

Об утверждении Требований к оснащению зданий, сооружений, помещений, открытых площадок, расположенных на территории свободной экономической зоны, созданной на территориях Донецкой Народной Республики, Луганской Народной Республики, Запорожской области и Херсонской области, на которой применяется таможенная процедура свободной таможенной зоны, техническими средствами таможенного контроля, инженерными, информационными, телекоммуникационными системами и средствами их обеспечения для целей совершения таможенных операций и проведения таможенного контроля

Приказ · № 556 · от 28.06.2023 · Федеральная таможенная служба · Действует без изменений

ФЕДЕРАЛЬНАЯ ТАМОЖЕННАЯ СЛУЖБА

ПРИКАЗ

МОСКВА

28 июня 2023 г. № 556

Об утверждении Требований к оснащению зданий, сооружений, помещений, открытых площадок, расположенных на территории свободной экономической зоны, созданной на территориях Донецкой Народной Республики, Луганской Народной Республики, Запорожской области и Херсонской области, на которой применяется таможенная процедура свободной таможенной зоны, техническими средствами таможенного контроля, инженерными, информационными, телекоммуникационными системами и средствами их обеспечения для целей совершения таможенных операций и проведения таможенного контроля

Зарегистрирован Минюстом России 30 июня 2023 г.

Регистрационный № 74091

В соответствии с частью 9 статьи 20 Федерального закона от 24 июня 2023 г. № 266-ФЗ "О свободной экономической зоне на территориях Донецкой Народной Республики, Луганской Народной Республики, Запорожской области и Херсонской области" и пунктом 1 Положения о Федеральной таможенной службе, утвержденного постановлением Правительства Российской Федерации от 23 апреля 2021 г. № 636 "Об утверждении Положения о Федеральной таможенной службе, внесении изменений в Положение о Министерстве финансов Российской Федерации и признании утратившими силу некоторых актов и отдельных положений некоторых актов Правительства Российской Федерации", приказываю:

1. Утвердить прилагаемые Требования к оснащению зданий, сооружений, помещений, открытых площадок, расположенных на территории свободной экономической зоны, созданной на территориях Донецкой Народной Республики, Луганской Народной Республики, Запорожской области и Херсонской области, на которой применяется таможенная процедура свободной таможенной зоны, техническими средствами таможенного контроля, инженерными, информационными, телекоммуникационными системами и средствами их обеспечения для целей совершения таможенных операций и проведения таможенного контроля.

2. Настоящий приказ вступает в силу по истечении 30 дней после дня его официального опубликования.

И.о. руководителя

генерал-полковник таможенной службы А.Б.Струков

Приложение

УТВЕРЖДЕНЫ

приказом ФТС России

от 28 июня 2023 г. № 556

Требования к оснащению зданий, сооружений, помещений, открытых площадок, расположенных на территории свободной экономической зоны, созданной на территориях Донецкой Народной Республики, Луганской Народной Республики, Запорожской области и Херсонской области, на которой применяется таможенная процедура свободной таможенной зоны, техническими средствами таможенного контроля, инженерными, информационными, телекоммуникационными системами и средствами их обеспечения для целей совершения таможенных операций и проведения таможенного контроля

1. Технические средства таможенного контроля, инженерные, информационные, телекоммуникационные системы и средства их обеспечения, необходимые для оснащения зданий, сооружений, помещений, открытых площадок 1 (далее - объекты таможенной инфраструктуры), создаются как комплекс информационно-технических средств (далее - КИТС).

1 Часть 9 статьи 20 Федерального закона от 24 июня 2023 г. № 266-ФЗ "О свободной экономической зоне на территориях Донецкой Народной Республики, Луганской Народной Республики, Запорожской области и Херсонской области" (далее - Федеральный закон № 266-ФЗ).

2. В КИТС объекта таможенной инфраструктуры входят следующие элементы:

комплексная система безопасности;

интегрированная структурированная кабельная система;

локальная вычислительная сеть (далее - ЛВС);

система связи;

система защиты информации;

вычислительные компоненты информационно-коммуникационных технологий (далее - ИКТ);

комплекс технических средств таможенного контроля (далее - ТСТК);

система считывания регистрационного номера транспортного средства.

3. Объекты таможенной инфраструктуры обеспечиваются наличием телевидения, системы оповещения о возникновении аварийных ситуаций, устройств и технических средств для создания единой синхронизированной сети точного времени.

4. В целях обеспечения условий для создания и функционирования элементов КИТС на объектах таможенной инфраструктуры должны быть предусмотрены:

помещения, предназначенные для размещения серверного, телекоммуникационного, активного сетевого, коммутационного и кроссового оборудования (далее - серверные и технологические помещения), температурно-влажностный режим в котором определяется исходя из параметров размещаемой аппаратуры и требований по обеспечению информационной безопасности;

система бесперебойного гарантированного электроснабжения;

кабельная (телефонная) канализация, кабельные вводы в здания;

места, обустроенные и оборудованные для размещения и безопасной эксплуатации ТСТК;

система молниезащиты и заземления.

5. Виды технических средств, необходимых для оснащения объектов таможенной инфраструктуры, и

их количество определяются исходя из:

режима работы (сменность) объекта таможенной инфраструктуры;

категории предполагаемых к перемещению (перемещаемых) товаров на (с) территорию(ии) участка участника СЭЗ 2 ;

2 Пункт 4 статьи 2 Федерального закона № 266-ФЗ .

порядка и технологий совершения таможенных операций при ввозе (вывозе) товаров, въезде (выезде) транспортных средств, входе (выходе) физических лиц на (с) территорию(ии) участка участника СЭЗ и проведения таможенного контроля на таком участке 3 .

3 Пункт 12 статьи 20 Федерального закона № 266-ФЗ .

6. Состав, тип оборудования, входящего в КИТС, определяются для конкретного объекта таможенной инфраструктуры с учетом:

назначения и категории объекта таможенной инфраструктуры по пожарной и взрывопожарной опасности (для производственных объектов), его месторасположения;

технических возможностей комплекса технических средств;

места установки оборудования;

объема, площади, протяженности и конфигурации объекта таможенной инфраструктуры;

климатических условий местности нахождения территории участка участника СЭЗ;

необходимости обеспечения электромагнитной совместимости оборудования, входящего в состав КИТС, а также обеспечения защиты от действия вибрации, механических ударов;

необходимости обеспечения экологических, эргономических и медико-биологических условий для работы персонала участника СЭЗ, эксплуатирующего комплекс технических средств.

7. Требованиями по оснащению являются:

7.1 Комплексная система безопасности (далее - КСБ).

7.1.1. КСБ предназначена для обеспечения:

охраны помещений объекта таможенной инфраструктуры, оборудования и других материальных ценностей, находящихся на объекте таможенной инфраструктуры;

контрольно-пропускного и внутриобъектового режимов;

безопасности работы должностных лиц таможенных органов;

возможности обнаружения запрещенных к вносу (ввозу) на территорию участка участника СЭЗ предметов;

контроля процесса пропуска физических лиц и транспортных средств на территорию участка участника СЭЗ;

защиты информации, составляющей государственную или иную охраняемую законом тайну, от утечки по техническим каналам и несанкционированного доступа.

7.1.2. КСБ объекта таможенной инфраструктуры включает в себя следующие системы:

автоматизированную систему охраны (далее - АСО);

систему оперативного теленаблюдения;

систему распознавания государственных регистрационных знаков транспортных средств.

7.1.3. Состав применяемого оборудования КСБ определяется с учетом:

состояния антитеррористической защищенности объекта таможенной инфраструктуры и организации его охраны;

объема, площади, протяженности и конфигурации объекта таможенной инфраструктуры;

освещенности объекта таможенной инфраструктуры в различное время суток.

7.1.4. АСО включает в себя следующие взаимосвязанные подсистемы:

охранную сигнализацию;

пожарную сигнализацию;
управление доступом;
охранное теленаблюдения;
сбор и обработка информации.

7.1.5. Подсистема охранной сигнализации должна обеспечивать:

постановку под охрану и снятие с охраны помещений или групп помещений;
обнаружение и фиксирование фактов открывания дверей и окон, разбития стекол, наличия движения в выделенных зонах и помещениях, сданных под охрану;
обнаружение и фиксирование фактов несанкционированного проникновения на объект таможенной инфраструктуры или ухода с него путем повреждения сигнального ограждения;
фиксирование срабатывания сигнализации на территории объекта таможенной инфраструктуры;
формирование сигналов для подсистемы управления доступом;
формирование сигналов для подсистемы охранного теленаблюдения и включение видеоизображений;
фиксирование информации обо всех принятых сигналах тревоги в базе данных с указанием даты, времени, наименования и (или) адреса в пределах места нахождения объекта таможенной инфраструктуры и ведение протокола такой фиксации.

Подсистема охранной сигнализации включает в себя сигнализационные датчики и средства обнаружения, обеспечивающие охрану помещений, территорий и открытых площадок.

Сигнализационные датчики и средства обнаружения устанавливаются:

на дверях, окнах, перегородках охраняемых помещений, сейфах;
на дверцах шкафов с аппаратурой радиационного контроля;
на устройствах наведения телевизионных камер;
по периметру территории объекта таможенной инфраструктуры.

Подсистема охранной сигнализации периметра территории таможенной инфраструктуры должна строиться на базе периметрального сигнализационного заградительного ограждения, оборудованного сигнализационными средствами обнаружения.

7.1.6. Подсистема пожарной сигнализации должна обеспечивать:

адресное обнаружение и фиксирование фактов появления очагов загорания, задымленности, повышения температуры;
формирование сигналов для подсистемы управления доступом;
формирование сигналов для подсистемы охранного теленаблюдения по приоритетному включению видеоизображений тревожной зоны и прилегающих зон;
формирование сигналов для устройств автоматического пожаротушения, дымоудаления;
фиксирование информации обо всех принятых сигналах тревоги в базе данных с указанием даты, времени, адреса и ведение протокола работы.

7.1.7. Подсистема управления доступом должна обеспечивать:

идентификацию персонала предприятия участника СЭЗ и иных лиц, осуществляющих деятельность на территории участка участника СЭЗ и управление доступом на территорию участка участника СЭЗ;
управление автоматическими пропускными устройствами: с центрального пульта управления, с местного пульта у пропускного устройства;
формирование сигналов для подсистемы охранной сигнализации при возникновении нештатных ситуаций, в том числе попытках взлома в подсистеме управления доступом;
формирование сигналов для подсистемы охранного теленаблюдения по приоритетному включению видеоизображений сигнализации при возникновении нештатных ситуаций попытках взлома в подсистеме управления доступом;
фиксирование информации обо всех событиях в базе данных с указанием даты, времени,

наименования и места нахождения объекта таможенной инфраструктуры (при наличии) и ведение протокола фиксации такой информации.

Подсистема управления доступом включает:

считыватели и исполнительные устройства контроля доступа;

видеодомофоны;

электромеханические замки;

устройства электронные для хранения и учета ключей;

смарт-карты должностных лиц таможенного органа и персонала.

7.1.8. Подсистема охранного теленаблюдения должна обеспечивать: постоянное наблюдение за оперативной обстановкой на объекте таможенной инфраструктуры;

наблюдение за объектами таможенной инфраструктуры в любое время суток;

одновременный вывод изображений от подключенных камер в окна произвольного размера и расположения на экране монитора;

наведение телевизионных камер по тревожным сигналам подсистемы охранной сигнализации или адаптивному программному детектору движения;

отображение и автоматическую запись видеоинформации по сигналам от подсистем охранной и пожарной сигнализации, подсистемы управления доступом;

распознавание ситуаций с использованием искусственного интеллекта (обнаружение оставленного предмета, остановка объекта в заданном секторе больше заданного времени, детектирование совокупного перемещения объектов в соответствии с направлением заданного вектора) с выдачей тревожной индикации на мониторах;

создание архива видеозаписей.

Подсистема охранного теленаблюдения включает:

телевизионные камеры черно-белого или цветного изображения;

устройства управления режимом отображения;

устройства отображения (обеспечивает оперативный или постоянный просмотр текущей видеоинформации в режиме произвольного полиэкрана от одной или нескольких телевизионных камер или оперативный просмотр видеоархива подсистемы охранного телевидения по критериям: дата, время, номер телевизионной камеры, событие);

устройства регистрации, обеспечивающие запись изображений;

устройства передачи и распределения видеосигналов (обеспечивают передачу видеосигналов от удаленных телевизионных камер);

компьютерное оборудование (видеорегистраторы, автоматизированное рабочее место (далее - АРМ) и сервер управления);

сетевое оборудование.

Подсистема охранного телевидения строиться на базе цифровых систем видеонаблюдения и регистрации.

Управление вариообъективами и поворотными устройствами телевизионных камер должно осуществляться дистанционно.

7.1.9. Система оперативного теленаблюдения обеспечивает:

дистанционное визуальное наблюдение за оперативной обстановкой на объекте таможенной инфраструктуры;

снижение количества конфликтных ситуаций при совершении таможенных операций и проведении таможенного контроля;

отображение и запись видеоинформации с аудиоинформацией;

создание архива аудио- и видеозаписей;

копирование или передачу по каналам связи архива аудио-записей и видеозаписей в закрытый серверный ресурс регионального таможенного управления.

Система оперативного теленаблюдения включает:

телевизионные камеры цветного или черно-белого изображения;

устройства получения аудиоинформации;

устройства управления режимом отображения;

устройства отображения;

устройства регистрации;

устройства передачи телевизионных и аудиосигналов;

компьютерное оборудование (видеорегистраторы, АРМ и сервер управления);

сетевое оборудование (активное - коммутаторы - и пассивное - кабели, патч-панели и коннекторы).

Для исключения несанкционированного доступа устройства регистрации должны быть оснащены комплектом аппаратно-программных средств аутентификации пользователя.

Устройства передачи телевизионных и аудиосигналов должны обеспечивать передачу видеосигналов и аудиосигналов от удаленных камер и микрофонов к местам наблюдения и регистрации, а также при технической возможности каналов связи передачу видеоинформации и аудиоинформации с устройств регистрации в таможенный орган в режиме реального времени (с выполнением требований по информационной безопасности) по запросу.

Программное обеспечение системы должно предусматривать:

возможность управления внешними устройствами;

возможность записи телевизионной и аудиоинформации с указанием даты, времени, номера телевизионной камеры;

автоматическое диагностирование работоспособности подсистемы с указанием неисправных блоков;

протоколирование событий в системе: действия оператора и системного администратора,

функционирование оборудования, контроль изменения настроек системы, контроль установки дополнительных программ.

Оборудование системы (кроме периферийного) должно быть установлено в специальном помещении, исключающем доступ в него посторонних лиц.

Телевизионные камеры и устройства получения аудиоинформации должны устанавливаться открыто.

7.1.10. Система распознавания государственных регистрационных знаков транспортного средства должна обеспечивать:

фиксирование государственного регистрационного номера транспортного средства в любых погодных-климатических условиях и в любое время суток;

идентификацию транспортных средств по государственному регистрационному номеру транспортного средства, а также по его типу и грузоподъемности и внесение идентифицируемых параметров в базу данных.

Система распознавания государственных государственных знаков транспортных средств включает:

телевизионные камеры наружного исполнения;

специализированный контроллер на базе персонального компьютера;

фрейм-граббер;

осветитель видимого или инфракрасного диапазона;

коммутационные устройства;

специализированное программное обеспечение.

Система должна обеспечивать вероятность правильного распознавания регистрационного номерного знака в простых и сложных метеоусловиях при естественном или искусственном освещении на уровне не менее 90% при допустимых углах несовместного отклонения линии визирования от нормали к номеру:

в горизонтальной плоскости: 35° - 40°;

в вертикальной плоскости: 30° - 35°.

7.2. Структурная кабельная система (далее - СКС).

СКС включает в себя следующие подсистемы в зависимости от объекта таможенной инфраструктуры:

подсистему рабочих мест (точки подключения абонентского оборудования ЛВС и телефонной сети к СКС);

горизонтальную подсистему (отрезки кабельных линий, соединяющих информационные разъемы розеток рабочих мест с портами панелей переключений, входящих в состав этажного распределительного узла);

подсистему внутренних магистралей объекта таможенной инфраструктуры (отрезки кабельных линий, соединяющие центральный распределительный узел с этажными распределительными узлами);

этажные распределительные узлы объекта таможенной инфраструктуры;

центральный распределительный узел объекта таможенной инфраструктуры;

подсистему внешних магистралей объекта таможенной инфраструктуры (отрезки кабельных линий, соединяющие центральные распределительные узлы зданий, объединенных единой СКС);

узлы ввода (совокупность оборудования, предназначенного для обеспечения стыковки кабелей подсистемы внешних магистралей с внутренними кабельными сетями здания, являющегося объектом таможенной инфраструктуры).

Состав подсистем СКС определяется для каждого конкретного объекта таможенной инфраструктуры.

7.3. ЛВС.

ЛВС должна обеспечивать возможность объединения вычислительных средств объекта таможенной инфраструктуры и подключения автоматизированных рабочих мест должностных лиц таможенного органа к централизованным вычислительным ресурсам на основе современных и перспективных сетевых технологий.

7.4. Система связи должна обеспечивать:

включение в сеть связи общего пользования в соответствии с техническим заданием и исходными данными;

включение в ведомственную интегрированную телекоммуникационную сеть (ВИТС) ФТС России по основному каналу передачи данных с пропускной способностью не менее 2048 Кбит/с;

включение в ВИТС ФТС России по резервному каналу передачи данных с пропускной способностью не менее 2048 Кбит/с;

автоматическое переключение с основного на резервный канал передачи данных в случае, если основной канал передачи данных перестает осуществлять передачу трафика с заданным уровнем качества;

подключение выделенных рабочих мест таможенного органа к сети Интернет со скоростью доступа не менее 1 Мбит/с с учетом соблюдения требований по обеспечению информационной безопасности при использовании информационно-телекоммуникационных сетей международного информационного обмена (количество выделенных рабочих мест определяется в техническом задании).

7.4.1. Система связи обеспечивает функционирование аналоговых и цифровых телефонных аппаратов.

7.4.2. Оборудование подсистем передачи данных и ведомственной телефонной связи должно поддерживать сетевые протоколы и технологии, используемые в ВИТС ФТС России и сети связи общего пользования.

7.4.3. Аппаратам факсимильной связи должны быть назначены номера ведомственной телефонной связи таможенных органов с обеспечением включения в ВИТС ФТС России, а также, (при необходимости), номера телефонной сети связи общего пользования с выходом на эту сеть через

учрежденческо-производственную автоматическую телефонную станцию (УПАТС) (голосовой шлюз).

7.4.4. Абонентская установка телеграфной связи должна быть включена в сеть АТ-50/Телекс в соответствии с техническими условиями оператора связи (в случае обоснованной потребности).

7.4.5. Телекоммуникационное оборудование, активное сетевое оборудование, средства каналообразования, документальной связи и УПАТС (голосовой шлюз) должны быть обеспечены источниками бесперебойного электропитания.

7.5. Система защиты информации.

Система обеспечения безопасности информации (далее - СОБИ) включает следующие подсистемы:

межсетевого экранирования;

криптографической защиты информации, не составляющей государственную тайну, передаваемой по магистральным каналам ВИТС;

защиты информации от несанкционированного доступа;

антивирусной защиты информации;

обнаружения компьютерных атак;

анализа защищенности;

мониторинга и управления;

выявления каналов утечки информации и контроля информационных потоков;

криптографической защиты информации и электронной подписи;

идентификации и аутентификации.

7.6. Вычислительные компоненты ИКТ.

7.6.1. ИКТ включает следующие подсистемы:

вычислительной инфраструктуры;

хранения данных;

виртуализации;

инфраструктурные системы (при наличии);

системы авторизации, осуществляющие поддержку сервисов аутентификации и управления правами пользователей;

иные подсистемы вычислительных компонентов ИКТ.

7.6.2. Подсистему вычислительной инфраструктуры составляют средства вычислительной техники, обеспечивающие функционирование подсистем виртуализации и сервисов.

7.6.3. Подсистему хранения данных составляют средства, обеспечивающие систематизацию, накопление и хранение информации.

7.6.4. Подсистему виртуализации составляют виртуальные вычислительные среды, в том числе распределенные виртуальные среды хранения и обработки.

7.7. ТСТК.

7.7.1. Состав комплекса ТСТК формируется в соответствии с Перечнем технических средств таможенного контроля, используемых при проведении таможенного контроля, утвержденным приказом Министерства финансов Российской Федерации от 1 марта 2019 г. № 33н "Об утверждении перечня технических средств таможенного контроля, используемых при проведении таможенного контроля" 4 .

4 Зарегистрирован Минюстом России 13 мая 2019 г., регистрационный № 54604.

7.7.2. ТСТК, являющиеся средствами измерений, должны соответствовать требованиям, установленным Федеральным законом от 26 июня 2008 г. № 102-ФЗ "Об обеспечении единства измерений".

7.8. Требования к серверным и технологическим помещениям.

7.8.1. Серверные и технологические помещения предназначены для размещения телекоммуникационного и вычислительного оборудования, обеспечивающие функционирование

компонентов ЕАИС таможенных органов, автоматизированной системы внешнего доступа таможенных органов и иных вспомогательных систем таможенных органов, в части их комплексного оснащения сетями инженерно-технического обеспечения и оборудованием, обеспечивающими эксплуатацию серверных и технологических помещений как специально оборудованных помещений (далее - инженерные системы).

7.8.2. В серверном помещении (далее - серверная) располагаются вычислительные компоненты ИКТ и (или) телекоммуникационного (активного сетевого) оборудования (перечень оборудования определяется для каждого серверного помещения отдельно).

7.8.3. К технологическими помещениям относятся:

помещения телекоммуникационных узлов, не относящиеся к серверным помещениям в соответствии с подпунктом 15.5 настоящих Требований;

аппаратные;

распределительные узлы СКС;

кроссовые.

7.8.4. Суммарное энергопотребление всего ИКТ оборудования, эксплуатируемого в серверном помещении, составляет не менее 5 кВт.

7.8.5. Серверная и технологическое помещение должны обладать площадью как для беспрепятственной установки, эксплуатации и технического обслуживания основного оборудования, так и для размещения средств поддержки вычислительной техники, носителей данных и обслуживающего персонала.

7.8.6. Серверные и технологические помещения оборудуются системами и средствами противопожарной защиты в соответствии с требованиями законодательства Российской Федерации о пожарной безопасности.

7.8.7. Серверные должны быть оборудованы системой обеспечения микроклимата.

Система микроклимата должна обеспечивать всесезонное поддержание температурного режима и должна быть рассчитана на круглосуточную непрерывную работу.

7.8.8. Доступ в помещения серверных должен быть организован ограниченному кругу лиц.

Санкционированный доступ должен быть обеспечен инженерно-техническими средствами защиты и техническими средствами охраны, в том числе системами охранного видеонаблюдения и системами контроля и управления доступом с применением различных идентификаторов (для доступа в наиболее ответственные помещения возможно применение комбинации из нескольких различных параметров идентификации, например проксимити карта и какой-либо биометрический параметр).

7.8.9. В серверной рекомендуется установить камеры охранного видеонаблюдения, подключенные к имеющейся либо отдельной системе охранного видеонаблюдения с возможностью просмотра текущей видеоинформации и видеoarхива.

7.8.10. Все оборудование в серверной размещается в открытых стойках или закрытых шкафах, двери и боковые панели которых должны быть установлены и закреплены на своих местах или открытых стойках.

Количество стоек (шкафов) определяется исходя из имеющегося оборудования, его типа и размеров, способов монтажа и требований производителя.

7.8.11. Распределение оборудования по стойкам (шкафам) осуществляется с учетом совместимости (возможного взаимного влияния), оптимального распределения потребляемой мощности (а значит, и тепловыделения), оптимальности коммуникаций, габаритов и массы оборудования.

7.8.12. В закрытых стойках могут применяться дополнительные вентиляторы, встраиваемые системы охлаждения, модули отвода горячего воздуха.

7.9. Требования к технологическим помещениям.

7.9.1. В помещениях должно быть обеспечено поддержание оптимального температурного режима работы оборудования в диапазоне 18°C - 25°C.

7.9.2. Система бесперебойного гарантированного электроснабжения (далее - СБГЭ) должна обеспечивать работу КИТС, при:

длительном пропадании напряжения питающей сети;
кратковременном падении (провале) напряжения питающей сети;
импульсных и кратковременных перенапряжениях.

В СБГЭ должно быть предусмотрено наличие системы мониторинга и автоматического управления электропитанием.

СБГЭ должна обеспечивать выдачу команды для отключения серверов и рабочих станций с принудительным закрытием работающих программных приложений и сохранением находящихся в работе файлов при разряде аккумуляторных батарей.

Помещения, в которых размещаются СБГЭ, оборудуются инженерными средствами защиты и техническими средствами охраны, обеспечивающими защиту указанных помещений от несанкционированного проникновения посторонних лиц.

7.9.3. СБГЭ включает в себя следующие основные элементы:

источник бесперебойного питания (далее - ИБП), обеспечивающий электроснабжение потребителей электроэнергии, относящихся к первой категории, при кратковременном выходе параметров питающей сети за допустимые пределы, а также энергоснабжение потребителей электроэнергии с повышенными требованиями к качеству электрической энергии;

автономный источник электроэнергии - дизельную электростанцию (далее - ДЭС) (дизель-генератор), предназначенный для обеспечения электроснабжения потребителей электроэнергии при длительном пропадании напряжения питающей сети, а также подзарядки аккумуляторных батарей ИБП при отсутствии напряжения в основной питающей сети;

выделенную электrorаспределительную сеть (ВЭРС);

средства автоматизации - автоматы ввода резерва (АВР), обеспечивающие автоматизацию переключения нагрузки с фидера, имеющего неудовлетворительные параметры качества электроэнергии (предельные минимальные и максимальные значения напряжения и частоты), на исправный фидер, а также используемые для автоматизации запуска ДЭС;

устройства ограничения (подавления) высоковольтных импульсов, возникающих при грозовых разрядах или коммутации некоторых видов нагрузки.

7.9.4. Состав применяемого оборудования СБГЭ определяют по результатам проведения проектно-изыскательских работ и получения технических условий от электроснабжающих организаций.

7.9.5. ИБП в системе бесперебойного питания должен обеспечивать:

электроснабжение критической нагрузки на время (не менее 15 минут), необходимое для корректного свертывания работы средств вычислительной техники, активного сетевого оборудования локальной вычислительной сети или запуска ДЭС, при нарушениях в подаче электроэнергии сетями внешнего электроснабжения;

повышение качества электрической энергии, получаемой от питающей сети и поступающей к критической нагрузке;

создание гальванической развязки "электрическая сеть - критическая нагрузка" для решения вопросов электрической безопасности.