорное устройство релейной защиты;
- Программируемый логический контроллер;
- Процессор связи в системе АСТУ;
- Набор каналов связи;
- И т.д.

Также неотъемлемой характеристикой среды функционирования является комплекс организационных и инженерно-технических мер безопасности, реализованных на технологических участках инфраструктуры ПАО «Россети», в т.ч. мер, реализованных согласно требованиям Федерального закона от 21.07.2011 № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса».

4 ОПРЕДЕЛЕНИЕ ПРОБЛЕМЫ БЕЗОПАСНОСТИ

4.1 Активы

Защищаемыми активами ОО являются:

Согласовано:
секретарь конкурсной комиссии
АО «Тюменьэнерго» Давыдова Н.И.

Согласовано: Департамент правового обеспечения
АО «Тюменьэнерго» Звбля Я. Я.

– Объекты постоянной и временной памяти ОО при защите от несанкционированной модификации или удаления, содержащие следующую информацию:

- Конфигурационная информация ОО;
- Информация подсистемы регистрации событий информационной и технологической безопасности.

– Объекты постоянной и временной памяти ОО при защите от несанкционированного чтения, модификации или удаления, содержащие следующую информацию:

- Данные учетных записей пользователей (включая пароли);
- Атрибуты безопасности.

– Исполняемый код программных модулей ОО при защите от несанкционированного чтения, модификации (нарушения целостности) или удаления.

– Функционал подсистемы безопасности ОО при защите от нарушения работоспособности.

4.2 Угрозы безопасности для объекта оценки

Настоящим документом определены следующие базовые угрозы информационной безопасности, которым противостоят ВСЗИ АСТУ.

T.NOAUTH

Обход средств защиты

Злоумышленник получает доступ к активам без соответствующей авторизации путем обхода ФБО.

T.REPEAT

Перебор аутентификационной информации

Злоумышленник реализует атаку, направленную на получение аутентификационной информации пользователей путем ее подбора.

T.SPYINF

Отслеживание аутентификационной информации

Злоумышленник реализует атаку, направленную на получение идентификационной и/или аутентификационной информации путем организации внешнего наблюдения.

T.CTRL_TAMP

Нарушение целостности

Злоумышленник реализует атаку, обеспечивающую нарушение целостности активов ОО.

T.ACCESS

Нарушение правил контроля доступа

Злоумышленник, будучи авторизованным пользователем ОО, реализует атаку, направленную на получение доступа к активам без соответствующих полномочий.

T.DOS

Отказ в обслуживании

Злоумышленник реализует атаку, направленную на отказ в обслуживании за счет временной недоступности или неработоспособности компонентов системы.

T.BADCONF

Ошибочное конфигурирование

Пользователь ОО непреднамеренно выполняет некорректные действия, приводящие к нарушениям штатного и безопасного режима функционирования компонентов программного обеспечения.

Согласовано:
секретарь конкурсной комиссии
АО «Тюменьэнерго» Дурасова И.И.

Согласовано: Департамент правового обеспечения
АО «Тюменьэнерго» Зубов В. В.

T.REPUDIATE	Отрицание действий Пользователь ОО отрицает выполнение тех или иных действий с программной частью ОО.
T.AUDLACK	Отсутствие журналирования Действия (штатные или некорректные) оператора и/или факты нарушения безопасности в процессе выполнения повседневных задач обслуживающим персоналом, не регистрируются или не просматриваются для их дальнейшего анализа и/или исправления.
T.AUDFUL	Переполнение журналов События и инциденты безопасности не регистрируются вследствие переполнения объектов, обеспечивающих хранение данных журналов регистрации.

4.3 Угрозы безопасности для среды функционирования

TE.INTEG	Нарушение целостности программных компонентов Злоумышленник осуществляет действия, направленные на несанкционированное изменение целостности компонентов программного обеспечения
TE.CONNECT	Нарушение связности модулей ПО Злоумышленник осуществляет атаку на ту часть среды функционирования, которая обеспечивает передачу данных между модулями ОО, для нарушения связности ОО.
TE.MALWARE	Установка вредоносного ПО Злоумышленник выполняет установку вредоносного ПО с целью осуществления несанкционированного доступа активам, нарушения их целостности или доступности.

4.4 Политики безопасности Группы компаний «Россети»

ОО должен реализовывать следующие политики безопасности Группы компаний «Россети»:

P.DENY_UNAU	Защита от несанкционированного доступа Должно обеспечиваться предотвращение несанкционированного доступа к информации.
P.IDENT_ASSET	Идентификация и инвентаризация активов Должно обеспечиваться выявление незарегистрированных и несанкционированных технических устройств, и программных средств, которые могут привести к нарушению работы программного обеспечения.
P.AUDIT	Контроль обеспечения информационной безопасности Должен осуществляться контроль за действиями пользователей ОО и за событиями безопасности, связанными с ОО.

P.ACC_MON**Разграничение доступа**

Должно осуществляться разграничение доступа пользователей ОО к активам.

P.SECURE**Защита критической информации**

Должна осуществляться защита критически важной технологической информации на всех этапах ее жизненного цикла.

4.5 Предположения безопасности**4.5.1 Физические аспекты****A.LOCATE****Физический доступ к оборудованию**

Предполагается, что ресурсы ОО расположены в пределах контролируемой зоны, где исключен несанкционированный физический доступ к ОО.

4.5.2 Аспекты персонала**A.MANAGE****Административное управление**

Функционал безопасности ОО находится под управлением одного или нескольких компетентных сотрудников. Административный персонал системы не является беспечным, преднамеренно небрежным или враждебным и должен применять, и соблюдать инструкции, предусмотренные руководящими документами.

A.TEACHUSER**Квалификация пользователей**

Предполагается, что пользователи успешно обучены и имеют опыт в выполнении поставленных задач или групп задач в безопасной ИТ-среде, при этом квалифицированно используя систему управления ресурсами, принадлежащими им.

4.5.3 Процедурные аспекты**A.PEER.MGT****Административное управление средой функционирования**

Предполагается, что ОО (модуль NMIPanel) функционирует в ИТ-среде под тем же самым административным управлением с теми же самыми ограничениями политики безопасности, что реализованы в ОО.

4.5.4 Аспекты связности**A.CONNECT****Обеспечение связности**

Предполагается, что все связи и подключения между физически разделенными компонентами ФБО не защищаются посредством системы функций безопасности ОО, являясь физически или логически защищенными средой ОО, которая обеспечивает целостность передаваемых данных.

4.5.5 Аспекты использования меток времени

A.STM

Надежные метки времени

Предполагается, что среда функционирования ОО предоставляет ОО источник надежных меток времени при отсутствии такового в составе ОО.

5 ЦЕЛИ БЕЗОПАСНОСТИ

5.1 Цели безопасности для ОО

O.AUDITING

Аудит событий

ФБО должны быть способны фиксировать имеющие отношение к безопасности события. ФБО должны защищать эту информацию и предоставлять уполномоченным администраторам. Информация о событиях, имеющих отношение к безопасности, должна содержать время и дату имевшего место события, а также (при наличии) информацию о пользователе, имевшем отношение к событию. Эта информация должна быть достаточно детализированной, чтобы помочь уполномоченному администратору обнаружить попытки нарушения безопасности или потенциальное нарушение конфигурации основных характеристик ФБО, способное подвергнуть риску IT-активы.

O.ACCESS

Контроль доступа

ОО должен гарантировать обеспечение различных уровней доступа к объектам для субъектов с различными полномочиями.

O.I&A

Идентификация и аутентификация

ОО должен обеспечивать идентификацию и аутентификацию пользователя перед выполнением любых действий. При нескольких неуспешных попытках аутентификации ОО должен блокироваться для пользователя на определенный период времени. Вводимая аутентификационная информация должна быть защищена от внешнего наблюдения. Сеанс должен блокироваться после определенного времени бездействия.

O.MANAGE

Конфигурация безопасности

ОО должен разрешать администраторам эффективно управлять ОО и ФБО, и должен гарантировать, что только авторизованные администраторы могут получить доступ к любой операции, связанной с модификациями данных ОО.

O.AVAIL

Доступность

Должна быть обеспечена доступность функционала программного обеспечения. Программное обеспечение должно продолжать функционировать после выхода из строя каналов связи. Должны быть предусмотрены механизмы обеспечения продолжения функционирования при

переполнении баз данных. Должен осуществляться контроль целостности компонентов в процессе их загрузки. Должно быть исключено неконтролируемое, несанкционированное вмешательство в процессы перезагрузки или восстановления после сбоев компонентов программного обеспечения. В процессе функционирования программного обеспечения должны быть предусмотрены на периодической основе проверки на наличие уязвимостей компонентов программного обеспечения. Должны быть предусмотрены возможности восстановления данных и/или параметров конфигураций компонентов программного обеспечения из резервных копий в случае их компрометации или уничтожения. Должны быть предусмотрены возможности создания резервных копий в случае внесения изменений в конфигурации, с заданной периодичностью или комбинации этих вариантов.

5.2 Цели безопасности для среды функционирования

OE.PHYSICAL

Контроль физического доступа

Ответственные за ОО должны обеспечивать защиту частей ОО, критичных к политике безопасности, от физических атак, которые могут скомпрометировать цели безопасности ИТ.

OE.PROTECTION

Защита ОО

Среда функционирования должна защищать ОО и его активы от внешнего вмешательства или фальсификаций, включая защиту от вредоносного программного обеспечения.

OE.INSTALL

Безопасная установка

Ответственные за администрирование ОО должны создавать и применять процедуры, обеспечивающие установку, поставку, инсталляцию и конфигурирование аппаратных средств, ПО и компонентов встроенного ПО, которые составляют систему, способом, поддерживающим механизмы безопасности, реализуемые ОО.

OE.ADMIN

Квалификация администратора

Ответственные за администрирование ОО должны быть компетентными и заслуживающими доверия лицами, способными безопасно управлять ОО и содержащейся в нем информацией.

OE.RECODER

Действия по восстановлению

Ответственные за администрирование ОО должны обеспечивать процедуры и/или механизмы, удостоверяющие факт восстановления системы без компрометации системы безопасности после отказа или другого прерывания.

OE.TIME

Источник надежных меток времени

Среда функционирования должна предоставлять источник синхронизации точного времени для часов реального времени, входящих в состав ОО.

Согласовано:
секретарь конкурсной комиссии
АО «Тюменьэнерго» Д. В. Павлов Н. И.

Согласовано: Департамент правового обеспечения
АО «Тюменьэнерго» Зубов В. В.

5.3 Обоснование целей безопасности

В таблице 1 представлено отображение целей безопасности на угрозы информационной безопасности и политики информационной безопасности Группы компаний «Россети»:

Таблица 1. Сопоставление целей безопасности ОО угрозам безопасности и политикам безопасности

Цели	Угрозы/Политики
O.AUDITING	T.REPEAT T.REPUDIATE T.AUDLACK P.AUDIT
O.ACCESS	T.ACCESS P.ACCMON
O.I&A	T.NOAUTH T.REPUDIATE T.REPEAT T.SPYINF P.DENY_UAU
O.MANAGE	T.BADCONF P.ACC_MON
O.AVAIL	T.DOS T.BADCONF T.AUDFUL T.CTRL_TAMP P.SECURE

В таблице 2 представлено отображение целей безопасности среды функционирования ОО на угрозы безопасности, предположения и политики безопасности.

Таблица 2. Сопоставление целей безопасности среды функционирования угрозам безопасности, предположениям и политикам безопасности

Цели среды	Угрозы/Предположения/Политики
OE.ADMIN	A.MANAGE A.TEACHUSER P.ACC_MON
OE.PROTECTION	A.CONNECT A.PEER.MGT TE.MALWARE TE.INTEG
OE.TIME	A.STM P.AUDIT
OE.INSTALL	A.MANAGE P.IDENT_ASSET P.AUDIT TE.INTEG
OE.PHYSICAL	A.LOCATE
OE.RECODER	A.MANAGE P.SECURE

При модификации представленной модели угроз обоснование целей безопасности и оценка достаточности проводится в ходе разработки ЗБ.

Согласовано:
секретарь конкурсной комиссии
АО «Тюменьэнерго» Зорисина Н.М.

Согласовано: Департамент правового обеспечения
АО «Тюменьэнерго» Зубов В. В.

6 ТРЕБОВАНИЯ БЕЗОПАСНОСТИ

В данном разделе представлены функциональные требования безопасности и требования доверия к безопасности, которым должен удовлетворять ОО. Функциональные требования основаны на функциональных компонентах в соответствии с ГОСТ Р ИСО/МЭК 15408-2-2013.

Требования доверия сформулированы в соответствии с ГОСТ Р ИСО/МЭК 15408-3 и представлены в виде оценочного уровня доверия ОУД 4+ (усиленный) с включением компонент, сформулированных в явном виде.

6.1 Функциональные требования безопасности

Функциональные компоненты ГОСТ Р ИСО/МЭК 15408-2, на которых основаны функциональные требования безопасности, а также компоненты сформулированных в явном виде расширенных требований приведены в таблице 2.

Таблица 2. Функциональные компоненты ИБ

Идентификатор	Название компонента требований
FAU_GEN.1	Генерация данных аудита
FAU_GEN.2	Ассоциация идентификатора пользователя
FAU_SAR.1	Просмотр журналов аудита
FAU_STG.1	Защищенное хранение журнала аудита
FAU_STG.3	Действия в случае возможной потери данных аудита
FAU_STG.4	Предотвращение потери данных аудита
FDP_ACC.1	Ограниченное управление доступом
FDP_ACF.1	Управление доступом, основанное на атрибутах безопасности
FDP_ROL.2	Расширенный откат к исходному состоянию
FDP_SDI.2	Мониторинг целостности хранимых данных и предпринимаемые действия
FIA_AFL.1	Обработка отказов аутентификации
FIA_ATD.1	Определение атрибутов пользователя
FIA_UAU.2	Аутентификация до любых действий пользователя
FIA_UAU.7	Аутентификация с защищенной обратной связью
FIA_UID.2	Идентификация до любых действий пользователя
FMT_MSA.1	Управление атрибутами безопасности
FMT_MSA.3	Инициализация статических атрибутов
FMT_MTD.1	Управление данными ФБО
FMT_SMF.1	Спецификация функций управления
FMT_SMR.1	Роли безопасности
FTA_SSL.1	Блокирование сеанса, инициированное функциями безопасности

6.1.1 Аудит безопасности

FAU_GEN.1 Генерация данных аудита

FAU_GEN.1.1 Функции безопасности программного обеспечения должны генерировать запись аудита для следующих событий, потенциально подвергаемых аудиту:

- а) запуск и завершение выполнения функций аудита;
- б) все события, потенциально подвергаемые аудиту, на базовом уровне аудита;
- в) [другие специально определенные события, подвергаемые аудиту].

Согласовано:
секретарь конкурсной комиссии
АО «Тюменьэнерго» *Давыдова Н.Н.*

Согласовано: Департамент правового обеспечения
АО «Тюменьэнерго» *Зубов В. В.*

FAU_GEN.1.2

Функции безопасности программного обеспечения должны регистрировать в каждой записи аудита, по меньшей мере, следующую информацию:

- а) дата и время события, тип события, идентификатор субъекта, результат события (успешный или неуспешный);
- б) для каждого типа событий, потенциально подвергаемых аудиту, из числа определенных в функциональных компонентах, которые включены в задание по безопасности на конкретное программное обеспечение.

Замечания по применению:

В пункте б) FAU_GEN.1.1 выбран уровень аудита базовый, с учетом этого разработчик задания по безопасности в рамках сертификации должен следовать инструкциям ГОСТ Р ИСО/МЭК 15408-2 по включению в FAU_GEN.1 событий согласно выбранному уровню аудита, используя пункты в рубрике «Аудит» для каждого функционального компонента из ГОСТ Р ИСО/МЭК 15408-2, включенного в задание по безопасности и каждого компонента функциональных требований безопасности, определенных настоящими требованиями. Разработчик задания по безопасности может дополнительно указать в пункте с) FAU_GEN.1.1 другие события, которые программное обеспечение способно подвергать аудиту.

Зависимости:

FPT_STM.1 Надежные метки времени.

FAU_GEN.2

Ассоциация идентификатора пользователя

FAU_GEN.2.1

Для аудита событий, являющихся результатом действий идентифицированных пользователей, ФБО должны быть способны ассоциировать каждое событие, потенциально подвергаемое аудиту, с идентификатором пользователя, который был инициатором этого события.

Зависимости:

FAU_GEN.1 Генерация данных аудита;

FIA_UID.1 Выбор момента идентификации.

FAU_SAR.1

Просмотр журналов аудита

FAU_SAR.1.1

Функции безопасности программного обеспечения должны предоставлять [уполномоченным пользователям] возможность читать [данные аудита безопасности] из записей аудита.

FAU_SAR.1.2

Функции безопасности программного обеспечения должны предоставлять записи аудита в виде, позволяющем пользователю воспринимать содержащуюся в них информацию.

Зависимости:

FAU_GEN.1 Генерация данных аудита.

Согласовано:
секретарь конкурсной комиссии
АО «Тюменьэнерго» Зайцева Н.Н.

Согласовано: Департамент правового обеспечения
АО «Тюменьэнерго» Зубов В. В.

FAU_STG.1	Защищенное хранение журнала аудита
FAU_STG.1.1	Функции безопасности программного обеспечения должны защищать хранимые в журнале аудита записи от несанкционированного удаления.
FAU_STG.1.2	Функции безопасности программного обеспечения должны предотвращать несанкционированную модификацию хранимых записей в журналах аудита.
	<p><u>Замечания по применению:</u></p> <p>Программное обеспечение может обеспечивать хранение журналов аудита как локально, так и обеспечивать передачу журналов на удаленные серверы централизованной системы журналирования для дальнейшей обработки. В последнем случае в системе реализуется локальный стек для записей аудита, перед их отправкой на удаленные сервера, при этом к локальному стеку предъявляются все описанные выше требования.</p>
FAU_STG.3	Действия в случае возможной потери данных аудита
FAU_STG.3.1	Функции безопасности программного обеспечения должны [обеспечить предупреждение администратора системы] в случае, если журналы аудита превышают [допустимое ограничение].
	<p><u>Зависимости:</u></p> <p>FAU_STG.1 Защищенное хранение журналов аудита.</p>
FAU_STG.4	Предотвращение потери данных аудита
FAU_STG.4.1	Функции безопасности программного обеспечения должны записывать поверх самых старых хранимых записей аудита и [нет дополнительных действий] при переполнении журнала аудита.
	<p><u>Зависимости:</u></p> <p>FAU_STG.1 Защищенное хранение журналов аудита.</p>
6.1.2 Защита данных пользователя	
FDP_ACC.1	Ограниченное управление доступом
FDP_ACC.1.1	<p>Функции безопасности программного обеспечения должны осуществлять [ролевой контроль доступа] для:</p> <ul style="list-style-type: none"> [- субъектов: пользователи системы, процессы; - объектов: данные обрабатываемые программным обеспечением; операций: все реализованные программным обеспечением операции.]
	<p><u>Зависимости:</u></p> <p>FDP_ACF.1 Управление доступом, основанное на атрибутах безопасности.</p>

FDP_ACF.1	Управление доступом, основанное на атрибутах безопасности
FDP_ACF.1.1	<p>Функции безопасности программного обеспечения должны осуществлять [ролевой контроль доступа] к объектам основываясь на:</p> <p>[<i>- атрибутах безопасности субъекта: идентификатор субъекта, роль субъекта</i></p> <p><i>атрибутах безопасности объекта: идентификатор объекта, разрешения для объекта.</i>]</p>
FDP_ACF.1.2	<p>Функции безопасности программного обеспечения должны реализовать следующие правила определения того, разрешена ли операция управляемого субъекта на управляемом объекте:</p> <p>[<i>- субъект должен быть связан с правами доступа к объекту в соответствии с назначенной ролью.</i>]</p>
FDP_ACF.1.3	<p>Функции безопасности программного обеспечения должны явно разрешать доступ субъектов к объектам, основываясь на следующих дополнительных правилах:</p> <p>[<i>дополнительных правил нет.</i>]</p>
FDP_ACF.1.4	<p>Функции безопасности программного обеспечения должны явно отказывать в доступе субъектов к объектам, основываясь на следующих дополнительных правилах:</p> <p>[<i>дополнительных правил нет.</i>]</p> <p><u>Зависимости:</u></p> <p>FDP_ACC.1 Ограниченное управление доступом. FMT_MSA.3 Инициализация статических атрибутов.</p>
FDP_ROL.2	Расширенный откат к исходному состоянию
FDP_ROL.2.1	<p>Функции безопасности программного обеспечения должны осуществлять [управление доступом, основанное на ролях безопасности], чтобы разрешать откат всех операций [<i>на всех объектах системы</i>].</p>
FDP_SDI.2	Мониторинг целостности хранимых данных и предпринимаемые действия
FDP_SDI.2.1	<p>Функции безопасности программного обеспечения должны контролировать данные пользователя, хранимые в местах хранения, контролируемых ОО, на [<i>наличие ошибок контрольных сумм</i>] для всех объектов, основываясь на следующих атрибутах [<i>без дополнительных атрибутов</i>]</p>
FDP_SDI.2.2	<p>При обнаружении ошибки целостности данных функции безопасности программного обеспечения должны обеспечить [<i>загрузку данных по умолчанию (эталонных)</i>].</p>
6.1.3 Идентификация и аутентификация	
FIA_AFL.1	Обработка отказов аутентификации
FIA_AFL.1.1	<p>Функции безопасности программного обеспечения должны обнаруживать, когда произойдет [заданное</p>

Согласовано:
секретарь комиссии
АО «Тюменьэнерго» 27.08.2018

Согласовано: Департамент правового обеспечения
АО «Тюменьэнерго» Зубов В. В.

администратором или разработчиком количество неуспешных попыток аутентификации, относящихся к *[вводу пароля пользователя]*.

FIA_AFL.1.2

При достижении определенного числа неуспешных попыток аутентификации функции безопасности программного обеспечения должны выполнить *[блокировку доступа к ОО на заданный администратором или разработчиком период времени]*

Зависимости:

FIA_UAU.1 Выбор момента аутентификации

FIA_ATD.1

Определение атрибутов пользователя

FIA_ATD.1.1

Функции безопасности программного обеспечения должны поддерживать для каждого пользователя следующий список атрибутов безопасности:

[- идентификатор пользователя,

– пароль пользователя,

иные атрибуты, определенные в рамках Задания по безопасности на конкретное программное обеспечение.]

FIA_UAU.2

Аутентификация до любых действий пользователя

FIA_UAU.2.1

ФБО должны требовать, чтобы каждый пользователь был успешно аутентифицирован до разрешения **любого** действия, выполняемого при посредничестве ФБО от имени этого пользователя.

Зависимости:

FIA_UID.1 Выбор момента идентификации.

FIA_UAU.7

Аутентификация с защищенной обратной связью

FIA_UAU.7.1

ФБО должны предоставлять пользователю только *[количество введенных символов]* во время выполнения аутентификации.

Зависимости:

FIA_UID.1 Выбор момента идентификации.

FIA_UID.2

Идентификация до любых действий пользователя

FIA_UID.2.1

ФБО должны требовать, чтобы каждый пользователь был успешно идентифицирован до разрешения **любого** действия, выполняемого при посредничестве ФБО от имени этого пользователя.

6.1.4 Управление безопасностью

FMT_MSA.1

Управление атрибутами безопасности

FMT_MSA.1.1

Функции безопасности программного обеспечения должны осуществлять *[ПФБ управления доступом, основанную на ролях безопасности]*, предоставляющую возможность **модифицировать** атрибуты безопасности только *[уполномоченным пользователям]*.

Зависимости:

FDP_ACC.1 Ограниченное управление доступом или

FDP_IFC.1 Ограниченное управление информационными потоками.

FMT_SMR.1 Роли безопасности.

FMT_MSA.3**Инициализация статических атрибутов**

FMT_MSA.3.1

Функции безопасности должны осуществлять [ПФБ управления доступом, основанную на ролях безопасности], предусматривающую **ограничительные свойства** значений по умолчанию для атрибутов безопасности, которые используются для осуществления ПФБ.

FMT_MSA.3.2

ФБО должны позволять [уполномоченным пользователям] определять альтернативные начальные значения для отмены значений по умолчанию при создании объекта или информации.

Зависимости:

FMT_MSA.1 Управление атрибутами безопасности.

FMT_SMR.1 Роли безопасности.

FMT_MTD.1(1)**Управление данными функций безопасности**

FMT_MTD.1(1).1

Функции безопасности программного обеспечения должны ограничивать возможность **модификации** следующих данных [записи журнала аудита информационной безопасности, данные учетных записей пользователей] только [администраторам ИБ].

Зависимости:

FMT_SMR.1 Роли безопасности.

FMT_MTD.1(2)**Управление данными функций безопасности**

FMT_MTD.1(2).1

Функции безопасности программного обеспечения должны ограничивать возможность **модификации** следующих данных [пароли пользователей] только [владельцам].

Зависимости:

FMT_SMR.1 Роли безопасности.

FMT_SMF.1**Спецификация функций управления**

FMT_SMF.1.1

Функции безопасности программного обеспечения должны быть способны к выполнению следующих функций управления [добавление пользователя, удаление пользователя, модификация учетной записи пользователя, модификация свойств объекта, иные определяемые в ЗБ функции].

FMT_SMR.1**Роли безопасности**

FMT_SMR.1.1

Функции безопасности программного обеспечения должны поддерживать следующие роли:

[- администратор;

– оператор;

иные роли, определяемые в ЗБ.]

Зависимости:

FIA_UID.1 Выбор момента идентификации.

6.1.5 Доступ к программному обеспечению

FTA_SSL.1 Блокирование сеанса, инициированное функциями безопасности

FTA_SSL.1.1 ФБО должны блокировать интерактивный сеанс после [определяемый администратором или разработчиком интервал времени], для чего предпринимаются следующие действия:

а) очистка или перезапись устройств отображения, придание их текущему содержанию нечитаемого вида;

б) блокирование любых действий по доступу к данным пользователя/устройствам отображения, кроме необходимых для разблокирования сеанса.

FTA_SSL.1.2 ФБО должны требовать, чтобы до разблокирования сеанса произошли следующие события: [ввод пароля пользователя].

6.2 Требования доверия к безопасности

Требования доверия к безопасности ОО соответствуют ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности» и пакету доверия ОУД4 с усилением компонентами ADV_IMP.2 «Полное представление реализации ФБО», ALC_FLR.2 «Процедуры сообщений о недостатках», AVA_VAN.5 «Усиленный методический анализ» и компонентом доверия AMA_SIA_EXT.3 «Анализ влияния обновлений на безопасность ОО», сформулированным в явном виде (Табл. 3).

Таблица 3. Требования доверия к безопасности ОО

Классы доверия	Компоненты доверия	Названия компонентов доверия
ADV: Разработка	ADV_ARC.1	Описание архитектуры безопасности
	ADV_FSP.4	Полная функциональная спецификация
	ADV_IMP.2	Полное представление реализации ФБО
	ADV_TDS.3	Базовый модульный проект
AGD: Руководства	AGD_OPE.1	Руководство пользователя по эксплуатации
	AGD_PRE.1	Подготовительные процедуры
ALC: Поддержка жизненного цикла	ALC_CMC.4	Поддержка производства, процедуры приемки и автоматизации
	ALC_CMS.4	Охват УК отслеживания проблем
	ALC_DEL.1	Процедуры поставки
	ALC_DVS.1	Идентификация мер безопасности
	ALC_FLR.2	Процедуры сообщений о недостатках
	ALC_LCD.1	Определенная разработчиком модель жизненного цикла.
	ALC_TAT.1	Полностью определенные

Классы доверия	Компоненты доверия	Названия компонентов доверия
		инструментальные средства разработки
ATE: Тестирование	ATE_COV.2	Анализ покрытия
	ATE_DPT.2	Тестирование: модули обеспечения безопасности
	ATE_FUN.1	Функциональное тестирование
	ATE_IND.2	Выборочное независимое тестирование
AVA: Оценка уязвимостей	AVA_VAN.5	Усиленный методический анализ
AMA: Анализ влияния обновлений	AMA_SIA_EXT.3	Анализ влияния обновлений на безопасность ОО

6.2.1 Разработка (ADV)

ADV_ARC.1 Описание архитектуры безопасности

Зависимости

ADV_FSP.1 Базовая функциональная спецификация.

ADV_TDS.1 Базовый проект.

Элементы действий разработчика

ADV_ARC.1.1D Разработчик должен спроектировать ОО и обеспечить реализацию проекта таким образом, чтобы свойства безопасности ФБО невозможно было обойти.

ADV_ARC.1.2D Разработчик должен спроектировать ФБО и обеспечить их реализацию таким образом, чтобы ФБО обеспечивали собственную защиту от вмешательства недоверенных сущностей.

ADV_ARC.1.3D Разработчик должен предоставить «Описание архитектуры безопасности» ФБО.

Элементы содержания и представления свидетельств

ADV_ARC.1.1C Уровень детализации «Описания архитектуры безопасности» должен соответствовать представленному в проектной документации по ОО описанию абстракций (элементов представления ОО), осуществляющих выполнение ФТБ.

ADV_ARC.1.2C В «Описании архитектуры безопасности» должно быть включено описание доменов безопасности, обеспеченных согласованностью ФБО с ФТБ.

ADV_ARC.1.3C «Описание архитектуры безопасности» должно предоставлять информацию о том, насколько процесс инициализации ФБО является защищенным.

ADV_ARC.1.4C В «Описании архитектуры безопасности» должно быть продемонстрировано, что ФБО обеспечивают собственную защиту от вмешательства.

ADV_ARC.1.5C В «Описании архитектуры безопасности» должно быть продемонстрировано, что ФБО не допускают возможности обхода функциональных возможностей, осуществляющих выполнение ФТБ.

Элементы действий оценщика

ADV_ARC.1.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ADV_FSP.4 Полная функциональная спецификация

Зависимости:

ADV_TDS.1 Базовый проект.

Элементы действий разработчика

ADV_FSP.4.1D Разработчик должен представить функциональную спецификацию.

ADV_FSP.4.2D Разработчик должен представить прослеживание функциональной

Согласовано:
секретарь конкурсной комиссии
АО «Тюменьэнерго» Зубов В. В.

Согласовано: Департамент правового обеспечения
АО «Тюменьэнерго» Зубов В. В.

спецификации к функциональным требованиям безопасности.

Элементы содержания и представления свидетельств

ADV_FSP.4.1C В функциональной спецификации должны быть полностью представлены ФБО.

ADV_FSP.4.2C В функциональной спецификации должны быть описаны назначение и метод использования всех ИФБО.

ADV_FSP.4.3C В функциональной спецификации должны быть идентифицированы и описаны все параметры, связанные с каждым ИФБО.

ADV_FSP.4.4C В функциональной спецификации должны быть описаны все действия, связанные с каждым ИФБО.

ADV_FSP.4.5C Функциональная спецификация должна содержать описание сообщений обо всех непосредственных ошибках, которые могут возникнуть при вызове каждого ИФБО.

ADV_FSP.4.6C В прослеживании соответствия должно быть продемонстрировано прослеживание ФТБ к ИФБО в функциональной спецификации.

Элементы действий оценщика

ADV_FSP.4.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ADV_FSP.4.2E Оценщик должен сделать независимое заключение, что функциональная спецификация является точным и полным отображением функциональных требований безопасности ОО.

ADV_IMP.2 Полное отображение представления реализации ФБО

Зависимости: ADV_TDS.3 Базовый модульный проект

ALC_TAT.1 Полностью определенные инструментальные средства разработки

ALC_CMC.5 Расширенная поддержка

Элементы действий разработчика

ADV_IMP.2.1D Разработчик должен обеспечить оценщику доступ к представлению реализации для всех ФБО.

ADV_IMP.2.2D Разработчик должен обеспечить прослеживание всего представления реализации к описанию проекта ОО.

Элементы содержания и представления свидетельств

ADV_IMP.2.1C Представление реализации должно определить ФБО на таком уровне детализации, что ФБО могут быть созданы без дополнительных проектных решений.

ADV_IMP.2.2C Представление реализации должно быть изложено в том виде, какой используется персоналом, занимающимся разработкой.

ADV_IMP.2.3C В прослеживании между всем представлением реализации и описанием проекта ОО должно быть продемонстрировано их соответствие.

Элементы действий оценщика

ADV_IMP.2.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ADV_TDS.3 Базовый модульный проект

Зависимости:

ADV_FSP.4 Полная функциональная спецификация.

Элементы действий разработчика

ADV_TDS.3.1D Разработчик должен представить проект ОО.

ADV_TDS.3.2D Разработчик должен обеспечить прослеживание ИФБО в функциональной спецификации к более низкому уровню декомпозиции, представленному в проекте ОО.

Согласовано:
секретарь конкурсной комиссии
АО «Тюменьэнерго» - *Дорожнев Н.И.*

Согласовано: Департамент правового обеспечения
АО «Тюменьэнерго» *Зубов В. В.*

Элементы содержания и представления свидетельств

ADV_TDS.3.1C В проекте должно приводиться описание структуры ОО на уровне подсистем.

ADV_TDS.3.2C В проекте должно приводиться описание структуры ОО на уровне модулей.

ADV_TDS.3.3C В проекте должны быть идентифицированы все подсистемы ФБО.

ADV_TDS.3.4C В проекте должно приводиться описание каждой из подсистем ФБО.

ADV_TDS.3.5C В проекте должно приводиться описание взаимодействий всех подсистем ФБО между собой.

ADV_TDS.3.6C В проекте должно быть осуществлено прослеживание подсистем ФБО с модулями ФБО.

ADV_TDS.3.7C В проекте должен быть описан каждый осуществляющий выполнение ФТБ модуль с точки зрения его назначения и взаимодействия с другими модулями.

ADV_TDS.3.8C В проекте должен быть описан каждый осуществляющий выполнение ФТБ модуль с точки зрения его относящихся к ФТБ интерфейсов, значений, предоставляемых этими интерфейсами в ответ на запросы, взаимодействий с другими модулями и вызываемыми интерфейсами этих модулей.

ADV_TDS.3.9C В проекте должен быть описан каждый поддерживающий и не влияющий на выполнение ФТБ модуль с точки зрения его назначения и взаимодействия с другими модулями.

ADV_TDS.3.10C В прослеживании должно быть продемонстрировано, что все описанные в проекте ОО режимы функционирования прослеживаются к вызывающим их ИФБО.

Элементы действий оценщика

ADV_TDS.3.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ADV_TDS.3.2E Оценщик должен сделать независимое заключение, что проект является точным и полным отображением всех функциональных требований безопасности.

6.2.2 Руководства (AGD)**AGD_OPE.1 Руководство пользователя по эксплуатации****Зависимости:**

ADV_FSP.1 Базовая функциональная спецификация.

Элементы действий разработчика

AGD_OPE.1.1D Разработчик должен представить руководство пользователя по эксплуатации.

Элементы содержания и представления свидетельств

AGD_OPE.1.1C В руководстве пользователя по эксплуатации для каждой пользовательской роли должно быть представлено описание доступных пользователям функций, возможных прав и обязанностей, которыми следует управлять в защищенной среде функционирования, а также уместных предупреждений.

AGD_OPE.1.2C В руководстве пользователя по эксплуатации в рамках каждой пользовательской роли должно быть представлено описание принципов безопасной работы с предоставленными в ОО интерфейсами.

AGD_OPE.1.3C В руководстве пользователя по эксплуатации должно быть представлено описание доступных для каждой пользовательской роли функций и интерфейсов, особенно всех параметров безопасности под управлением пользователя, с указанием безопасных значений, если это уместно.

AGD_OPE.1.4C В руководстве пользователя по эксплуатации для каждой пользовательской роли должно быть представлено четкое представление каждого типа имеющих значение для безопасности событий, связанных с доступными пользователю обязательными для выполнения функциями, включая изменение характеристик безопасности сущностей, находящихся под управлением ФБО.

AGD_OPE.1.5C В руководстве пользователя по эксплуатации должны быть идентифицированы все возможные режимы работы ОО (включая операции после сбоев и ошибок эксплуатации), их последствия и участие в обеспечении безопасного функционирования.

AGD_OPE.1.6C В руководстве пользователя по эксплуатации для каждой пользовательской роли должно быть описание всех мер безопасности, предназначенных для выполнения целей безопасности для среды функционирования согласно описанию в ЗБ.

AGD_OPE.1.7C Руководство пользователя по эксплуатации должно быть четким и обоснованным.

Элементы действий оценщика

AGD_OPE.1.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

AGD_PRE.1 Подготовительные процедуры

Зависимости: отсутствуют.

Элементы действий разработчика

AGD_PRE.1.1D Разработчик должен предоставить ОО вместе с подготовительными процедурами.

Элементы содержания и представления свидетельств

AGD_PRE.1.1C В подготовительных процедурах должны описываться все шаги, необходимые для безопасной приемки поставленного ОО в соответствии с процедурами поставки разработчика.

AGD_PRE.1.2C В подготовительных процедурах должны описываться все необходимые шаги для безопасной установки ОО и безопасной подготовки среды функционирования в соответствии с целями безопасности для среды функционирования, описанными в ЗБ.

Элементы действий оценщика

AGD_PRE.1.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

AGD_PRE.1.2E Оценщик должен использовать подготовительные процедуры для подтверждения того, что ОО может быть безопасно подготовлен к работе.

6.2.3 Поддержка жизненного цикла (ALC)

ALC_CMC.4 Поддержка генерации, процедуры приемки и автоматизация.

Зависимости:

ALC_CMS.1 Охват УК ОО.

ALC_DVS.1 Идентификация мер безопасности.

ALC_LCD.1 Определенная разработчиком модель жизненного цикла.

Элементы действий разработчика

ALC_CMC.4.1D Разработчик должен предоставить ОО и маркировку для ОО.

ALC_CMC.4.2D Разработчик должен предоставить документацию УК.

ALC_CMC.4.3D Разработчик должен использовать систему УК.

Согласовано:
секретарь канцелярии комиссии
АО «Тюменьэнерго» Зубов В. В.

Согласовано: Департамент правового обеспечения
АО «Тюменьэнерго» Зубов В. В.

Элементы содержания и представления свидетельств

ALC_CMC.4.1C ОО должен быть помечен уникальной маркировкой.

ALC_CMC.4.2C В документации УК должно содержаться описание метода, используемого для уникальной идентификации элементов конфигурации.

ALC_CMC.4.3C В системе УК должны быть уникальным образом идентифицированы все элементы конфигурации.

ALC_CMC.4.4C В системе УК должны быть предусмотрены такие автоматизированные меры, при применении которых в элементы конфигурации могут быть внесены только санкционированные изменения.

ALC_CMC.4.5C Система УК должна поддерживать производство ОО автоматизированными средствами.

ALC_CMC.4.6C Документация УК должна включать в себя план УК.

ALC_CMC.4.7C В плане УК должно быть описание того, каким образом система УК используется для разработки ОО.

ALC_CMC.4.8C План УК должен содержать описание процедур, используемых для приемки модифицированных или вновь созданных элементов конфигурации как части ОО.

ALC_CMC.4.9C В свидетельствах должно быть продемонстрировано, что все элементы конфигурации сопровождаются системой УК.

ALC_CMC.4.10C В свидетельствах должно быть продемонстрировано, что система УК функционирует в соответствии с планом УК.

Элементы действий оценщика

ALC_CMC.4.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ALC_CMS.4 Охват УК отслеживания проблем

Зависимости: отсутствуют

Элементы действий разработчика

ALC_CMS.4.1D Разработчик должен представить список элементов конфигурации для ОО.

Элементы содержания и представления свидетельств

ALC_CMS.4.1C Список элементов конфигурации должен включать следующее: сам ОО; свидетельства оценки, необходимые по требованиям доверия к безопасности; представление реализации; сведения о недостатках безопасности и стадии их устранения.

ALC_CMS.4.2C Элементы конфигурации должны быть уникально идентифицированы в списке элементов конфигурации.

ALC_CMS.4.3C Для каждого значимого для ФБО элемента конфигурации в списке элементов конфигурации должен быть указан разработчик.

Элементы действий оценщика

ALC_CMS.4.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ALC_DEL.1 Процедуры поставки

Зависимости: отсутствуют.

Элементы действий разработчика

ALC_DEL.1.1D Разработчик должен задокументировать процедуры поставки ОО или его частей потребителю.

ALC_DEL.1.2D Разработчик должен использовать процедуры поставки.

Элементы содержания и представления свидетельств

ALC_DEL.1.1C

Документация поставки должна содержать описание всех процедур, необходимых для поддержания безопасности при распространении версий ОО

Согласовано:
секретарь конкурсной комиссии
АО «Тюменьэнерго» Зубов В.В.

Согласовано: Департамент правового обеспечения
АО «Тюменьэнерго» Зубов В.В.

потребителю.

Элементы действий оценщика

ALC_DEL.1.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ALC_DVS.1 Идентификация мер безопасности

Зависимости: отсутствуют.

Элементы действий разработчика

ALC_DVS.1.1D Разработчик должен представить документацию по безопасности разработки.

Элементы содержания и представления свидетельств

ALC_DVS.1.1C Документация по безопасности разработки должна содержать описание всех физических, процедурных, организационных и других мер безопасности, которые необходимы для защиты конфиденциальности и целостности проекта ОО и его реализации в среде разработки.

Элементы действий оценщика

ALC_DVS.1.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ALC_DVS.1.2E Оценщик должен подтвердить, что меры безопасности применяются.

ALC_FLR.2 Процедуры сообщений о недостатках

Зависимости: отсутствуют.

Цели

Чтобы разработчик имел возможность соответствующим образом реагировать на сообщения пользователей ОО о недостатках безопасности и знал, кому посылать исправления, пользователям ОО необходимо иметь представление о том, каким образом представлять сообщения о недостатках безопасности разработчику. Руководство по исправлению недостатков, предоставляемое разработчиком пользователям ОО, обеспечивает знание пользователями ОО этой важной информации.

Элементы действий разработчика

ALC_FLR.2.1D Разработчик должен предоставить процедуры устранения недостатков, предназначенные для разработчиков ОО.

ALC_FLR.2.2D Разработчик должен установить процедуру получения и отработки всех сообщений о недостатках безопасности и запросов на их исправление.

ALC_FLR.2.3D Разработчик должен предоставить руководство по устранению недостатков, предназначенное для пользователей ОО.

Элементы содержания и представления свидетельств

ALC_FLR.2.1C Документация процедур устранения недостатков должна содержать описание процедур по отслеживанию всех ставших известными недостатков безопасности в каждом релизе ОО.

ALC_FLR.2.2C Процедуры устранения недостатков должны содержать требование представления описания сути и последствий каждого недостатка безопасности, а также состояния процесса исправления этого недостатка.

ALC_FLR.2.3C Процедуры устранения недостатков должны содержать требование к тому, что для каждого недостатка безопасности должны быть идентифицированы корректирующие действия.

ALC_FLR.2.4C Документация процедур устранения недостатков должна содержать описание методов, используемых для предоставления пользователям ОО информации о недостатках, материалов исправлений и руководства по внесению исправлений.

- ALC_FLR.2.5C Процедуры устранения недостатков должны описывать средства, посредством которых разработчик получает от пользователей ОО сообщения и запросы о предполагаемых недостатках безопасности в ОО.
- ALC_FLR.2.6C Процедуры обработки ставших известными недостатков безопасности должны обеспечить, чтобы любые ставшие известными недостатки были исправлены, а для пользователей ОО выпущены процедуры по исправлению.
- ALC_FLR.2.7C Процедуры обработки ставших известными недостатков безопасности должны обеспечить такие защитные меры, чтобы любые исправления этих недостатков не приводили к появлению новых недостатков.
- ALC_FLR.2.8C Руководство по устранению недостатков должно описывать средства, посредством которых пользователи ОО могут сообщать разработчикам о любых предполагаемых недостатках безопасности в ОО.

Элементы действий оценщика

- ALC_FLR.2.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ALC_LCD.1 Определенная разработчиком модель жизненного цикла.

Зависимости: отсутствуют.

Элементы действий разработчика

- ALC_LCD.1.1D Разработчик должен установить модель жизненного цикла, используемую при разработке и сопровождении ОО.
- ALC_LCD.1.2D Разработчик должен представить документацию по определению жизненного цикла.

Элементы содержания и представления свидетельств

- ALC_LCD.1.1C Документация по определению жизненного цикла должна содержать описание модели, применяемой при разработке и сопровождении ОО.
- ALC_LCD.1.2C Модель жизненного цикла должна обеспечить необходимый контроль над разработкой и сопровождением ОО.

Элементы действий оценщика

- ALC_LCD.1.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ALC_TAT.1 Полностью определенные инструментальные средства разработки

Зависимости:

ADV_IMP.1 Подмножество реализации ФБО.

Элементы действий разработчика

- ALC_TAT.1.1D Разработчик должен идентифицировать каждое инструментальное средство, используемое для разработки ОО.
- ALC_TAT.1.2D Разработчик должен задокументировать выбранные опции инструментальных средств разработки, обусловленные реализацией.

Элементы содержания и представления свидетельств

- ALC_TAT.1.1C Все инструментальные средства разработки, используемые для реализации, должны быть полностью определены.
- ALC_TAT.1.2C В документации по инструментальным средствам разработки должны быть однозначно определены значения всех языковых конструкций, используемых в реализации.
- ALC_TAT.1.3C В документации по инструментальным средствам разработки должны быть однозначно определены значения всех опций, обусловленных реализацией.

Согласовано:
секретарь конкурсной комиссии
АО «Тюменьэнерго» Зубова Н.Н.

Согласовано: Департамент правового обеспечения
АО «Тюменьэнерго» Зубов В. В.

Элементы действий оценщика

ALC_TAT.1.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

6.2.4 Тестирование (АТЕ)**АТЕ_COV.2 Анализ покрытия****Зависимости:**

ADV_FSP.2 Детализация вопросов безопасности в функциональной спецификации
АТЕ_FUN.1 Функциональное тестирование

Элементы действий разработчика

АТЕ_COV.2.1D Разработчик должен представить анализ покрытия тестами.

Элементы содержания и представления свидетельств

АТЕ_COV.2.1C Анализ покрытия тестами должен демонстрировать соответствие между тестами из тестовой документации и ИФБО из функциональной спецификации.

АТЕ_COV.2.2C Анализ покрытия тестами должен демонстрировать, что все ИФБО из функциональной спецификации были подвергнуты тестированию.

Элементы действий оценщика

АТЕ_COV.2.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

АТЕ_DPT.2 Тестирование: модули, осуществляющие безопасность**Зависимости:**

ADV_ARC.1 Описание архитектуры безопасности.

ADV_TDS.3 Базовый модульный проект.

АТЕ_FUN.1 Функциональное тестирование.

Элементы действий разработчика

АТЕ_DPT.2.1D Разработчик должен представить анализ глубины тестирования.

Элементы содержания и представления свидетельств

АТЕ_DPT.2.1C Анализ глубины тестирования должен демонстрировать соответствие между тестами в тестовой документации и подсистемами ФБО, а также осуществляющими выполнение ФТБ модулями из проекта ОО.

АТЕ_DPT.2.2C Анализ глубины тестирования должен демонстрировать, что все подсистемы ФБО из проекта ОО были подвергнуты тестированию.

АТЕ_DPT.2.3C Анализ глубины тестирования должен демонстрировать, что осуществляющие выполнение ФТБ модули из проекта ОО были подвергнуты тестированию.

Элементы действий оценщика

АТЕ_DPT.2.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

АТЕ_FUN.1 Функциональное тестирование**Зависимости:**

АТЕ_COV.1 Свидетельство покрытия

Элементы действий разработчика

АТЕ_FUN.1.1D Разработчик должен протестировать ФБО и задокументировать результаты.

АТЕ_FUN.1.2D Разработчик должен представить тестовую документацию.

Элементы содержания и представления свидетельств

АТЕ_FUN.1.1C Тестовая документация должна состоять из планов тестирования, а также ожидаемых и фактических результатов тестирования.

АТЕ_FUN.1.2C В планах тестирования должны быть идентифицированы тесты, которые

Согласовано:
секретарь конкурсной комиссии
А.П. Тюменцев

Согласовано: Департамент правового обеспечения
АС «Тюменьэнерго» Зубов В. В.

необходимо выполнить, а также должны содержаться описания сценариев проведения каждого теста. В эти сценарии должны быть включены также любые зависимости последовательности выполнения тестов от результатов других тестов.

ATE_FUN.1.3C Ожидаемые результаты тестирования должны продемонстрировать прогнозируемые данные на выходе успешного выполнения тестов.

ATE_FUN.1.4C Фактические результаты тестирования должны соответствовать ожидаемым.

Элементы действий оценщика

ATE_FUN.1.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ATE_IND.1 Независимое тестирование на соответствие

Зависимости:

ADV_FSP.1 Базовая функциональная спецификация.

AGD_OPE.1 Руководство пользователя по эксплуатации.

AGD_PRE.1 Подготовительные процедуры.

Элементы действий разработчика

ATE_IND.1.1D Разработчик должен представить ОО для тестирования.

Элементы содержания и представления свидетельств

ATE_IND.1.1C ОО должен быть пригоден для тестирования.

Элементы действий оценщика

ATE_IND.1.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ATE_IND.1.2E Оценщик должен протестировать подмножество ФБО так, чтобы подтвердить, что ФБО функционируют в соответствии со спецификациями.

6.2.5 Оценка уязвимостей (AVA)

AVA_VAN.5 Усиленный методический анализ

Зависимости: ADV_ARC.1 Описание архитектуры безопасности

ADV_FSP.2 Детализация вопросов безопасности в функциональной спецификации

ADV_TDS.3 Базовый модульный проект

ADV_IMP.1 Представление реализации ФБО

AGD_OPE.1 Руководство пользователя по эксплуатации

AGD_PRE.1 Подготовительные процедуры

Цели

Оценщиком проводится анализ уязвимостей с целью установить наличие потенциальных уязвимостей.

Оценщик проводит тестирование проникновения с целью удостовериться в том, что потенциальные уязвимости не могут быть использованы в среде функционирования ОО. Тестирование проникновения проводится оценщиком, исходя из потенциала нападения – Высокий.

Элементы действий разработчика

AVA_VAN.5.1D Разработчик должен представить ОО для тестирования.

Элементы содержания и представления свидетельств

AVA_VAN.5.1C ОО должен быть пригоден для тестирования.

Элементы действий оценщика

AVA_VAN.5.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

AVA_VAN.5.2E Оценщик должен выполнить поиск информации в общедоступных

Согласовано:

секретарь конкурсной комиссии

АО «Тюменьэнерго» Зарякова Н.И.

Согласовано: Департамент правового обеспечения

АО «Тюменьэнерго» Зубов В. В.

AVA_VAN.5.3E Оценщик должен провести независимый методический анализ уязвимостей ОО с использованием документации руководств, функциональной спецификации, проекта ОО, описания архитектуры безопасности и представления реализации, чтобы идентифицировать потенциальные уязвимости в ОО.

AVA_VAN.5.4E Оценщик должен провести тестирование проникновения, основанное на идентифицированных уязвимостях, чтобы сделать заключение, что ОО является стойким к нападениям, выполняемым нарушителем, обладающим **Высоким** потенциалом нападения.

6.2.6 Анализ обновлений (АМА)

AMA_SIA_EXT.3 Экспертиза анализа влияния обновлений ОО на безопасность ОО.

Элементы действий разработчика (заявителя)

AMA_SIA_EXT.3.1D Разработчик (заявитель) должен представлять ежегодно в испытательную лабораторию материалы анализа влияния обновлений ОО на безопасность ОО и среды, в которой ОО функционирует, а также полный пакет обновлений ОО с момента проведения последнего внешнего контроля.

Элементы содержания и представления документированных материалов

AMA_SIA_EXT.3.1C Материалы анализа влияния обновлений на безопасность ОО должны для каждого обновления ОО содержать краткое описание влияния обновления на задание по безопасности, представление функций безопасности ОО, реализацию функций безопасности ОО или содержать логическое обоснование отсутствия такого влияния.

AMA_SIA_EXT.3.2C Материалы анализа влияния на безопасность ОО должны для каждого обновления ОО, влияющего на задание по безопасности, представления, реализацию функций безопасности ОО, идентифицировать все функции безопасности и компоненты ОО, на которые воздействует данное обновление.

AMA_SIA_EXT.3.3C Материалы анализа влияния обновлений на безопасность ОО должны для каждого обновления содержать аргументацию для принятия испытательной лабораторией решения о возможности использования обновления эксплуатантами ОО и необходимости или отсутствии необходимости проведения повторных испытаний системы обнаружения вторжений.

Элементы действий испытательной лаборатории

AMA_SIA_EXT.3.1E Испытательная лаборатория должна подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению документированных материалов, а также то, что обновления ОО не влияют на ОО и среду его функционирования.

6.3 Обоснование требований безопасности

В таблице 4 представлено отображение функциональных требований безопасности на цели безопасности.

Таблица 4. Соответствие требований и целей безопасности

Функциональные требования безопасности	Цели безопасности
FAU_GEN.1	O.AUDITING
FAU_GEN.2	O.AUDITING

Согласовано:
генеральный конкурсный комисси
... 2008 г. 2 класс Н.Н.

Согласовано: Департамент правового обеспечения
АО «Тюменьэнерго» 20.11.2012

Функциональные требования безопасности	Цели безопасности
FAU_SAR.1	O.AUDITING
FAU_STG.1	O.AUDITING, O.AVAIL
FAU_STG.3	O.AUDITING, O.AVAIL
FAU_STG.4	O.AUDITING, O.AVAIL
FDP_ACC.1	O.ACCESS
FDP_ACF.1	O.ACCESS
FDP_ROL.2	O.AVAIL
FDP_SDL1	O.AVAIL
FIA_AFL.1	O.I&A
FIA_ATD.1	O.I&A
FIA_UAU.2	O.I&A
FIA_UAU.7	O.I&A
FIA_UID.2	O.I&A
FMT_MSA.1	O.MANAGE
FMT_MSA.3	O.MANAGE
FMT_MTD.1	O.MANAGE
FMT_SMR.1	O.MANAGE, O.ACCESS
FTA_SSL.1	O.I&A

Как следует из сопоставления функциональные требования безопасности являются необходимыми и достаточными для достижения базовых целей безопасности.

7 ОТВЕТСТВЕННОСТЬ

Работники Группы компаний «Россети», указанные в пункте 1.4 настоящих Требований, несут персональную ответственность за соблюдение Требований.

Согласовано:
секретарь конкурсной комиссии
АО «Тюменьэнерго» *Дурасова Н.И.*

Согласовано: Департамент правового обеспечения
АО «Тюменьэнерго» *Зубов В. В.*

Приложение 2
к распоряжению ПАО «Россети»
от 30.05.2017 № 282р

СПИСОК ДЗО ПАО «РОССЕТИ»

1.	ПАО «ФСК ЕЭС»
2.	ПАО «МРСК Центра»
3.	ПАО «МРСК Центра и Приволжья»
4.	ПАО «МРСК Северо-Запада»
5.	ПАО «МРСК Волги»
6.	ОАО «МРСК Урала»
7.	ПАО «МРСК Сибири»
8.	ПАО «МРСК Юга»
9.	ПАО «МРСК Северного Кавказа»
10.	ПАО «Ленэнерго»
11.	АО «Тюменьэнерго»
12.	ПАО «МОЭСК»
13.	АО «Янтарьэнерго»
14.	ПАО «Кубаньэнерго»
15.	ПАО «ТРК»
16.	ПАО «Дагестанская энергосбытовая компания»
17.	АО «Ингушэнерго»
18.	ПАО «Каббалкэнерго»
19.	ПАО «Севкавказэнерго»
20.	АО «Карачаево-Черкесскэнерго»
21.	АО «Калмэнергообит»
22.	АО «Тываэнергообит»

Согласовано:
секретарь конкурсной комиссии
АО «Тюменьэнерго» Турасова Н.И.

Согласовано: Департамент правового обеспечения
АО «Тюменьэнерго» Зубов