МИНИСТЕРСТВО СПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

(МИНСПОРТ РОССИИ)

МИНИСТЕРСТВО СПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
г. Москва
Регистрационный № 70646
от "21" октября 2022.

ПРИКАЗ

«22» августа 2022 г. № 676

Об утверждении требований к информационным системам контроля доступа

В соответствии с абзацем четвертым пунктом 5 Правил обеспечения безопасности при проведении официальных спортивных соревнований, утвержденных постановлением Правительства Российской Федерации от 18 апреля 2014 г. № 353 (Собрание законодательства Российской Федерации, 2014, № 18, ст. 2194; 2022, № 21, ст. 3467)[1], п р и к а з ы в а ю:

1. Утвердить прилагаемые требования к информационным системам контроля доступа.

2. Контроль за исполнением настоящего приказа возложить на первого заместителя Министра спорта Российской Федерации А.Р. Кадырова.

Министр О.В. Матыцин

[1] Пункт 1 Положения о Министерстве спорта Российской Федерации, утвержденного постановлением Правительства Российской Федерации от 19.06.2012 № 607 (Собрание законодательства Российской Федерации, 2012, № 26, ст. 3525).

УТВЕРЖДЕНЫ
приказом Министерства спорта
Российской Федерации
от «22» августа 2022 г. № 676

Требования
к информационным системам контроля доступа

I. Общие положения

1. Настоящий документ определяет требования к информационным системам контроля доступа объекта спорта (далее – СКД), применяемым в целях аутентификации зрителей, участников официальных спортивных соревнований, определенных решением Правительства Российской Федерации в соответствии с частью 2.2 статьи 20 Федерального закона от 4 декабря 2007 г. № 329-ФЗ «О физической культуре и спорте в Российской Федерации» (Собрание законодательства Российской Федерации, 2007, № 50, ст. 6242; 2022, № 1, ст. 31) (далее – соревнования), а также иных лиц, задействованных в проведении соревнований (далее – посетители).

2. СКД должна включать следующее оборудование:

на пешеходных контрольно-пропускных пунктах (далее – КПП): устройства преграждающие управляемые далее – УПУ) в виде турникетов и (или) моторизированных калиток, имеющих электромеханический привод ее двери для доступа маломобильных групп населения, испытывающих затруднения при самостоятельном передвижении (далее – МГН), оборудованные стационарными считывающими устройствами СКД и мониторными устройствами СКД для отображения фотографии, частично маскированных данных фамильно-именной группы и возраста посетителей, а также статуса доступа «разрешен» («запрещен»);

на транспортных КПП: мобильные считывающие устройства СКД на полосах въезда (выезда) транспортного средства.

Необходимое количество УПУ на КПП рассчитывается по формуле $a \times b \div c \div d$, где:

a – вместимость объекта спорта;

b = 0,5 – коэффициент увеличения пиковой нагрузки, равной 50% от вместимости объекта спорта;

c = 450 – пропускная способность УПУ СКД (450 человек/час);

d = 0,5 – коэффициент, отражающий период затрачиваемого времени на проход на объект спорта (30 минут).

Пропускная способность КПП, оборудованного СКД, обеспечивается количеством точек пропуска (стационарных металлообнаружителей) в зонах осмотра посетителей, рассчитываемым по формуле $a \times b \div c \div d$, где:

a – вместимость объекта спорта;

b = 0,7 – коэффициент увеличения пиковой нагрузки, равной 70% от вместимости объекта спорта;

c = 300 – пропускная способность стационарного металлообнаружителя при двух осматривающих (300 человек/час);

d = 0,5 – коэффициент, отражающий период затрачиваемого времени на проход на объект спорта (30 минут).

3. С использованием СКД должна обеспечиваться фиксация фактов входа (выхода) посетителей с территории объекта спорта через его ограждение периметра места проведения соревнования (далее – периметр безопасности) :

в отношении зрителей – со времени начала пропуска зрителей на территорию объекта спорта и до официального времени окончания соревнования в соответствии с положением (регламентом) соревнования:

через пешеходные КПП периметра безопасности объекта спорта путем считывания идентификатора электронного документа, предоставляющего право доступа на соревнование, сформированного информационной системой идентификации болельщиков (далее – СИБ) на основании действующей персонифицированной карты для посещения спортивного соревнования (далее – ПК) и приобретенного билета (абонемента) или иного документа, дающего право на посещение соревнования (далее – электронный документ, предоставляющий право доступа на соревнование), в виде QR-кода на УПУ СКД, работающих на выход;

через транспортные КПП путем считывания идентификатора электронного документа, предоставляющего право доступа на соревнование, в виде QR-кода, мобильными считывающими устройствами СКД;

в отношении участников соревнования, иных лиц, задействованных в проведении соревнования (далее – аккредитованные посетители), – в течение всего дня проведения соревнования независимо от времени начала и окончания соревнования:

через пешеходные КПП путем считывания идентификатора электронного документа, предоставляющего право доступа на соревнование, в виде QR-кода на УПУ СКД, используемых для входа и выхода аккредитованных посетителей;

через транспортные КПП в салоне транспортного средства путем считывания идентификатора электронного документа, предоставляющего право доступа на соревнование, в виде QR-кода мобильными считывающими устройствами СКД.

4. Линия контроля прав доступа на пешеходные и транспортные КПП периметра безопасности объекта спорта должна располагаться перед линией осмотра посетителей.

II. Требования к структуре и архитектуре построения СКД

5. СКД должна являться частью информационной и телекоммуникационной инфраструктуры объекта спорта.

6. СКД должна представлять собой автоматизированную информационную систему в защищенном исполнении и иметь аттестат соответствия требованиям по защите информации, выдаваемый в соответствии с пунктом 22 Порядка

организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утвержденного приказом Федеральной службы по техническому и экспортному контролю от 29 апреля 2021 г. № 77[1], иметь оценку эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных согласно пункту 6 Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21[2], с изменениями, внесенными приказами ФСТЭК России от 23 марта 2017 г. № 49[3], от 14 мая 2020 г. № 68 (далее – приказ ФСТЭК № 21)[4].

7. Функционирование СКД должно осуществляться под управлением ее объектового сервера.

8. Топология информационной сети должна быть радиально-узловой, в которой основным узлом является объектовый сервер СКД.

9. СКД должна иметь иерархическую структуру:

верхний уровень иерархической структуры СКД должен представлять собой центральное устройство управления (объектовый сервер) и автоматизированные рабочие места (далее – АРМ) для конфигурирования, мониторинга состояния технических средств, формирования отчетов;

нижний уровень иерархической структуры СКД должен представлять собой УПУ, стационарные считыватели, мониторные устройства, мобильные считывающие устройства.

10. В соответствии с пунктом 4.2.2 ГОСТ Р 51241-2008 «Национальный стандарт Российской Федерации. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний», утвержденного приказом Ростехрегулирования от 17 декабря 2008 г. № 430-ст (М.: Стандартинформ, 2009), способ управления доступом должен быть универсальным (сетевым). Средства управления должны объединяться в единую систему по локальной вычислительной сети (далее – ЛВС).

11. СКД должна функционировать на базе физически выделенной ЛВС.

12. ЛВС для нужд СКД должна включать в свой состав следующие подсистемы:

проводная ЛВС;

беспроводная ЛВС;

пограничный сегмент взаимодействия с внешними сетями.

13. Выделенная проводная ЛВС для нужд СКД должна строиться на базе иерархической архитектуры, состоящей из уровня доступа, уровня агрегации и уровня ядра. Пропускная способность коммутационного оборудования ЛВС должна обеспечивать стабильную работу системы.

---

[1] Зарегистрирован Минюстом России 10 августа 2021 г., регистрационный № 64589.
[2] Зарегистрирован Минюстом России 14 мая 2013 г., регистрационный № 28375.
[3] Зарегистрирован Минюстом России 25 апреля 2017 г., регистрационный № 46487.
[4] Зарегистрирован Минюстом России 8 июля 2020 г., регистрационный № 58877.

14. Выделенная беспроводная ЛВС для нужд СКД должна строиться с применением универсальных точек беспроводного доступа, поддерживающих режим работы в стандартном частотном диапазоне сетей Wi-Fi.

III. Требования к функциональным характеристикам СКД

15. СКД должна обеспечивать возможность организации раздельного доступа зрителей и аккредитованных посетителей с соответствующим разграничением прав доступа через разные точки пропуска КПП.

16. СКД должна обеспечивать возможность разграничения прав доступа зрителей через разные КПП, соответствующие зрительским секторам.

17. СКД должна обеспечивать следующий алгоритм доступа посетителей:

считывание идентификатора электронного документа, предоставляющего право доступа на соревнование, в виде QR-кода на стационарных считывателях УПУ СКД, мобильных считывающих устройствах СКД;

автоматический контроль действительности электронного документа, предоставляющего право доступа на соревнование, и наличия прав доступа;

подача управляющей команды на УПУ;

отображение на экране мониторного устройства СКД и дисплее мобильного считывающего устройства СКД фотографии, частично маскированных данных фамильно-именной группы и возраста посетителя, на которого оформлен предъявленный электронный документ, предоставляющий право доступа на соревнование, а также статуса доступа «разрешен» («запрещен»);

визуальное сличение контролером-распорядителем идентичности фотографии, отображенной на мониторе СКД или дисплее мобильного считывающего устройства СКД, с лицом посетителя, предъявившего электронный документ, предоставляющий право доступа на соревнование.

18. При доступе на объект спорта посетителя, не достигшего возраста 14 лет, СКД должно обеспечиваться дополнительное отображение на мониторном устройстве и дисплее мобильного считывающего устройства цветовой индикации для оповещения контролера-распорядителя о факте его прохода в место проведения соревнования.

19. СКД должна обеспечивать:

автоматический запрет прохода по одному электронному документу, предоставляющему право доступа на соревнование, более одного человека;

возможность использования электронного документа, предоставляющего право доступа на соревнование, для повторного входа при условии его считывания на стационарном считывателе СКД УПУ, работающего на выход или на мобильном считывающем устройстве СКД, при выходе посетителя с территории объекта спорта через его периметр безопасности;

возможность применения усиленной квалифицированной электронной подписи в автоматическом режиме при работе с электронными документами, предоставляющими право доступа на соревнование, и при осуществлении информационного взаимодействия с СИБ;

сбор, хранение и использование для доступа информации о выпущенных электронных документах, предоставляющих право доступа на соревнование, и их владельцах (включая фотографию, год рождения и частично маскированные данные фамильно-именной группы посетителя);

работу в автономном (децентрализованном) режиме в отсутствие связи с сервером СИБ;

ведение персонифицированного архива всех событий доступа (вход, выход, отказы от прохода, попытки проходов), изменений состояния и режимов работы ее технических средств, действий (команд) операторов;

передачу событий доступа, регистрируемых в ее архиве, в СИБ в режиме реального времени;

мониторинг состояния всех ее составных частей;

защищенный информационный обмен с СИБ в режиме реального времени по единому протоколу оператора СИБ, для получения информации о сформированных электронных документах, предоставляющих право доступа на соревнование, и их владельцах (включая фотографию, год рождения и частично маскированные данные фамильно-именной группы), а также для передачи из СКД в СИБ полного архива событий доступа.

Для обеспечения конфиденциальности при информационном обмене между СКД и СИБ должны применяться сертифицированные средства криптографической защиты информации. Класс средства криптографической защиты информации (далее – СКЗИ) определяется в соответствии с составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности, утверждённых приказом ФСБ России от 10 июля 2014 г. № 378 (зарегистрирован Минюстом России 18 августа 2014 г., регистрационный № 33620).

20. В день, следующий за днем окончания соревнования, в СКД должна удаляться информация, полученная из СИБ до дня и в день проведения соревнования, а также архив событий доступа, сформированный СКД в день проведения соревнования (при условии полной передачи архива событий доступа в СИБ).

21. Технические решения всех составных частей СКД должны исключать возможность:

записи на любой съемный (внешний) машинный носитель информации, полученной из СИБ;

любых изменений информации, полученной из СИБ, а также информации, содержащейся в архиве событий доступа и в архиве изменения состояния, режимов работы технических средств СКД и действий (команд) операторов.

22. При отключении основного электропитания СКД должна обеспечивать автоматический переход и работу от встроенных источников бесперебойного электропитания в течение не менее 30 минут.

23. Критически важные для работоспособности компоненты СКД (в том числе, серверное оборудование, оборудование и линии связи, передачи и защиты информации) должны иметь системы резервирования и дублирования и обеспечивать автоматический переход на резерв при отказе основного оборудования без сбоев в работе СКД и с сохранением всех происходящих событий, подлежащих фиксированию в ее архиве.

IV. Требования к типовому составу СКД

24. В состав СКД должно входить следующее основное оборудование:

объектовый сервер СКД;

АРМ технической поддержки СКД;

оборудование мест для осуществления контроля посетителей и транспортных средств (далее – точка доступа);

оборудование связи и передачи информации;

оборудование защиты информации;

запасные части и принадлежности к СКД.

25. СКД должна включать в свой состав полный комплект эксплуатационной и другой организационно-технической документации, необходимой для технической поддержки и обеспечения бесперебойной работы СКД, ее составных частей и информационного обмена с СИБ.

26. Турникеты СКД должны функционировать на вход и на выход или только на вход.

27. К точкам доступа транспортного КПП периметра безопасности объекта спорта должны относиться мобильные точки доступа на полосах въезда (выезда) транспортных средств на основе мобильных считывающих устройств СКД.

28. Средства СКД должны обеспечивать конфигурирование пешеходных точек доступа для разграничения доступа зрителей и аккредитованных посетителей, а также для разграничения доступа зрителей через КПП для прохода в секторы активной поддержки команд.

29. Оборудование СКД пешеходной точки доступа на основе турникета должно включать:

УПУ (турникет);

стационарный считыватель идентификатора документа, предоставляющего право доступа на соревнование, в виде QR-кода, объединенный с элементами отображения информации (дисплеем) о процессе доступа и установленный для регистрации входа;

стационарный считыватель идентификатора документа, предоставляющего право доступа на соревнование, в виде QR-кода, объединенный с элементами отображения информации (дисплеем) о процессе доступа и установленный для регистрации выхода (только для точки доступа, функционирующей на вход и на выход);

контроллер доступа (допускается конструктивное объединение с УПУ или считывателями);

мониторное устройство для отображения фотографии, частично маскированных данных фамильно-именной группы и возраста владельца предъявленного электронного документа, предоставляющего право доступа на соревнование, а также статуса доступа «разрешен» («запрещен»).

30. Оборудование СКД пешеходной точки доступа на основе моторизованной калитки для МГН должно включать:

УПУ (моторизованная калитка);

стационарный считыватель идентификатора документа, предоставляющий право доступа на соревнование, в виде QR-кода, объединенный с элементами отображения информации (дисплеем) о процессе доступа и установленный для регистрации входа;

стационарный считыватель идентификатора документа, предоставляющего право доступа на соревнование, в виде QR-кода, объединенный с элементами отображения информации (дисплеем) о процессе доступа и установленный для регистрации выхода (только для точки доступа, функционирующей на вход и на выход);

контроллер доступа (допускается конструктивное объединение с УПУ или считывателями);

мониторное устройство для отображения фотографии, частично маскированных данных фамильно-именной группы и возраста владельца предъявленного электронного документа, предоставляющего право доступа на соревнование, а также статуса доступа «разрешен» («запрещен»).

31. Оборудование СКД мобильной точки доступа должно включать:

мобильное считывающее устройство для считывания идентификатора электронного документа, предоставляющего право доступа на соревнование, содержащее дисплей для отображения информации о статусе доступа «разрешен» («запрещен»), фотографии и частично маскированных данных фамильно-именной группы и возраста владельца предъявленного электронного документа, предоставляющего право доступа на соревнование.

точка беспроводного доступа в ЛВС.

V. Требования к типовому оборудованию СКД

32. УПУ (турникеты, моторизованные калитки для МГН) СКД пешеходных КПП периметра безопасности объекта спорта должны иметь сервопривод (доводчик) ротора.

33. УПУ (турникеты, моторизованные калитки для МГН) СКД должны иметь возможность механической разблокировки.

34. Конструктивные характеристики моторизованных калиток для МГН должны обеспечивать возможность доступа маломобильных посетителей, в том числе на креслах-колясках.

35. Стационарные считывающие устройства СКД должны обеспечивать вывод на встроенный дисплей (в случае технической возможности) графической информации о текущем режиме доступа и другой информации

для помощи посетителям при прохождении ими процедуры доступа либо предусматривать другой способ индикации текущего режима доступа.

36. Мониторные устройства СКД должны обеспечивать отображение фотографии, частично маскированных данных фамильно-именной группы и возраста владельца предъявленного электронного документа, предоставляющего право доступа на соревнование и статуса доступа «разрешен» («запрещен»).

37. Мобильные считывающие устройства СКД должны содержать встроенный дисплей для отображения фотографии и частично маскированных данных фамильно-именной группы и возраста владельца предъявленного электронного документа, предоставляющего право доступа на соревнование, а также для отображения статуса доступа «разрешен» («запрещен»).

38. Стационарные считывающие устройства СКД должны обеспечивать:

чтение идентификатора электронного документа, предоставляющего право доступа на соревнование в виде QR-кода;

передачу в базу данных СКД информации о считанных QR-кодах электронного документа, предоставляющего право доступа на соревнование;

прием из базы данных СКД решения о разрешении (запрете) доступа посетителя на объект спорта;

регистрацию факта прохода посетителя;

передачу в базу данных СКД информации о факте прохода посетителя;

работу в автономном режиме при потере связи с базой данных СКД с сохранением в своей памяти не менее одной тысячи записей о совершенных проходах;

передачу в базу данных СКД после восстановления связи сохраненной во время автономного режима работы информации о совершенных проходах.

39. Мобильные считывающие устройства СКД должны обеспечивать:

чтение идентификатора электронного документа, предоставляющего право доступа на соревнование в виде QR-кода;

беспроводную передачу в базу данных СКД информации о считанных QR-кодах электронного документа, предоставляющего право доступа на соревнование;

беспроводный прием из базы данных СКД решения о разрешении (запрете) доступа посетителей на объект спорта;

регистрацию факта прохода посетителей;

беспроводную передачу в базу данных СКД информации о факте прохода посетителей;

работу в автономном режиме при потере связи с базой данных СКД с сохранением в памяти не менее одной тысячи записей о совершенных проходах;

беспроводную передачу в базу данных СКД после восстановления связи сохраненной во время автономного режима работы информации о совершенных проходах;

отображение на встроенном дисплее фотографии и частично маскированных данных фамильно-именной группы и возраста владельца предъявленного электронного документа, предоставляющего право доступа на соревнование, а также отображение статуса доступа «разрешен» («запрещен»);

работу в беспроводной ЛВС, выделенной для нужд СКД и функционирующей в стандартном частотном диапазоне сетей Wi-Fi;

беспроводной обмен данными с базой данных СКД в беспроводной ЛВС, выделенной для нужд СКД и функционирующей в стандартном частотном диапазоне сетей Wi-Fi;

работу от автономных источников питания в течение не менее трех часов.

40. Контроллеры СКД в составе точек доступа должны обеспечивать в автоматическом режиме:

сравнение считанных QR-кодов электронных документов, предоставляющих право доступа на соревнование с хранящимися в базе данных СКД;

вывод на экран мониторного устройства фотографии, частично маскированных данных фамильно-именной группы и возраста посетителя, на которого оформлен электронный документ, предоставляющий право доступа на соревнование, статуса доступа «разрешен» («запрещен»), а также дополнительной цветовой индикации для привлечения внимания и оповещения контролера-распорядителя при доступе посетителя, не достигшего возраста 14 лет;

формирование команды разблокирования УПУ точки доступа при наличии прав на проход;

формирование команды автоматической блокировки УПУ точки доступа при отсутствии факта прохода через определенное время после считывания разрешенного QR-кода электронного документа, предоставляющего право доступа на соревнование (отказ от прохода);

регистрацию и передачу в базу данных СКД информации о факте, месте, времени и направлении совершенного посетителем прохода.

41. Контроллеры СКД в составе точек доступа объекта спорта должны обеспечивать в ручном режиме:

полную блокировку УПУ точки доступа;

разблокировку УПУ с возможностью установки блокировки входа или блокировки выхода.

42. УПУ, входящие в состав точек доступа, должны поддерживать:

режим контролируемого входа;

режим контролируемого выхода;

режим контролируемого двунаправленного прохода вход (выход).

43. УПУ, входящие в состав точек доступа, должны обеспечивать:

прием и обработку сигналов от контроллеров СКД в целях осуществления: разового прохода через турникет в направлении входа, разового прохода через турникет в направлении выхода, свободного прохода через турникет (режим разблокировано);

формирование сигналов для контроллеров СКД, информирующих о следующих событиях: готовность УПУ к проходу в направлении входа (выхода), совершение прохода через УПУ в направлении входа (выхода), наличие ошибки в работе УПУ;

формирование разрешающего и запрещающего сигналов для функционирования внешнего устройства индикации на вход (выход).

44. УПУ должны иметь возможность механического разблокирования для осуществления свободного неконтролируемого прохода.

45. Оборудование СКД точек доступа на КПП объекта спорта должно иметь элементы грозозащиты, обеспечивающие защиту от опасных напряжений, возникающих в проводах соединительных линий за счет электромагнитных полей и наводок при грозе, а также защиту от атмосферных осадков и прямых солнечных лучей, а также обеспечивать температурный режим работы установленных технических средств.

46. Информационное взаимодействие СКД и СИБ осуществляется в порядке, установленном постановлением Правительства Российской Федерации от 24 июня 2022 г. № 1130 «О порядке взаимодействия информационной системы идентификации болельщиков с информационными системами в целях идентификации и (или) аутентификации зрителей, участников официального спортивного соревнования, иных лиц, задействованных в проведении такого соревнования» (Собрание законодательства Российской Федерации, 2007, № 50, ст. 6242) (далее – Порядок взаимодействия).

VI. Требования к защите информации СКД

47. В СКД должны обеспечиваться защита обрабатываемой и хранящейся в ней информации, а также защищенный информационный обмен с СИБ и иными внешними системами в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (Собрание законодательства Российской Федерации, 2006, № 31, ст. 3451; 2021, № 27, ст. 5159), постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (Собрание законодательства Российской Федерации, 2012, № 45, ст. 6257), приказом ФСТЭК № 21, приказом ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» (зарегистрирован Минюстом России 18 августа 2014 г., регистрационный № 33620).

48. В СКД должны применяться сертифицированные средства защиты информации.

49. Технические и проектные решения СКД должны ограничивать возможность несанкционированного доступа к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование СКД, и в помещения, в которых они постоянно расположены.

50. В СКД должен обеспечиваться уровень защищенности персональных данных в соответствии с моделью угроз безопасности информации для каждого объекта спорта, согласованной с ФСБ России и ФСТЭК России, разработанной

в соответствии с пунктом 2 Порядка взаимодействия, и иметь оценку эффективности реализованных мер по обеспечению безопасности персональных данных согласно пункту 6 приказа ФСТЭК России № 21.

VII. Требования к электроснабжению оборудования СКД

51. СКД должна относиться к первой категории электроприемников по надежности электроснабжения в соответствии с подпунктом 1.2.18 Правил устройства электроустановок, утвержденных приказом Минэнерго России от 8 июля 2002 г. № 204 (признан Минюстом России не нуждающимся в государственной регистрации, письмо Минюста России от 12 августа 2002 г. № 07/7673-ЮД).

52. СКД должна быть обеспечена электропитанием от гарантированной сети переменного тока напряжением 220/380 В, частотой 50 Гц от двух независимых фидеров через аппаратуру автоматического включения резерва (щит автоматического ввода резерва).