### Требования к надежности Системы

Под надёжностью Системы понимается ее комплексное свойство сохранять во времени, в установленных нормативно-технической и (или) рабочей документацией пределах, значения параметров, характеризующих способность Системы выполнять свои функции, определяемые её назначением, режимами и условиями эксплуатации.

Критерием предельного состояния следует считать моральное старение Системы, не соответствие её текущим задачам, когда моральное старение невозможно устранить посредством технического надзора и плановым ремонтом.

Оборудование и ПО, применяемое в Системе, должны проектироваться для круглосуточной работы, позволять осуществлять резервирование и восстановление Системы после сбоев.

Система в целом должна обеспечивать выполнение целевых функций в режиме 24 часа в день, 365 дней в году за исключением периодов технического обслуживания, предусмотренных технической документацией. Критерием выполнения данного требования является значение коэффициента готовности.

К критическим компонентам Системы относятся:

* средства обработки и хранения данных;
* средства телекоммуникации и информационного взаимодействия компонентов Системы;
* средства и компоненты обеспечения информационной безопасности.

Надежность Системы должна обеспечиваться:

* отсутствием нерезервированных точек отказа критических компонентов Системы: созданием резервированных серверов, использованием высоконадежных систем хранения данных, дублированием каналов связи между серверами системы, использованием технологии виртуализации;
* возможностью "горячей" замены элементов (например, горячая замена компонентов серверов, источников питания и т.п.);
* использованием технических средств повышенной отказоустойчивости;
* наличием на объектах автоматизации запасных изделий и приборов;
* защитой технических средств по электропитанию путем использования источников бесперебойного питания;
* дублированием носителей информационных массивов;
* дублированием сети передачи данных;
* соблюдением правил эксплуатации и технического обслуживания программно-аппаратных средств;
* предварительным обучением эксплуатационного и обслуживающего персонала.

Требования к надежности приведены в таблице 1.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Таблица 1 – Требования к надежности | | | | | |
| **Сервер** | **Кластеризация** | **Виртуализация** | **Наличие RAID, тип** | **Резервирование блоков питания** | **Коэффициент готовности** |
| Серверы системы | Да | Да | Да, RAID 10 | Да | 0,99 |

Сбои в работе ПО и КТС, телекоммуникационной инфраструктуры или сетей электроснабжения не должны приводить к внесению искажений в первичные данные, получаемые и хранимые в БД, и в хранимые результаты обработки первичных данных. Сохранность информации должна обеспечиваться на аппаратном, системно-техническом, общесистемном программном и организационном уровнях.

При разработке проектных решений по обеспечению высокой надежности необходимо использовать свойства применяемой аппаратной платформы, СУБД, функциональные свойства специализированного общесистемного и прикладного программного обеспечения, а также соответствующие организационные меры.

Для обеспечения надежности Системы должно обеспечиваться непрерывное выполнение следующих функций:

* функций сбора информации;
* функций передачи информации для её последующей обработки;
* функции передачи обработанной информации вышестоящим системам.
* Надежность Системы должна быть обеспечена:
* надежностью работы технических средств Системы;
* надежность работы ПО Системы;
* квалификацией обслуживающего персонала.

На этапе разработки проектной документации для каждой группы функций должно быть определено конкретное содержание понятия «отказ» и критерии отказа по каждому виду отказов.

Виды отказов функций Системы и формулировки критериев отказов каждого вида должны быть установлены с учетом возможных причин и характера последствий отказов функции.

Среднее время восстановления исправного состояния Системы должно быть определено на этапе разработки проектной документации или на этапе сдачи Системы в эксплуатацию, но не должно превышать 8 часов (с учетом достаточного уровня квалификации обсуживающего и ремонтного персонала, а также наличия (получения и доставки) по месту необходимого комплекта ЗИП).

Надежность сохранения информации в Системе должна обеспечиваться применением программно-технических методов организации базы данных с использованием документирования проводимых обращений к БД и транзакций с использованием стандартных средств архивации.

Восстановление технических средств Системы в случае отказа должно происходить путем замены отказавших модулей. Восстановление программных средств Системы должно производиться с использованием резервных копий баз данных, образов системных дисков и конфигурационных файлов. Среднее время восстановления Системы должно быть не более 8 часов (без учета времени доставки).

Система должна обеспечивать сохранение работоспособности при отключении электроэнергии на время до 1 часа за счет применения источников бесперебойного питания.

Среднее время восстановления работоспособности компонентов Системы по любой из выполняемых функций не должно превышать 1 часа.

Система должна обеспечивать непрерывную круглосуточную работу, сохраняя возможность выполнения основных функций при выходе из строя отдельных элементов.

Должны быть использованы следующие основные способы повышения надежности Системы:

* обеспечение бесперебойного питания Системы;
* диагностика технических средств и ПО;
* защита от выдачи ложных команд и использования недостоверной информации;
* контроль информации на входе (ввод пользователями некорректных данных);
* защита данных и программного обеспечения от несанкционированного вмешательства;
* резервирование сбора и хранения данных.

В Системе должны быть предусмотрены меры по недопущению прерывания выполняемых функций, при любых единичных отказах элементов обеспечения безопасности.

В Системе должно быть предусмотрено горячее резервирование с автоматическим переключением на резерв.

В части требований электромагнитной совместимости уровню электромагнитной обстановки по месту размещения уровень помехоустойчивости Системы должен соответствовать электромагнитной обстановке в местах размещения на объектах автоматизации.

Для обеспечения работоспособности в условиях эксплуатации объектов автоматизации ПТК Системы должны соответствовать требованиям устойчивости к импульсному магнитному полю по ГОСТ Р 50649, степень жесткости 4.

В Системе должна быть обеспечена взаимозаменяемость однотипных компонентов ТЛВС без необходимости последующей регулировки и наладки.

Переключение с основного компонента ТЛВС на резервный и обратно не должно приводить к потере работоспособности Системы, а также к потере данных.

Программно-технический комплекс в части требований по надежности должен соответствовать ГОСТ 4.148-85, ГОСТ 24.701-86 и ГОСТ 27.003-90. Программно-технический комплекс должен создаваться как восстанавливаемая и ремонтопригодная система, рассчитанная на длительное функционирование.

В ПО Системы должны использоваться отлаженные библиотеки элементов и типовых алгоритмов.

Степень резервирования ТЛВС Системы должна быть определена на стадии разработки проектной документации после выбора и анализа характеристик надежности ПТК Системы.

Периодичность и продолжительность остановов ПТК должны регламентироваться графиком ремонтов оборудования.

Время наработки на отказ ТЛВС Системы должно быть не менее 5 лет.

В состав ЗИП должен входить необходимый комплект запасных частей (компонентов ТЛВС Системы), инструмента и принадлежностей (расходных материалов) в объеме, достаточном для оперативного устранения неисправностей на период не менее трех лет непрерывной эксплуатации.

Квалификация обслуживающего персонала должна быть обеспечена проведением обучения, стажировки, аттестации, привлечением к работам по внедрению, модернизации (расширению) Системы, периодическими (не реже 1 раза в год) курсами по повышению квалификации с последующей переаттестацией.

Квалификация пользователей должна быть обеспечена проведением инструктажа, разрешением и периодическими подтверждениями (не реже 1 раза в год) допуска к работе с Системой.

В Системе должна быть предусмотрена возможность проведения штатных регламентных работ. При этом суммарный простой серверного оборудования не должен превышать 12 дней в год на единицу техники.

В Системе должны быть предусмотрены средства защиты от неквалифицированных действий персонала, способных привести к нарушениям в работе Системы.

### Требования безопасности

Все внешние элементы технических средств системы, находящиеся под напряжением, должны иметь защиту от случайного прикосновения, а сами технические средства иметь зануление или защитное заземление в соответствии с ГОСТ 12.1.030-81 и "Правилами устройства электроустановок" (ПУЭ).

Технические средства должны быть установлены так, чтобы обеспечивалась безопасность при их монтаже, наладке, эксплуатации, техническом обслуживании и ремонте.

Система электропитания должна обеспечивать защитное отключение при перегрузках и коротких замыканиях в цепях нагрузки, а также аварийное ручное отключение.

Шкафы должны быть оснащены механическими блокировками двери, исключающими самопроизвольное или несанкционированное открытие. Степень защиты шкафов – не менее IP54. Шкаф должен закрываться ключом без выпирающей ручки.

Общие требования пожарной безопасности должны соответствовать нормам на бытовое электрооборудование. В случае возгорания не должно выделяться ядовитых газов и дымов. После снятия электропитания должно быть допустимо применение любых средств пожаротушения.

Факторы, оказывающие вредные воздействия на здоровье со стороны всех элементов системы (в том числе инфракрасное, ультрафиолетовое, рентгеновское и электромагнитное излучения, вибрация, шум, электростатические поля, ультразвук строчной частоты и т.д.), не должны превышать действующих норм (СанПиН 2.2.272.4.1340-03).

Уровень освещения рабочих мест персонала должен соответствовать характеру и условиям труда согласно СанПиН 2.2.4.3359-16.

#### Общие требования безопасности системы

Технические средства Системы должны соответствовать действующим требованиям промышленной безопасности, установленным Федеральным законом от 21.07.1997 №116-ФЗ «О промышленной безопасности опасных производственных объектов».

В Системе должен быть предусмотрен комплекс мер по предотвращению несанкционированного доступа (вмешательства).

Технические средства Системы и их компоненты не должны оказывать вредного воздействия на здоровье человека. Поверхность корпусов (оболочек) технических средств, с которыми возможно соприкосновение обслуживающего персонала в процессе эксплуатации и технического обслуживания не должна превышать 55 ºС.

Технические средства Системы не должны превышать санитарных норм в местах расположения обслуживающего и технического персонала по уровням освещенности, вибрации и шума.

АРМ Системы должны соответствовать требованиям СанПиН 2.2.2/2.4.1340-03.

Уровни шума и звуковой мощности, исходящей от технических средств Системы в местах расположения персонала, не должны превышать значений, установленных ГОСТом 12.1.003 ССБТ «Шум. Общие требования безопасности», и санитарным нормам. При этом должны быть учтены уровни шумов и звуковой мощности, создаваемые всеми источниками.

#### Требования информационной безопасности системы

Информационная безопасность Системы должна соответствовать требованиями ГОСТ Р 50739, ГОСТ Р МЭК 27033-1.

Безопасность технологической сети должна быть обеспечена с целью предотвращения или сведения к минимуму последствий событий, таящих угрозу функционированию ООО «XXX».

Безопасность технологической сети должна быть реализована путём защиты от вмешательств посторонних лиц в процесс функционирования Системы путем:

* аутентификации пользователей Системы;
* разграничения доступа зарегистрированным пользователям Системы к информационным, программным и техническим ресурсам Системы;
* регистрация действий пользователей Системы при использовании защищаемых ресурсов ООО «XXX»;
* при невозможности использовать физически отделенный канал связи для технологической сети использовать межсетевые экраны.

Информационная безопасность Системы должна соответствовать требованиям ГОСТ Р 50739 и внутренним документам Компании, описывающим требования к обеспечению информационной безопасности, которые должны включать:

* использование в Системе специальных вспомогательных функций или функциональных операций, реализующих самодиагностику исправности оборудования и/или блокировку ошибочных сигналов, вызванных отказами управляющих функций;
* фиксацию и сохранение (для последующего анализа) необходимой информации о случаях появления и развития аварийных ситуаций на объекте и/или отказов в Системе;
* применение специальных программных и/или технических средств защиты информационных сетей от несанкционированного доступа, а также от утечки или перехвата информации;
* контроль допустимости и автоматическую фиксацию случаев вмешательства работников и внесения им изменений в работу Системы;
* конструктивные ограничения возможности несанкционированного доступа посторонних людей к органам формирования заданий и командных сигналов, передаваемых на объект автоматизации, а также к элементам настройки алгоритмов, по которым выполняются функции Системы;
* конструктивные и/или иные меры, препятствующие проникновению посторонних лиц в места размещения ПТК Системы (боксы, шкафы, пункты, залы и т. п.), а также хищению данных ПТК, их частей, запасных элементов и расходных материалов.

#### Требования к экологической безопасности системы

Технические средства Системы не должны выделять токсические вещества выше предельно-допустимых концентраций, установленных для атмосферного воздуха, а также дурно пахнущие вещества согласно:

* ГОСТ 12.1.007-76 «Система обеспечения безопасности труда. Вредные вещества. Классификация и общие технические требования»;
* ГОСТ 12.1.005-88 «Система стандартов безопасности труда. Общие санитарно-гигиенические требования к воздуху рабочей зоны».

#### Требования к электробезопасности системы

Конструкция технических средств Системы должна обеспечить защиту работников от поражения электрическим током в соответствии с требованиями ГОСТ 12.2.003 и ГОСТ Р 50571.3-2009.

Технические средства Системы должны обеспечивать защиту работников от поражения электрическим током в соответствии с требованиями ГОСТ 12.1.030. Все внешние элементы технических средств, находящиеся под напряжением, должны иметь защиту от случайного прикосновения, а корпуса технических средств должны иметь защитное заземление в соответствии с ГОСТ 12.1.030, СНиП 12-03 и ПУЭ. Должен отсутствовать риск возгорания устройства или короткого замыкания в линии в случае выхода его из строя в результате перегрузки.

Согласно п. 444.5.1 ГОСТ Р 50571-4-44-2011 все проводники защитного заземления и функционального заземления должны быть присоединены к одной и той же главной заземляющей шине. При этом должны быть обеспечены требования производителей ПТК по подключению к функциональному заземлению.

Конструкция технических средств Системы должна обеспечивать:

* чистку и оттирку корпусов (оболочек) технических средств без снятия напряжения;
* измерение сопротивления изоляции, замену компонентов (электронных блоков) со снятием напряжения;
* защитное заземление технических средств Системы должно соответствовать правилам ПУЭ.

Технические средства Системы должны быть оснащены индикацией наличия напряжения электропитания на месте установки (монтажа), коммутационными устройствами и средствами защиты по цепям питания.

На технических средствах Системы, находящихся под напряжением выше безопасного, должны быть предусмотрены запрещающие знаки и надписи в соответствии с требованиями ГОСТ 12.4.026-2015 «Система стандартов безопасности труда. Цвета сигнальные и знаки безопасности».

Электрическое сопротивление изоляции цепей кабельной проводки между собой должно быть не менее 40 МОм/км при температуре (20 ± 5) °С.

#### Требования к пожарной безопасности системы

Технические средства Системы должны соответствовать требованиям "Правил противопожарного режима в РФ" утв. постановлением Правительства РФ № 390 от 25.04.2012 г.

Электронные изделия, применяемые в Системе, должны отвечать требованиям ГОСТ Р 53314.

Кабельные изделия, применяемые в Системе, должны соответствовать требованиям ГОСТ 53315.

Электрические и/или электронные технические средства Системы и порядок их применения должны соответствовать требованиям Федерального закона от 21.12.1994 № 69-ФЗ «О пожарной безопасности», требованиям ПУЭ и правилам техники безопасности электрических цепей ГОСТ 12.2.007.0, а средства вычислительной техники – требованиям по безопасности, установленным ГОСТ 25861.

Пожаробезопасность технических средств Системы должна обеспечиваться:

* применением в составе технических средств Системы защитных устройств электрических цепей от токов перегрузки и коротких замыканий;
* применением трудногорючих или негорючих материалов, веществ и покрытий;
* проверкой сопротивления изоляции персоналом;
* применением пожаростойких и не распространяющих горение кабелей.

### Требования к эргономике и технической эстетике

#### Требование к интерфейсу

Взаимодействие человека с Системой осуществляется через АРМ. Взаимодействие пользователей с прикладным программным обеспечением, входящим в состав системы должно осуществляться посредством визуального графического интерфейса. Навигационные элементы должны быть выполнены в удобной для пользователя форме. Ввод-вывод данных системы, прием команд и отображение результатов должны выполняться в интерактивном режиме. Интерфейс должен соответствовать современным эргономическим требованиям и обеспечивать удобный доступ к основным функциям и операциям системы.

Интерфейс должен быть рассчитан на преимущественное использование манипулятора типа "мышь" и сенсорное управление на экранах электроники, то есть управление системой должно осуществляться с помощью набора экранных меню, кнопок, значков и подобных элементов.

Экранные формы не должны быть перенасыщены информацией и разнообразием цветовой гаммы. Фон графических экранов должен быть не ярким и выбран из "спокойной" цветовой гаммы (например, RGB (18, 113, 147), RGB (85, 160, 185) или RGB (218, 236, 240)). Отображение основных объектов должно быть выполнено в 2D формате.

Система должна обеспечивать корректную обработку ситуаций, вызванных неверными действиями пользователей, неверным форматом или недопустимыми значениями входных данных. В указанных случаях Система должна выдавать пользователю соответствующие сообщения, после чего возвращаться в рабочее состояние, предшествовавшее неверной (недопустимой) команде или некорректному вводу данных.

Все надписи экранных форм, а также сообщения, выдаваемые пользователю, должны быть на русском языке (допускается формирование системных сообщений на английском языке, но их количество должно быть минимизировано).

Экранные формы должны удовлетворять требованиям унификации:

* все экранные формы пользовательского интерфейса должны быть выполнены в едином графическом дизайне, с одинаковым расположением основных элементов управления и навигации;
* для обозначения сходных операций должны использоваться сходные графические условные обозначения, кнопки и другие управляющие (навигационные) элементы. Термины, используемые для обозначения типовых операций (добавление информационной сущности, редактирование поля данных), а также последовательности действий пользователя при их выполнении, должны быть унифицированы.

### Требования к эксплуатации, техническому обслуживанию, ремонту и хранению

Система должна быть рассчитана на непрерывный круглосуточный режим работы за исключением периодов технического обслуживания, предусмотренных технической документацией.

К техническим средствам АССДА относятся узлы кластера, на котором размещаются виртуальные сервера и АРМ Системы либо физические серверы, если виртуализация не используется.

Условия и режим эксплуатации, обеспечивающие использование технических средств системы, должны соответствовать техническим описаниям и инструкциям по эксплуатации используемых технических средств и должны быть не хуже следующих условий эксплуатации:

* температура окружающего воздуха: от +5 до +35 °C;
* относительная влажность окружающего воздуха при температуре 30°С: от 40 до 90% без конденсации;
* атмосферное давление от 84 до 107 кПа;
* режим эксплуатации круглосуточный;
* виды, периодичность и регламент обслуживания технических средств должны быть указаны в соответствующих инструкциях по эксплуатации.

Периодическое обслуживание используемых технических средств должно проводиться в соответствии с требованиями технической документации разработчика Системы, но не реже одного раза в год.

В процессе проведения периодического технического обслуживания должен проводиться внешний и внутренний осмотр и чистка технических средств, проверка контактных соединений, проверка параметров функционирования, работоспособности технических средств и тестирование их взаимодействия.

На основании результатов тестирования технических средств должны проводиться анализ причин возникновения обнаруженных дефектов и приниматься меры по их ликвидации.

Обслуживание должно производиться квалифицированным персоналом, имеющим опыт работы и прошедшим соответствующее производственное обучение.

Восстановление работоспособности технических средств должно проводиться в соответствии с инструкциями разработчика и поставщика технических средств и документами по восстановлению работоспособности технических средств и завершаться проведением их тестирования.

Размещение помещений и их оборудование должны исключать возможность бесконтрольного проникновения в них посторонних лиц и обеспечивать сохранность находящихся в этих помещениях технических средств.

Размещение оборудования, технических средств должно соответствовать требованиям техники безопасности, санитарным нормам и требованиям пожарной безопасности.

Все пользователи Системы должны соблюдать правила эксплуатации электронной вычислительной техники.

Все пользователи Системы должны соблюдать правила эксплуатационной документации на Систему. Квалификация персонала и его подготовка должны соответствовать технической документации.

Должен быть предусмотрен комплект запасных частей и принадлежностей (ЗИП) в объёме не меньшем, чем указанный в главе 5.3.5 «Требования к техническому обеспечению» данного ТЗ.

### Требования к защите информации от несанкционированного доступа

В целях обеспечения нормальной работы системы и защиты информации, от воздействий лиц, не имеющих права доступа к ней, в ПО Системы должны быть предусмотрены средства защиты информации от несанкционированного доступа:

* идентификация и аутентификация пользователей при помощи пароля и исключение деятельности не идентифицированных пользователей в Системе;
* выделение пользователям прав доступа на основе ролевой модели доступа. Предоставление пользователю доступа только к той информации и функциям Системы, которые соответствуют ролям, присвоенным пользователю.

Система должна обеспечивать аутентификацию пользователей и управление доступом на следующих уровнях:

* операционная система виртуальных или физических серверов, и АРМ;
* ПО СУБД;
* базовое ПО Системы.

Проверка подлинности должна происходить с помощью индивидуального логина и пароля.

На уровне виртуальных серверов и АРМ должны использоваться механизмы авторизации, встроенные в операционные системы.

На уровнях базового ПО и ПО СУБД должны быть использованы механизмы авторизации, встроенных в это ПО.

В Системе должна быть реализована функция аудита, в задачи которой входит запись следующих событий с метками времени: регистрация, разрегистрация пользователей и их действия в режиме исполнения. Данная информация должна быть защищена от изменения или удаления.

В целях защиты информации должны применяться следующие организационно-технические методы защиты аппаратно-программных средств, на базе которых работает Система:

* ограничением доступа в помещения, где расположены технические средства Системы и физические серверы, если виртуализация не используется, либо серверы кластера, если используются виртуальные серверы Системы;
* ограничение доступа к физическим серверам, если виртуализация не используется, или к серверам кластера, если используются виртуальные сервера Системы, за счет их размещения в запираемых на ключ шкафах;
* периодическая смена паролей (периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 6 месяцев);
* периодическая антивирусная проверка (периодичность проверки на вирусы и вредоносное ПО определяется принятой политикой безопасности, но не должна превышать 1 месяца);
* организация бесперебойного питания наиболее важных аппаратных средств, на базе которых функционирует Система (серверов кластера или физических серверов, коммутационного оборудования, АРМ);
* хранение критичной к потере информации на дисковых массивах с резервированием;
* создание резервных копий критичной информации;
* использование возможностей операционной системы и прикладных программ по защите от несанкционированного доступа;
* в формулярах на АРМ и на виртуальные или физические серверы должны быть определены и зафиксированы списки программного обеспечения, разрешенного к использованию.

Подробные требования по защите информации приведены в п. 5.4. ТЗ "Общие архитектурные решения автоматизированной системы управления производством ООО «XXX»".

### Требования к функциям отображения информации в едином пользовательском интерфейсе

Отображение информации в едином пользовательском интерфейсе должно выполняться компонентами подсистемы пользовательского интерфейса.

Компоненты подсистемы пользовательского интерфейса должны обеспечивать удобный персонализированный доступ к технологической информации. Эти компоненты должны обеспечивать:

* возможность построения графического человеко-машинного интерфейса, с использованием экранных форм, одиночных и групповых трендов;
* возможность использования SQL-запросов для обработки архивных и оперативных данных;
* использование языков программирования высокого уровня для написания программ, обрабатывающих данные и расширяющих возможности стандартных клиентских приложений;
* пользовательский интерфейс на русском языке.

Инструментами отображения информации на рабочих местах являются:

* web-клиент без установки дополнительного ПО (web-браузер, «тонкий клиент» Системы);
* «толстый клиент» Системы.

Предоставление информации пользователям должно осуществляться по запросу, и содержать процедуры и инструментарий для работы с накопленными историческими и текущими данными, которые должны позволять:

* просматривать данные в табличном виде и в виде графиков исторических трендов за требуемый период времени;
* фильтровать данные по времени, параметру качества сигнала;
* рассчитывать интегральные показатели за заданный период времени;
* интерпретировать совокупность сигналов как наступление некоторого события;
* определять моменты изменения состояния оборудования по совокупности параметров;
* производить расчет наработки оборудования за заданный период;
* осуществлять фильтрацию информации о производственных и аварийных событиях по времени.

#### Экранные формы

Общими требованиями к экранным формам являются их обзорность и эргономичность. Навигационное меню экранных форм должно обеспечивать легкость и оперативность обзора всего производственного процесса. Необходимо предусмотреть возможность расширения навигационного меню.

Экранные формы должны отображать:

* мгновенные значения параметров, получаемых из локальных АСУ ТП;
* вычисляемые параметры, расчет которых производится в подсистеме обработки информации;
* текстовую информацию и цветовую индикацию.

#### Журнал тревожных сообщений

Система должна обеспечивать возможность обработки отклонений параметров процесса от установленных границ.

Графический интерфейс просмотра алармов и событий должен обеспечивать:

* оперативный выбор временного интервала просмотра;
* набор фильтров по приоритетам алармов и событий;
* группировку алармов по принадлежности к отдельным объектам производства или персоналиям;
* поиск алармов и событий;
* вывод сформированного с помощью фильтров рапорта на печать.

#### Тренды истории

Система должна иметь возможность формирования и просмотра трендов. Система отображения трендов должна удовлетворять следующим характеристикам:

* тренд должен быть оснащен набором сервисных функций по оптимизации просмотра (переназначение перьев, изменение периода, масштабирование и т. п.);
* необходимо предусмотреть возможность вывода трендов на печать.