

УТВЕРЖДАЮ

Заместитель директора – главный инженер
филиала ПАО «Россети Московский регион» –
Северные электрические сети

О.М. Баталов

ОТ « » 202 г.

Задание на проектирование

по титулу: «Модернизация ПС 220 кВ №676 «Уча» путем установки систем инженерно-технических средств охраны МО, г.о. Мытищи, д. Манюхино»

ПРОЕКТНАЯ ОРГАНИЗАЦИЯ

(наименование организации)

(ДОЛЖНОСТЬ)

(Ф.И.О.)

(подпись)

« 20 г.

М.П.

ГИП

(Ф.И.О.)

(подпись)

Идентификационный номер специалиста

[illegible]

ЛИСТ СОГЛАСОВАНИЯ

Наименование подразделения	Должность исполнителя	Фамилия, имя, отчество	Подпись	Дата
Департамент КБПиО	Директор департамента	Авдеев И.Н.		02.04.2026
Блок главного инженера филиала СЭС	Заместитель главного инженера по высоковольтным сетям	Дементьев Д.Н.		
Блок главного инженера филиала СЭС	Заместитель главного инженера по системам связи	Некрасов Д.Н.		
Блок капитального строительства филиала СЭС	Начальник отдела проектно-изыскательных работ	Дробнов М.П.		
Блок капитального строительства филиала СЭС	Заместитель директора по капитальному строительству – начальник управления	Жук Д.С.		

№ п/п	Перечень основных требований	Содержание требований
1	2	3
1	Общие требования к системе и обеспечению информационной безопасности	<p>Организация работ по установке инженерно-технических средств охраны должна соответствовать следующим нормативно-правовым, нормативным актам и документам:</p> <ul style="list-style-type: none"> – Федеральный закон от 21.07.2011 № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса»; – Федеральный закон от 27 июля 2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»; – Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»; – Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне»; – Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»; – Постановление Правительства РФ от 05.05.2012 г. № 458 «Об утверждении Правил по обеспечению безопасности и антитеррористической защищенности объектов топливно-энергетического комплекса»; – Постановление Правительства Российской Федерации от 03 августа 2024 г. № 1046 «Об утверждении требований обеспечения безопасности и антитеррористической защищенности объектов топливно-энергетического комплекса»; – Постановлением Правительства Российской Федерации от 16.02.2008 № 87 «О составе разделов проектной документации и требованиях к их содержанию»; – Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»; – Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»; – Приказ ПАО «Россети» от 14.12.2017 г. № 156 «Об утверждении Программы повышения качества производственного контроля (производственного комплаенса) в Группе компаний Россети, направленная на минимизацию уровня производственного травматизма» (пункты 16, 17); – Приказ ПАО «Россети» от 11.10.2024 г. № 463 «Об утверждении Требований обеспечения антитеррористической защищенности объектов ПАО «Россети» и его дочерних обществ, которым не присвоена категория опасности, либо объектов, не подлежащих категорированию». – «Правила устройства электроустановок» (ПУЭ). <p>При проектировании также необходимо учесть требования и положения иных нормативно-правовых, нормативных актов и документов, в том числе в сферах государственной и коммерческой тайны, противодействия коррупции, информационной и противопожарной безопасности, охраны труда, охраны окружающей среды и т.д., а также руководствоваться последними редакциями актов и документов, действующих на момент разработки проектной и рабочей документации.</p>
2	Заказчик	ПАО «Россети Московский регион»

3	Цель и задачи комплекса работ	<p>Обеспечение непрерывного и устойчивого электроснабжения потребителей на территории г. Москвы и Московской области (в том числе в период проведения значимых мероприятий) в зоне ответственности ПАО «Россети Московский регион».</p> <p>Создание системы безопасности и антитеррористической защищенности энергообъектов ПАО «Россети Московский регион», соответствующей требованиям нормативно-правовых документов.</p> <p>Обеспечение управления безопасностью и антитеррористической защищенностью ПАО «Россети Московский регион» в единой системе ситуационно-аналитического управления ПАО «Россети».</p> <p>Комплекс работ по обеспечению безопасности предназначен для решения следующих задач:</p> <ul style="list-style-type: none"> – организация круглосуточного мониторинга оперативной обстановки в части безопасности функционирования электросетевых объектов (террористические и другие угрозы безопасности электроснабжению, пожары, несчастные случаи, происшествия и др.). – приведение инженерно-технических средств охраны объектов в соответствие требованиям нормативно-правовых документов; – обеспечение круглосуточного контроля соблюдения установленного режима безопасности и антитеррористической защищенности на энергообъектах и в районах их размещения; – обеспечение информационно-аналитической поддержки Оперативного штаба по обеспечению надежности электроснабжения руководства ПАО «Россети Московский регион» и ЦУБ ПАО «Россети» в режиме повседневной деятельности и при чрезвычайных ситуациях на электросетевых объектах; – обеспечение передачи оперативной информации о состоянии безопасности от дежурных работников электросетевых объектов до ДП РЭС филиалов ПАО «Россети Московский регион», ДП ОЗ филиалов ПАО «Россети Московский регион», ЦУБ ПАО «Россети Московский регион» (дежурный по безопасности ЦУБ), ЦУБ ПАО «Россети» (дежурный по безопасности ЦУБ) в единой системе передачи оперативной информации ПАО «Россети» (электронный оперативный журнал); – обеспечение взаимодействия дежурной службы ЦУБ ПАО «Россети Московский регион» с дежурными службами вышестоящих органов управления электросетевого комплекса, других организаций и ведомств в соответствии с установленными полномочиями; – обеспечение системного анализа регулярно собираемой подразделениями безопасности информации и подготовки отчетно-аналитических документов; – оснащение ЦУБ ПАО «Россети Московский регион» и ИТЦ филиалов, современными, автоматизированными средствами контроля за состоянием комплексной безопасности объектов и модернизация системы сбора и передачи информации с объектового уровня. <p>Проведение комплекса работ позволит привести систему безопасности и антитеррористической защищенности объектов в соответствие требованиям нормативно-правовых документов, а также сократить время на сбор информации и принятие наиболее эффективных управленческих решений в области безопасности.</p> <p>Построенные системы будут использованы в текущей производственной деятельности ПАО «Россети Московский регион».</p>
---	-------------------------------	--

		регион» для сокращения сроков реагирования на угрозы и возникновение чрезвычайных ситуаций и происшествий природного, техногенного и иного характера за счет повышения уровня физической защищенности энергообъектов Общества.
4	Исполнитель	Определяется по итогам закупочной процедуры
5	Характеристика объектов	ПС 220 кВ №676 «Уча»: оснащение инженерно - техническими средствами охраны, длина периметра 841 п.м.
6	Вид строительства	Реконструкция
7	Требования к качественным характеристикам выполнения работ	<p>7.1. Подрядчик гарантирует:</p> <ul style="list-style-type: none"> – качество выполнения всех работ в соответствии с рабочей документацией, действующими нормами и техническими условиями; – своевременное устранение недостатков и дефектов, выявленных при приемке работ и в период гарантийной эксплуатации объекта. <p>7.2. Гарантийный срок качества выполненных работ устанавливается в течение 12 (двенадцати) месяцев от даты ввода в промышленную эксплуатацию.</p> <p>Если в период гарантийного срока обнаружатся дефекты, препятствующие нормальной эксплуатации, то Подрядчик обязан устранить их за свой счет и в согласованные сроки.</p> <p>Для участия в составлении акта, фиксирующего дефекты, согласования порядка и сроков их устранения Подрядчик обязан командировать своего представителя не позднее 3-х (трех) дней со дня получения письменного извещения Заказчика.</p> <p>Гарантийный срок в этом случае продлевается соответственно на период устранения дефектов.</p> <p>7.3. Сторона, предоставившая материалы, конструкции гарантирует их надлежащее качество, соответствие их государственным стандартам и техническим условиям, обеспеченность их соответствующими сертификатами и другими документами, удостоверяющими их качество.</p> <p>7.4. Указанные гарантии не распространяются на случаи преднамеренного повреждения объекта со стороны третьих лиц, вследствие нормального износа объекта или неверной эксплуатации, либо ненадлежащего ремонта объекта, произведенного самим Заказчиком или привлеченными им третьими лицами.</p>
8	Сроки выполнения работ	<p>Начало работ: с момента заключения договора на выполнение ПИР.</p> <p>Окончание работ: сроки окончания договора ПИР.</p>
9	Требования к инженерно-техническим средствам охраны ПС 220 кВ №676 «Уча»	<p>Энергообъекты ПАО «Россети Московский регион», которым категория опасности не присвоена, оснащаются инженерно-техническими средствами охраны в соответствии с приказом ПАО «Россети» от 11.10.2024 г. № 463 «Об утверждении Требований обеспечения антитеррористической защищенности объектов ПАО «Россети» и его дочерних обществ, которым не присвоена категория опасности, либо объектов, не подлежащих категорированию».</p> <p>При реализации проекта предусмотреть применение отечественного импортозамещающего оборудования, оборудования с высокой степенью локализации производства на территории Российской Федерации или предусмотреть применение аналогичного оборудования производства государств, не поддерживавших санкционную политику в отношении России, имеющего сертификаты соответствия, акты и протоколы испытаний, подтверждающие технические характеристики (Приказ ПАО «Россети» от 05.02.2020 № 46 «Об утверждении корпоративного плана импортозамещения ПАО «Россети»).</p>

Объемы работ по созданию или реконструкции инженерно-технических средств охраны на энергообъекте определяется данным техническим заданием и могут уточняться на этапе предпроектного обследования, исходя из типа и категории Объекта, анализа его уязвимости, оценки эффективности существующей системы физической защиты и требований нормативно-правовых документов.

Модернизация комплекса инженерно-технических средств охраны (КИТСО) ПС 220 кВ №676 «Уча» включает:

1. инженерно-технические средства защиты:

- 1.1. инженерные заграждения;
 - а) противотаранное устройство;
- 1.2. инженерные средства и сооружения;
 - а) защита кабель каналов
 - б) защита трансформаторов

2. технические средства охраны:

- 2.1. система охранной сигнализации;
- 2.2. система охранная телевизионная;
- 2.3. система контроля и управления доступом (СКУД);
- 2.4. система сбора и обработки информации.
- 2.5. система охранного освещения;
- 2.6. система оповещения;
- 2.7. система электропитания ИТСО.

Система охранной сигнализации, система охранная телевизионная, система сбора и обработки информации, система контроля и управления доступом и система охранного освещения должны поддерживать сопряжение друг с другом и представлять единую комплексную систему безопасности объекта, с передачей сигналов на пост охраны, центр управления безопасностью (ЦУБ) и информационно-технический центр (ИТЦ) филиала.

В целях обеспечения управления безопасностью и антитеррористической защищенностью объектов ПАО «Россети Московский регион» в единой системе ситуационно-аналитического управления ПАО «Россети», а также интеграции существующих и создаваемых систем управления безопасностью в ИТЦ филиала ПАО «Россети Московский регион – Северные электрические сети и ЦУБ ПАО «Россети Московский регион», рекомендуется использование систем безопасности на базе ISS, ITV. При выборе оборудования учитывать совместимость поддержки протокола ONVIF, а также программного интерфейса интеграции приложений API.

9.1. Инженерно-технические средства защиты должны включать:

- инженерное заграждение;
- инженерные средства и сооружения;

Инженерно-технические средства защиты объекта должны обеспечивать круглогодичную защищенность объекта от актов незаконного вмешательства путем разрушения, взлома строительных защитных конструкций, преодоления ограждений, вскрытия запирающих устройств.

9.1.1. Инженерные заграждения по функциональному назначению подразделяются на:

- а) основное ограждение;
- б) дополнительное ограждение.

К основному ограждению предъявляются следующие требования:

	<p>а) конструкция и материалы должны обеспечивать высокую прочность, надежность защиты, долговечность и экономичность в эксплуатации;</p> <p>б) высота ограждения должна затруднять преодоление путем перелеза, а также удовлетворять режимным условиям объекта.</p> <p>Основное ограждение возводится по периметру объекта, в нем не должно быть лазов, проломов и других повреждений, не запираемых и неконтролируемых ворот и калиток, а также облегчающих несанкционированное проникновение на территорию объекта конструкций. Основное ограждение должно быть сплошным.</p> <p>Ограждение должно исключать случайный проход людей (животных), въезд транспорта или затруднять проникновение нарушителей на охраняемую территорию.</p> <p>Суммарная высота основного ограждения и верхнего дополнительного ограждения от уровня земли должна составлять не менее 2,5 метра.</p> <p>При выборе типа и высоты основного ограждения должен учитываться риск совершения актов незаконного вмешательства в отношении объекта.</p> <p>Сплошное ограждение может быть:</p> <p>а) железобетонным (толщина не менее 100 миллиметров);</p> <p>б) сплошным металлическим (толщина листа не менее 2 миллиметров).</p> <p>Верхнее дополнительное ограждение представляет собой противоперелезный козырек на основе спиральной или плоской армированной колючей ленты диаметром не менее 0,5 метра или проволочного (сетчатого) полотна шириной не менее 0,6 метра и устанавливается сверху основного ограждения, на внешних сторонах крыш и (или) стен одноэтажных зданий высотой до 4 метров, являющихся составной частью периметра объекта.</p> <p>Разрешается размещать на основном ограждении или рядом с ним:</p> <p>а) систему охранной сигнализации;</p> <p>б) систему охранную телевизионную;</p> <p>в) систему охранного освещения.</p> <p>9.1.2. Инженерные средства и сооружения.</p> <p>Инженерные средства и сооружения обеспечивают создание для подразделений охраны необходимых условий по выполнению задач по защите охраняемого объекта.</p> <p>К инженерным средствам и сооружениям относятся:</p> <p>а) инженерное оборудование постов охраны;</p> <p>б) защитные конструкции</p> <p>в) разграничительные и предупредительные знаки;</p> <p>г) контрольно-пропускные пункты.</p> <p>К защитным конструкциям относятся:</p> <p>а) средства защиты трансформаторов (устройство защитного каркаса силового трансформатора из фундаментных блоков ФБС, просечного металлического листа);</p> <p>б) средства защиты кабельных каналов от огневого поражения;</p> <p>в) установка блоков, ежей по защите въездных групп ПС,</p> <p>г) средства защиты дверных проемов (для наружных дверей и дверей помещений критических элементов объекта):</p> <ul style="list-style-type: none"> – металлические дверные конструкции; – металлические конструкции со вставками из защитного остекления;
--	--

		<p>Для предупреждения о запрещении прохода в запретную зону по линии ее ограждения устанавливаются предупредительные знаки с надписями: «Запретная зона! Проход (проезд) запрещен (закрыт)», «Внимание! Охраняемая территория». Надписи делаются на русском языке</p> <p>Предупредительные знаки устанавливаются по внутреннему ограждению запретной зоны на расстоянии не более 50 метров друг от друга на ограждении или с использованием отдельных столбов, а также на изгибах (углах) запретной зоны, калитках и воротах в запретную зону.</p> <p>Основное ограждение объекта на въездах (выездах) оборудуется основными и запасными (аварийными) воротами, закрывающимися на внутренний замок. Подвеска ворот должна исключать их снятие с петель без применения инструмента. Расстояние от нижнего края створок ворот до уровня земли должно быть не более 0,1 м.</p> <p>Ворота изготавливаются сплошными из металлоконструкций. Конструкция ворот должна обеспечивать их жесткую фиксацию в закрытом положении.</p> <p>Для электромеханических приводов, дополнительно к дистанционному, предусматривается ручное открывание ворот.</p> <p>Высота ворот должна составлять не менее 2,0 м. Ворота должны быть оборудованы дополнительным верхним ограждением высотой не менее 500±20 мм, изготовленным из спирального барьера «Егоза» (учитывая конструктивные особенности автоматических откатных ворот).</p> <p>Калитка должна запираться на врезной, накладной замок или на засов с висячим замком (с внутренней стороны).</p> <p>Въезды (выезды) объекта должны быть оборудованы противотаранными устройствами, создающими препятствие проезду.</p> <p>9.1.3. Контрольно-пропускной пункт оборудуется на основном входе (выходе) и направлении въезда (выезда) объекта.</p> <p>На контрольно-пропускном пункте двери для прохода людей, выходящие за территорию объекта, оборудуются смотровым глазком и переговорным устройством или видеодомофоном, а также внешним освещением. Снаружи устанавливается телекамера для наблюдения за подступами.</p> <p>Двери контрольно-пропускного пункта, выходящие за территорию объект, оборудуются замковыми устройствами. Окна и двери оборудуются защитными конструкциями.</p> <p>Освещенность зон контрольно-пропускного пункта в любое время суток составляет не менее 20 люксов - для прохода людей, не менее 75 люксов - для проходных коридоров и будок охраны, не менее 3 люксов - для площадки осмотра. Освещенность в помещениях контрольно-пропускных пунктов мест, где производится проверка пропусков, должна быть не менее 150 люксов.</p> <p>Устройства управления механизмами открывания, прохода (проезда), техническими средствами охраны, охранном освещением и оповещением должны располагаться в помещении контрольно-пропускного пункта и быть ограничены от доступа к ним посторонних лиц.</p> <p>Зона контрольно-пропускного пункта, отведенная для прохода людей, оборудуется следующими инженерно-техническими средствами:</p> <ul style="list-style-type: none"> а) ограждения проходов; б) преграждающее управляемое устройство;
--	--	---

	<p>в) кабина (помещение) работника подразделения охраны контрольно-пропускного пункта.</p> <p>Для ограждения проходов используются барьеры из металлоконструкций, дерева и других материалов.</p> <p>В качестве преграждающих управляемых устройств устанавливают турникеты или шлюзовые кабины, оснащенные считывателями системы контроля и управления доступом на вход и выход.</p> <p>Контрольно-пропускной пункт должен обеспечивать защиту сотрудников подразделения охраны от возможных враждебных действий нарушителей, при этом должна обеспечиваться невозможность наблюдения посторонними лицами за внутренним пространством помещения.</p> <p>Контрольно-пропускной пункт должен быть оснащен электроотопительными, осветительными приборами, индивидуальным электрическим щитком, электрическими и телекоммуникационными розетками, системой кондиционирования, необходимой мебелью (столы, стулья, шкафы и т.д.), АРМ оператора службы охраны Объекта, СКУД и другими техническими средствами охраны.</p> <p>Оконные проемы оборудуются защитными металлическими конструкциями, представляющими из себя наклонную сетку с ячейкой не более 20х20 мм. Все дверные проемы оборудуются стальными дверными конструкциями.</p> <p>9.2. Технические средства охраны (далее-ТСО), входящие в комплекс технических средств охраны объекта, через систему сбора и обработки информации должны быть интегрированы между собой и представлять из себя единую автоматизированную систему безопасности объекта.</p> <p>ТСО включают:</p> <ul style="list-style-type: none"> – систему охранной сигнализации; – систему охранную телевизионную; – систему контроля и управлением доступом СКУД; – систему сбора и обработки информации; – систему охранного освещения.; – систему электропитания ИТСО <p>ТСО должны обеспечивать:</p> <ul style="list-style-type: none"> – оценку ситуации на основе всех имеющихся данных и возможность принятия эффективных мер по реагированию на возникающие ситуации с предварительно-сформированными сценариями; – оперативное наблюдение и контроль за обстановкой на объекте; – программируемую автоматическую реакцию любой системы ТСО на тревожные события в другой системе и за счёт этого снижение влияния человеческого фактора; – протоколирование событий с возможностью их достоверного анализа; – распределение прав доступа к информации; – хранение протоколов событий на цифровых накопителях в течение не менее 30 суток. <p>Техническими средствами охраны оборудуются периметр объекта, контрольно-пропускные пункты (при наличии), периметр критических элементов объекта, а также другие площадки, здания и помещения, определяемые субъектом топливно-энергетического комплекса.</p>
--	---

		<p>При размещении технических средств охраны вне помещения, а также в неотапливаемых помещениях должны применяться оборудование соответствующего климатического исполнения и использоваться всепогодные запираемые шкафы с охранным извещателем, контролирующим открывание или взлом двери такого шкафа.</p> <p>Во взрывопожароопасных местах объекта топливно-энергетического комплекса должны применяться технические средства охраны во взрывозащищенном исполнении.</p> <p>Локальная вычислительная сеть технических средств охраны должна представлять собой отдельную физически изолированную сеть или сегмент локально-вычислительной сети объекта топливно-энергетического комплекса, доступ в который ограничен соответствующими правами.</p> <p>При наличии объективных факторов обмен данными с внешними системами (сетями) должен быть организован с применением сертифицированных средств защиты информации.</p> <p>При интеграции технических средств охраны должен обеспечиваться:</p> <ul style="list-style-type: none"> – автоматический вывод на выделенный тревожный монитор или автоматизированное рабочее место изображений, получаемых с камер, контролирующих участок срабатывания охранной сигнализации, для подтверждения факта совершения противоправных действий, определения характера нарушения, оценки ситуации, а также принятия необходимых мер; – автоматическое позиционирование поворотной видеокамеры (при наличии у нее такой возможности) на участок срабатывания охранной сигнализации; – автоматическое включение светильников и дополнительного охранного освещения (при его наличии) на участке срабатывания системы охранной сигнализации; – автоматическое включение устройств оповещения о тревоге по сигналам, полученным от технических средств охраны, в соответствии с алгоритмами, определенными субъектом топливно-энергетического комплекса. <p>В случае отказа алгоритмов интеграции должна быть предусмотрена возможность ручного управления всеми системами.</p> <p>9.2.1. Система охранной сигнализации (далее - СОС).</p> <p>Система охранной сигнализации должна поддерживать сопряжение с другими системами комплекса инженерно-технических средств охраны - системой охранной телевизионной, системой сбора и обработки информации.</p> <p>Система охранной сигнализации включает следующие технические средства:</p> <ul style="list-style-type: none"> а) периметральные средства обнаружения, предназначенные для обнаружения нарушителей на открытых площадках (периметр объекта, границы локальных зон и др.); б) средства обнаружения проникновения - автоматические и неавтоматические охранные извещатели (тревожная сигнализация), предназначенные для охраны помещений; в) средства сбора и обработки информации - приборы приемно-контрольные, а также блоки, устройства и модули в составе комплексных (интегрированных) систем, обеспечивающие прием извещений от охранных извещателей, обработку и отображение информации, осуществление местного звукового и светового оповещения, управление взятием (снятием) на (с) охраны.
--	--	---

Система охранной сигнализации охраняемого объекта должна обеспечивать получение и обработку тревожных извещений с периметральных средств обнаружения, автоматических и неавтоматических извещателей, возможность учета и хранения сигнальной информации, отображения информации о тревожных событиях с возможным дублированием в ИТЦ филиала, при наличии физической охраны, на пост охраны.

Управление системой охранной сигнализации должно осуществляться с применением административного пароля от несанкционированного доступа к управлению.

Периметральные средства обнаружения нарушителя и извещатели должны обнаруживать несанкционированное проникновение нарушителя в зону с вероятностью не ниже 0,90 и выдавать тревожное извещение по проводному или беспроводному каналу связи.

Информация о событиях, формируемая системой охранной сигнализации, должна храниться не менее 30 суток.

Периметральными средствами обнаружения или охранными извещателями оборудуются периметр объекта, выделенные зоны охраны, уязвимые зоны и критические элементы объекта.

Периметральными средствами обнаружения или охранные извещатели должны быть размещены таким образом, чтобы исключить возможность обхода или преодоления их зоны обнаружения без формирования извещения о тревоге.

Климатическое исполнение периметральных средств обнаружения и извещателей должно соответствовать климатической зоне применения.

Периметральные средства обнаружения и извещатели должны обеспечивать помехозащищенность. Их допустимое удаление от помеховых факторов должно быть не менее значений, указанных в эксплуатационной документации.

Периметральные средства обнаружения и извещатели устанавливаются максимально скрытно или замаскировано, они не должны иметь визуально обнаруживаемых регулировок или элементов индикации.

Кабельные линии средств обнаружения прокладываются по внутренней стороне основного ограждения в металлических или пластиковых коробах, трубах, каналах либо в специальных подземных траншеях.

Периметральные средства обнаружения устанавливаются по периметру (границе территории) зоны или объекта:

а) на (вблизи) основных и дополнительных ограждениях по периметру;

б) вблизи ограждений выделенных локальных зон внутри охраняемой территории объекта и непосредственно на таких ограждениях.

Периметральные средства обнаружения и охранные извещатели в автоматическом режиме работы должны:

а) с заданной вероятностью обнаруживать действия нарушителя и выдавать сигнал срабатывания (извещение) о его проникновении;

б) выдавать сигнал о неисправности при отказе или взломе;

в) с заданной достоверностью (вероятностью, средней наработкой на ложную тревогу) не выдавать ложные сигналы при воздействии негативных факторов природного и техногенного характера;

г) иметь электромагнитную совместимость с технологическим оборудованием охраняемого объекта, системами комплекса инженерно-технических средств охраны;

д) при отключении сетевого источника электропитания и переходе на резервный автономный источник сохранять работоспособность и не выдавать ложных тревог в течение не менее 24 часов в дежурном режиме и не менее 3 часов в режиме тревоги (СОТ и СОО не менее 25 минут);

е) не требовать обслуживания и настройки в течение срока эксплуатации, за исключением периодических регламентных и ремонтных работ.

Периметральные средства обнаружения должны иметь вход управления, который позволяет подать на него с пульта централизованного наблюдения сигнал дистанционного контроля для проверки работоспособности.

Линия основного ограждения оборудуется однорубежной системой периметральной охранной сигнализации. При этом:

– двухпозиционные средства обнаружения радиолучевого принципа действия с поляризованным излучением применяются на сплошных ограждениях (железобетонных, кирпичных и металлических);

– средства обнаружения вибрационного (трибоэлектрического) принципа действия применяются на просматриваемых ограждениях.

Ворота и калитки блокируются «на открывание» и «на проникновение». Блокировка «на открывание» осуществляется установкой на створки ворот (калиток) магнитоконтактных датчиков положения, блокировка на «проникновение» - установкой радиолучевых двухпозиционных извещателей. Ворота и калитки выделяются в отдельные шлейфы сигнализации.

9.2.2. Система охранная телевизионная.

Система охранная телевизионная (СОТ) предназначена для:

а) объективного контроля за обстановкой в охранных зонах объекта (территория, помещения, критические элементы);

б) выявления и подтверждения фактов несанкционированных действий нарушителей;

в) установления фактической угрозы конкретных противоправных действий;

г) оценки ситуации и идентификации нарушителей.

Видеокамеры устанавливаются на отдельных опорах, кронштейнах, закрепленных на основном ограждении, опорах охранного освещения, конструкциях объекта, стенах зданий и сооружений или внутри помещений, в том числе на дистанционно управляемых поворотных платформах.

Место и высота установки каждой видеокамеры, тип объектива и угол наклона его оптической оси определяются исходя из условия формирования необходимой зоны наблюдения, в том числе непрерывной зоны для наблюдения замкнутого периметра объекта.

На объектах без постоянного присутствия обслуживающего персонала применяются элементы системы охранной телевизионной (видеокамеры, устройства записи, управления, коммутации и др.), которые имеют повышенную защищенность и которые размещаются в местах, исключающих возможность их умышленного повреждения.

Для установления факта реальной угрозы противоправных действий нарушителя в местах размещения критических элементов объекта видеокамеры должны обеспечивать детализацию и распознаваемость обстановки.

		<p>Система охранная телевизионная объекта должна обеспечивать:</p> <ul style="list-style-type: none"> а) передачу визуальной информации о состоянии периметра, контролируемых зон и помещений на пост централизованной охраны объекта; б) в случае получения сигнала срабатывания технических средств охраны (извещения о тревоге) передачу оператору изображения из охраняемой зоны для оценки характера возможного нарушения, направления движения нарушителя с целью определения оптимальных мер силового или технологического противодействия; в) работу в автоматизированном режиме; г) визуальный контроль объекта и прилегающей к нему территории; д) визуальный контроль за действиями подразделений охраны при несении службы, предоставление необходимой информации для координации этих действий; е) архивирование и последующее воспроизведение записи всех значимых событий для их анализа в автоматическом режиме или по команде оператора; ж) оперативный доступ к видеоархиву путем задания времени, даты и идентификатора телевизионной камеры; з) совместную работу с системой контроля и управления доступом и системой охранной сигнализации; и) автоматический вывод изображений с телевизионных камер по сигналам технических средств охраны или видеодетекторов; к) разграничение доступа к управлению и видеоинформации с целью предотвращения несанкционированных действий. <p>С использованием выделенного канала связи, реализуемого в рамках отдельного проекта, система охранная телевизионная объекта должна иметь опциональную возможность:</p> <ul style="list-style-type: none"> а) передачи визуальной информации о состоянии периметра, контролируемых зон и помещений в ИТЦ филиала и ЦУБ; б) предоставления оператору ИТЦ филиала и ЦУБ дополнительной информации о состоянии наблюдаемого (охраняемого) объекта с целью исключения ложных тревог, включение видеозаписи для последующего анализа; <p>Средствами системы охранной телевизионной оборудуются следующие локальные зоны объекта:</p> <ul style="list-style-type: none"> а) периметр территории объекта или его наиболее уязвимые части; б) все контрольно-пропускные пункты (при наличии) и запасные проходы (проезды) на объект (при наличии); в) досмотровые помещения (комнаты), зоны досмотра (при наличии); г) помещение диспетчерского пункта (ЩУ) (при наличии). <p>Видеокамеры, предназначенные для объективного контроля обстановки вблизи критических элементов, должны иметь повышенную защищенность. Их следует устанавливать вне прямой досягаемости выведения из строя случайными нарушителями.</p> <p>Уровень зоны наблюдения в темное время суток должен обеспечивать заданные параметры телевизионного наблюдения.</p> <p>Зоны охранного освещения должны совпадать или несколько превышать по габаритам зоны обзора видеокамеры. При необходимости наблюдения больших территорий должны применяться объективы с переменным фокусным расстоянием и поворотные платформы с дистанционным управлением.</p>
--	--	---

		<p>Вне помещений (на улице) следует комплектовать видеокамеры объективами с автоматической регулировкой диафрагмы.</p> <p>СОТ создается с применением сетевых технологий (IP-система) на основе программно-аппаратных средств российской разработки. Подключение сетевых программно-аппаратных средств к периферийному оборудованию осуществлять с помощью коммутаторов российского производства.</p> <p>Подключение сетевых ПАК к периферийному оборудованию осуществлять с помощью коммутаторов российского производства.</p> <p>Стационарные видеокамеры должны обеспечивать высокое качество изображения при разрешении не менее 1080p пикселей с частотой не менее 25 кадров/с и осуществляют передачу видеоданных одновременно двумя потоками не хуже h.264.</p> <p>Характеристики используемых видеокамер должны соответствовать требованиям нормативно-правовых документов.</p> <p>Система охранная телевизионная должна обеспечивать возможность документирования видеоинформации с привязкой к дате и времени записи события с дискретностью не более одной секунды.</p> <p>Запись видеоинформации от камер должна осуществляться по следующим правилам:</p> <ul style="list-style-type: none"> – непрерывная запись в дежурном режиме с разрешением не менее 1080p с частотой не менее 25 кадров/с, с глубиной архива не менее 30 суток на 1 канал в формате не хуже h.264; – тревожная запись, включающаяся при срабатывании СОС в зоне обзора соответствующей камеры либо при обнаружении движения в кадре, с разрешением не менее 1080p с частотой не менее 25 кадров/с в формате не хуже h.264. <p>Видеокамеры должны работать в режиме день-ночь - при понижении уровня освещенности должно происходить автоматическое переключение из полноцветного режима в чёрно - белый.</p> <p>Для обзора внутренней территории объекта, в том числе для контроля состояния оборудования применяются цветные купольные позиционируемые (поворотные) гибридные видеокамеры.</p> <p>Стационарные видеокамеры должны быть размещены в погодных кожухах для обеспечения их работоспособности в диапазонах температур от -35°C до +40°C со степенью защиты IP66.</p> <p>Для защиты видеокамер и коммутационных портов сетевого оборудования от импульсных перенапряжений, возникающих в результате электрических разрядов, молний или воздействия электрических наводок, должны быть установлены устройства защиты от импульсных перенапряжений.</p> <p>Видеокамеры должны располагаться таким образом, чтобы исключить не просматриваемые участки («мертвые» зоны) и, что бы один и тот же участок попадал в зону обзора как минимум двух видеокамер.</p> <p>При возникновении тревожного события в одной из систем (СОС, СКУД (при наличии), СОТ) на экран монитора оператора в автоматическом режиме должно выводиться изображение от телекамеры, в зоне обзора которой произошло событие.</p> <p>Видеосигналы с видеокамер должны поступать на сетевой видеорегистратор (сервер), который обеспечивает их передачу пользователям и запись (архивирование).</p> <p>Одновременно с процессом записи видеорегистратор (сервер) должен обеспечивать предоставление пользователям текущих</p>
--	--	--

	<p>видеопотоков с видеокамер, которые он записывает, с функциями удаленного управления камерами.</p> <p>Независимо от процессов записи видеорегистратор (сервер) должен обеспечивать предоставление видеопотоков из архива по запросу, при этом должны быть доступны следующие функциональные возможности:</p> <ul style="list-style-type: none"> – поиск интересующих записей по указанной камере на определенный день/час/минуту/секунду; – просмотр в режиме реального времени видеозаписи с возможностью управления: просмотр вперед/назад и пауза; – ускоренный просмотр (до стократного ускорения) как в прямом, так и в обратном направлении. <p>Видеоинформация должна отображаться на автоматизированном рабочем месте (АРМ) оператора охраны объекта в различных режимах - полноэкранном, мультиэкранном, по заданной программе.</p> <p>АРМ выполняется на базе персонального компьютера. В состав АРМ включается дополнительный жидкокристаллический монитор с размером видимого изображения по диагонали 24 дюйма.</p> <p>Для передачи видеосигналов на объекте устанавливаются коммутаторы предпочтительно российского производства.</p> <p>Вся видеоинформация должна храниться на цифровых накопителях информации для категорированных объектов не менее 30 суток.</p> <p>9.2.3. Система контроля и управления доступом (СКУД).</p> <p>Система контроля и управления доступом обеспечивает санкционированный доступ на объект и в зоны ограниченного доступа на объекте путем идентификации личности по одному признаку или по комбинации различных идентификационных признаков, включая:</p> <ul style="list-style-type: none"> – вещественный код (карточки доступа, ключи touch-memo и другие устройства); – запоминаемый код (клавиатуры, кодонаборные панели и другие устройства); – биометрические признаки (отпечатки пальцев, сетчатка глаз и другие признаки); – фотопроверификацию. <p>Система контроля и управления доступом объекта должна обеспечивать:</p> <ul style="list-style-type: none"> – управление доступом персонала на охраняемые территории по уровню доступа, согласно разрешений; – формирование ретроспективных справок и отчетов; – учёт рабочего времени работников предприятия; – учёт изготовления и выдачи электронных пропусков; – совместную работу с другими, установленными на объекте, системами (системой охранного телевидения); – санкционированный доступ и предотвращение несанкционированного доступа людей и транспорта на объекты, в отдельные зоны, здания и помещения; – выдачу информации на пульт охраны объекта и пульт централизованного наблюдения комплекса технических средств охраны о попытках несанкционированного доступа на объект; – работоспособность в автономном и сетевом режиме с автоматическим переходом из первого во второй при обрыве связи, нарушении ЛВС (универсальность системы). <p>В состав СКУД объекта могут входить:</p> <ul style="list-style-type: none"> – устройства, преграждающие с ручным, полуавтоматическим или автоматическим управлением в составе преграждающих
--	---

	<p>конструкций и исполнительных устройств, обеспечивающие частичное (турникет) или полное (дверь) перекрытие проема прохода;</p> <ul style="list-style-type: none"> – устройства ввода идентификационных признаков в составе считывателей и идентификаторов личности; – периферийные программно-аппаратные устройства управления, центральные программно-аппаратные устройства управления, располагаемые на пульте централизованного наблюдения; – видеодомофон. <p>СКУД должна обеспечивать выполнение функциональных требований:</p> <ul style="list-style-type: none"> – открывание преграждающих устройств при считывании зарегистрированного в памяти системы идентификационного признака, запрет открывания при считывании незарегистрированного идентификационного признака; – запись идентификационных признаков идентификатора в память системы, защиту от несанкционированного доступа при этом; – защита от манипулирования путем перебора или подбора идентификационных признаков; – сохранение идентификационных признаков в памяти при отказе и отключении электропитания; – ручное, автоматическое аварийное открывание преграждающих устройств, для прохода при аварийных ситуациях, пожаре, технических неисправностях в соответствии с установленным режимом и правилами противопожарной безопасности; – выдача сигнала тревоги при аварийном открывании преграждающих устройств, в случае несанкционированного проникновения; – регистрация и протоколирование текущих (штатных) и тревожных событий, приоритетное отображение тревожных событий на пульте централизованного наблюдения; – задание временных режимов действия идентификаторов и уровней доступа по командам оператора; – защиту программно-аппаратных средств системы контроля и управления доступом от несанкционированного доступа к элементам управления, информации, базам данных; – автоматический контроль исправности технических средств и линий передачи информации; – возможность автономной работы периферийных технических средств, с сохранением ими основных функций при отказе связи с пультом централизованного наблюдения; – установку с пультом централизованного наблюдения режима свободного доступа при аварийных и чрезвычайных ситуациях, блокировку прохода по точкам доступа в случае нападения на объект; – возможность подключения дополнительных программно-аппаратных средств специального контроля и досмотра; – интегрирование с системой охранного телевидения. <p>Считыватели или идентификаторы должны обеспечивать надежное считывание идентификационного признака с идентификатора и его передачу на устройства управления и обмен информацией.</p> <p>Конструкция и внешний вид считывателя (идентификатора) не должны приводить к раскрытию применяемых кодов.</p>
--	--

		<p>Программно-аппаратные средства управления СКУД должны обеспечивать:</p> <ul style="list-style-type: none"> в отношении аппаратных средств управления (контроллеров): <ul style="list-style-type: none"> – прием информации от считывателей, ее обработку и выработку сигналов управления на исполнительные устройства; – обмен информацией по линии связи между контроллерами и средствами управления; – сохранность данных в памяти, в том числе при обрыве линий связи с пультом централизованного наблюдения, отключении и/или переходе на резервное питание; – контроль линий связи между считывателями, контроллерами и пультом централизованного наблюдения; – протоколы обмена должны обеспечивать необходимую помехоустойчивость, скорость и защиту информации; – в отношении программного обеспечения: <ul style="list-style-type: none"> – занесение кодов идентификаторов в память системы; – задание характеристик точек доступа, установку временных интервалов и уровней доступа для пользователей; – протоколирование текущих событий, ведение и поддержание базы данных; – регистрацию прохода через точки доступа в протоколе; – сохранение базы данных и системных параметров на резервном носителе информации, в том числе при сбоях в системе; – приоритетный вывод информации о нарушениях; – возможность управления преграждающими и исполнительными устройствами в случае чрезвычайной ситуации. <p>Программное обеспечение устройств управления системы контроля и управления доступом должно быть устойчиво к случайным или преднамеренным воздействиям (отключение питания аппаратных средств, программный или аппаратный рестарт аппаратных средств, случайные нажатие клавиш на клавиатуре или перебор пунктов меню программы).</p> <p>Воздействия не должны приводить к открыванию управляемых преграждающих устройств и изменению действующих кодов доступа.</p> <p>Система контроля и управления доступом при отключении электропитания должна обеспечивать сохранение своих настроек, в том числе настроек базы данных идентификационных признаков и архива событий, а также работу управляемых преграждающих устройств в автономном режиме при потере связи с сервером.</p> <p>Информация о событиях, формируемая системой контроля и управления доступом, должна храниться не менее 30 суток.</p> <p>9.2.4. Система сбора и обработки информации.</p> <p>Система сбора и обработки информации комплекса технических средств охраны должна обеспечивать:</p> <ul style="list-style-type: none"> – прием тревожных извещений о проникновении на объект; – управление взятием (снятием) объекта (зоны объекта) с охраны; – отображение полученной информации на посту централизованной охраны и ИТЦ филиала; – видеоверификацию полученной информации из зон установки видеокамер; – возможность доступа к архивным данным технических средств охраны для проведения их анализа. <p>Система сбора и обработки информации комплекса технических средств охраны должна обеспечивать возможность интеграции существующих и создаваемых систем управления безопасностью</p>
--	--	---

филиалов ИТЦ и ЦУБ ПАО «Россети Московский регион».

Система сбора и обработки информации комплекса технических средств охраны должна включать:

- объектовые технические средства сбора и первичной обработки информации с сигнализационных систем;
- подсистему передачи извещений проводного (радиоканального) типа;
- технические средства приема, обработки информации и ее представления в виде, удобном для принятия управленческих решений;
- линии связи и управления.

Система сбора и обработки информации должна обеспечивать возможность доступа к управлению только с поста охраны, ИТЦ филиала или ЦУБ ПАО «Россети Московский регион».

Дистанционное вмешательство в работу системы сбора и обработки информации через какой-либо другой внешний канал связи и интерфейс должно быть полностью исключено.

Подсистема передачи извещений должна обеспечивать передачу извещений (тревожных, служебных, информационных) от охраняемого объекта (средств, сбора и обработки информации) до пульта централизованного наблюдения, реализованного в рамках отдельного проекта.

9.2.5. Система охранного освещения.

Система охранного освещения должна обеспечивать:

- необходимые условия видимости ограждения территории, периметров зданий, зоны внешней территории, прилегающей к объекту, дорог, мест несения службы подразделений охраны;
- гарантированную освещенность не менее 10 люкс во всех контролируемых зонах;
- освещенность на уровне земли в горизонтальной плоскости или на уровне 0,5 метра от земли на одной стороне вертикальной плоскости, перпендикулярной к линии границы, не менее 0,5 люкс (в темное время суток);
- равномерно освещенную сплошную полосу шириной не менее 3 метров по периметру объекта;
- возможность автоматического включения дополнительных источников света на отдельных зонах охраняемой территории (периметра) при срабатывании системы охранной сигнализации;
- ручное управление аппаратурой освещения;
- использование энергосберегающих технологий;
- совместимость с техническими средствами системы охранной сигнализации и системы охранной телевизионной.

Электрическая сеть охранного освещения по периметру и на территории объекта должна разделяться на самостоятельные участки в соответствии с зонами системы охранной сигнализации и (или) зонами наблюдения системы охранной телевизионной. Она должна подключаться к отдельной группе распределительного щита, расположенного на периметре объекта расположенного в помещении охраны, закрытого на замок и оборудованного охранной сигнализацией.

Осветительные приборы системы охранного освещения должны быть установлены на основном ограждении или на отдельных опорах, фасадах (крышах) зданий и сооружений таким образом, чтобы исключить засветку видеокамер.

Светильники наружного охранного освещения должны быть защищены от механических повреждений, иметь рабочий диапазон температур, соответствующий климатической зоне, класс защиты

не ниже IP56 и обеспечивать световую эффективность не менее 100 люмен/ватт.

Освещенность мест в помещениях контрольно-пропускных пунктов, где производится проверка пропусков, должна быть не менее 150 люкс.

9.2.6. Система оповещения

Система оповещения о тревоге, чрезвычайных ситуациях на охраняемом объекте и его территории создается для оперативного информирования персонала о тревоге или чрезвычайной ситуации (нападении, террористическом акте и др.), привлечения внимания сторонних лиц, находящихся в непосредственной близости от объекта.

Система оповещения должна обеспечивать выполнение следующих функциональных требований:

- подачу звуковых и (или) световых сигналов в зданиях, помещениях и на территории объекта;
- возможность трансляции речевой информации.

Количество оповещателей (громкоговорителей) и их мощность должно обеспечивать слышимость во всех местах постоянного или временного пребывания персонала объекта и обеспечивать разборчивость передаваемых речевых сообщений.

Громкоговорители не должны иметь регуляторов громкости и разъемных соединений.

Коммуникации системы оповещения допускается проектировать совмещенными с радиотрансляционной сетью объекта.

Система оповещения должна интегрироваться с техническими средствами системы охранной сигнализации и системы охранной телевизионной.

9.2.7. Система электропитания

Электропитание комплекса инженерно-технических средств охраны объекта должно быть бесперебойным и осуществляться от двух независимых источников переменного тока или от одного источника переменного тока с автоматическим переключением на резервное питание от аккумуляторных батарей (в аварийном режиме) и оповещением персонала физической защиты о переходе на электропитание от резервного источника.

Для поддержания электропитания при переключении между двумя независимыми источниками питания предусматриваются аккумуляторные батареи.

Основное электропитание должно осуществляться от электрической сети переменного тока номинальным напряжением 220/380 В, резервное электропитание - от резервного ввода электрической сети переменного тока (независимый фидер) или от аккумуляторных батарей.

Линейно-кабельная сеть комплекса инженерно-технических средств охраны представляет собой совокупность кабельных линий, кабельного оборудования (боксы, шкафы, коробки) и линейно-кабельных устройств (кабельная канализация, вводы, распределительные шкафы), предназначенных для передачи в системах комплекса инженерно-технических средств охраны энергии электропитания сигнальной, речевой и видеоинформации, а также сигналов управления.

Основными требованиями к линейно-кабельной сети являются:

- а) скрытность прокладки проводных линий, кабелей связи и электропитания;

	<p>б) резервирование линий, кабелей и коммутационного оборудования;</p> <p>в) автономность от технологических кабельных сетей объекта.</p> <p>Кабельная сеть комплекса инженерно-технических средств охраны должна прокладываться в соответствии с требованиями нормативно-технической документации по устройству электроустановок и линейных сооружений сетей связи на промышленных предприятиях.</p> <p>Для достижения скрытности и исключения свободного доступа кабельная сеть комплекса инженерно-технических средств охраны прокладывается в грунте на глубине не менее 0,5 метра в поливинилхлоридных, асбоцементных или металлических трубах по территории или в кабельных каналах в зданиях объекта.</p> <p>Кабельная сеть, проложенная по периметру объекта, в целях повышения надежности обеспечения электроэнергией технических средств охраны должна быть электрически замкнутой в кольцо.</p> <p>В кабельной сети технических средств охраны предусматривается резерв соединительных линий не менее 10 процентов общей емкости кабеля.</p> <p>Распределительные коробки и боксы, установленные вне шкафов в зданиях (сооружениях) и контролируемых зонах, а также люки кабельных колодцев на территории объекта должны быть оборудованы средствами системы охранной сигнализации.</p> <p>Помещения, в которых размещены электрощиты, должны быть оборудованы средствами системы охранной сигнализации и системы контроля и управления доступом.</p> <p>Переключение с основного электропитания на резервное и обратно должно происходить автоматически без нарушения работы технических средств охраны за время не более 10 миллисекунд.</p> <p>При работе от резервного источника должно обеспечиваться функционирование комплекса инженерно-технических средств охраны в течение не менее 24 часов в дежурном режиме и не менее 3 часов в режиме тревоги.</p> <p>Приводы ворот, шлагбаумов и турникетов должны обеспечиваться электроэнергией от одного источника питания.</p> <p>Емкость аккумуляторной батареи должна обеспечивать работу инженерно-технических средств охраны узловых элементов линейных объектов в течение не менее 24 часов в дежурном режиме и не менее 3 часов в режиме тревоги, а средств системы охранной телевизионной и системы сбора и обработки информации - не менее 0,25 часа.</p> <p>Местоположение аварийных источников электропитания определяется исходя из их минимальной уязвимости при возможных противоправных действиях нарушителей.</p> <p>9.3. Требования к размещению оборудования технических средств охраны:</p> <p>Оборудование должно иметь защиту от несанкционированного доступа, механических повреждений и размещаться в местах, исключающих возможность его умышленного повреждения.</p> <p>9.4. Требования к условиям эксплуатации и стойкости к внешним воздействиям.</p> <p>Оборудование, устанавливаемое вне помещений, должно безотказно функционировать в диапазоне температур от -45°C до +40°C и относительной влажности 98% при +25°C, а также при воздействии атмосферных осадков и порывов ветра, характерных для климатической зоны размещения объекта.</p>
--	---

		<p>Предусмотреть заземление и грозозащиту наружных устройств. Оборудование, устанавливаемое в помещениях, должно безотказно функционировать в диапазоне температур от +5°C до +40°C и относительной влажности 80%.</p> <p>9.5. Требования стандартизации и унификации. Проектные решения должны использовать однотипные компоненты технических средств охраны в целях обеспечения снижения расходов на обслуживание и ремонт, взаимозаменяемости используемых компонентов, удобства эксплуатации. Должна обеспечиваться взаимная совместимость оборудования и программного обеспечения всех используемых систем на объекте. При производстве работ по модернизации необходимо учитывать «Типовые требования к корпоративному стилю оформления объектов, принадлежащих ПАО «Россети Московский регион».</p> <p>9.6. Требования к срокам эксплуатации и гарантии: Гарантийный срок службы инженерно-технических средств защиты должен быть не менее одного года. Срок службы - не менее 8 (восьми) лет.</p>
10	Особенности выполнения работ	<p>Работы выполняются в соответствии с утвержденным обеими сторонами планом-графиком.</p> <p>СМР и ПНР выполняются в соответствии с «Правилами технической эксплуатации электрических станций и сетей», «Правилами эксплуатации электроустановок потребителей» и с соблюдением Правила по охране труда при эксплуатации электроустановок и других отраслевых регламентирующих документов.</p> <p>Работы, выполняемые на территории Заказчика, осуществляются в рабочее время, определяемое Правилами внутреннего трудового распорядка соответствующих объектов филиалов ПАО «Россети Московский регион», в согласованное с Заказчиком время, на основании допуска к работам, оформляемым Заказчиком. При необходимости, по договоренности с ответственными лицами со стороны Заказчика, может обеспечиваться круглосуточный доступ и доступ в выходные и праздничные дни.</p>
11	Охрана труда и техника безопасности	<p>При выполнении работ необходимо руководствоваться требованиями по охране труда и технике безопасности, изложенными в следующих нормативных документах:</p> <ul style="list-style-type: none"> – Правила по охране труда при эксплуатации электроустановок; – Правила технической эксплуатации электроустановок потребителей; – Положение по особенностям расследования несчастных случаев на производстве в отдельных отраслях и организациях; – Действующей редакции Регламента допуска подрядных и субподрядных организаций для работ на линиях электропередачи, подстанциях и проведения общестроительных и ремонтных работ на объектах ПАО «Россети Московский регион» и допуска командированного персонала для работ в действующих, строящихся, реконструируемых электроустановках ПАО «Россети Московский регион»; – Других соответствующих нормативных документах РФ.

12	Противопожарные мероприятия	<p>Пожарную безопасность обеспечить:</p> <ul style="list-style-type: none"> – разработкой требований по пожарной безопасности на местах установки защитных шкафов и оборудования, использованием существующих на объектах систем пожарной сигнализации; – размещением оборудования в соответствии с ВНТП211-93, что обеспечивает свободный доступ для проведения противопожарных мероприятий в аварийных ситуациях; <p>выбором марок кабелей и проводов в соответствии с назначением и соблюдением норм по току и напряжению.</p>
13	Исходные данные, передаваемые Заказчиком	<p>Основные исходные данные, передаваемые Заказчиком Исполнителю:</p> <ul style="list-style-type: none"> – Перечень объектов с указанием адресов; – Архивная топографическая съемка или генеральный план объекта защиты в редактируемом формате dwg (при наличии); – Архивные материалы инженерно-геологических изысканий (при наличии). <p>Перечень исходных данных уточняется Исполнителем и Заказчиком в процессе проведения работ.</p>
14	Проектирование и согласование документации с Заказчиком	<p>Техническим заданием не предусматриваются работы по выполнению инженерных изысканий на объекте. В случае отсутствия у Заказчика актуальных или архивных версий инженерно-геологических и топографо-геодезических изысканий, исполнитель выполняет работы по проектированию КИТСО, используя в качестве исходных данных и подосновы общедоступные электронные карты местности, данные обмеров, полученные в ходе предпроектного обследования объекта, а также данные специализированных справочников по геологии в районе производства работ. В ходе предпроектного обследования Заказчик оказывает содействие в нанесении на подоснову (план объекта) подземных коммуникаций, расположенных в зоне проектирования КИТСО.</p> <p>Этапы проектирования КИТСО:</p> <p>Исполнитель:</p> <p>Разрабатывает принципиальные технические решения (ПТР). ПТР должны содержать краткое описание функционала системы, а также перечень применяемого специального оборудования КИТСО, типы ограждений, элементов инженерной защиты, с указанием наименования производителей и марок.</p> <p>Заказчик:</p> <p>Рассматривает и согласовывает представленные исполнителем ПТР. Допускается согласование с учетом замечаний, подлежащих устранению на следующих этапах проектирования.</p> <p>Исполнитель:</p> <p>Разрабатывает в соответствии с ГОСТ Р 21.101-2020 рабочую документацию, содержащую рабочие чертежи, планы расположения оборудования, схемы подключений, спецификации оборудования и материалов, ведомости объемов работ. Согласовывает документацию с филиалом ПАО «Россети Московский регион» – «Северные электрические сети» и с исполнительным аппаратом ПАО «Россети Московский регион».</p> <p>Сметную документацию выполнить согласно Методики определения сметной стоимости строительства, реконструкции, капитального ремонта, сноса объектов капитального строительства, работ по сохранению объектов культурного наследия (приказ Минстроя РФ от 04.08.2020 №421/пр в действующей редакции)</p>

	<p>ресурсно-индексным методом с использованием Федеральной сметно-нормативной базы ФСНБ-2022 для объектов Московской области, с применением методик, справочников и сборников включенных в Федеральный реестр сметных нормативов (ФРСН).</p> <p>Представляет Заказчику разработанную документацию в одном экземпляре на электронном носителе, в электронном и программном форматах, и обеспечивает ее сопровождение при согласовании в профильных подразделениях Заказчика.</p> <p>Заказчик:</p> <p>Рассматривает представленную исполнителем рабочую документацию на предмет соответствия техническому заданию и утвержденным ранее ПТР. В случае наличия замечаний однократно оформляет их свод для подготовки Исполнителем ответов и утверждения перечня принятых замечаний для итоговой корректировки документации. Письменно согласовывает итоговую версию рабочей документации и допускает ее в дальнейшее производство работ.</p> <p>Исполнитель:</p> <p>После утверждения электронной версии документации передает ее в установленном порядке в филиал ПАО «Россети Московский регион» - «Северные электрические сети» в следующем составе:</p> <p>Документации передаются заказчику в количестве:</p> <ul style="list-style-type: none"> - бумажная версия – по 2 экземпляра; - электронная версия в формате PDF (цвет, с согласованиями, с разбивкой по томам, каждый том отдельным файлом) – 3 экземпляра на 3-х компакт дисках (в т.ч. 2 экз. – для торгово-закупочных процедур); - электронная версия в системе AutoCAD (*.dwg) и текстовые документы в системе MS Office – 1 экземпляр. <p>Сметная документация передается заказчику в количестве:</p> <ul style="list-style-type: none"> - бумажная версия – 2 экземпляра; - электронная версия в формате PDF – 3 экземпляра на 3-х компакт дисках (в т.ч. 2 экз. – для торгово-закупочных процедур); - электронная редактируемая версия сметной документации: - в формате Smeta.ru (*.sob) – 1 экз.; - в формате АРПС 1.10. (*.apr) – 1 экз.; - в формате MS Office Excel – 1 экз.
--	---

Начальник отдела комплексной и информационной безопасности филиала ПАО «Россети Московский регион» - Северные электрические сети

А.В. Фирстов

СОГЛАСОВАНО

Директор по безопасности - начальник управления безопасности филиала ПАО «Россети Московский регион» - Северные электрические сети

А.И. Бабич