

**УТВЕРЖДАЮ**

Заместитель генерального  
директора по безопасности  
ОАО «Тюменьэнерго»

  
С.Ю. Квачадзе

« \_\_\_\_ » \_\_\_\_\_ 2015 г.

## **ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

на внедрение системы контроля над утечками данных  
ОАО «Тюменьэнерго»

**Лот: «Внедрение системы контроля над утечками данных в  
ОАО «Тюменьэнерго»**

**Исполнитель:**

Ведущий специалист службы  
информационной безопасности  
ОАО «Тюменьэнерго»

  
И.Н. Оплетаев

г. Сургут, 2015

Исполнено: Утверждение правового обеспечения  
ОАО «Тюменьэнерго» Исполнитель И.Н.

# ОГЛАВЛЕНИЕ

|            |   |    |
|------------|---|----|
| 1          | Общие положения .....   | 4  |
|            | Наименование системы.....   | 4  |
|            | Сроки выполнения работ .....  | 4  |
| 1.1.1.     | Назначение системы.....   | 4  |
| 1.1.2.     | Цели создания системы.....  | 4  |
| 2          | Перечень нормативных документов.....  | 4  |
| 3          | Характеристики объекта автоматизации.....   | 5  |
| 3.1        | Перечень объектов защиты ОАО «Тюменьэнерго».....  | 5  |
| 3.2        | Требования к системе.....   | 5  |
| 3.2.1      | Требования к системе в целом .....  | 5  |
| 3.2.2      | Требования к структуре и функционированию Системы .....   | 6  |
| 3.2.3      | Требования к функционалу .....  | 6  |
| 3.2.4      | Требования к способам и средствам связи для информационного обмена.....                           | 9  |
| 3.2.5      | Требования к характеристикам взаимосвязей со смежными системами.....                              | 9  |
| 3.2.6      | Требования к режимам функционирования Системы .....   | 10 |
| 3.2.7      | Требования по диагностированию системы .....  | 10 |
| 3.2.8      | Перспективы развития, модернизации системы .....  | 10 |
| 3.2.9      | Требования к численности и квалификации персонала системы и режиму его работы. ....               | 10 |
| 3.2.10     | Показатели назначения .....   | 10 |
| 3.2.11     | Требования к надежности.....  | 11 |
| 3.2.12     | Требования к эргономике и технической эстетике .....  | 11 |
| 3.2.13     | Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов системы..... | 12 |
| 3.2.14     | Требования к защите информации от несанкционированного доступа .....                              | 12 |
| 3.2.15     | Требования по сохранности информации при авариях .....  | 12 |
| 3.2.16     | Требования к патентной чистоте .....  | 12 |
| 3.2.17     | Требования к стандартизации и унификации.....   | 12 |
| 3.2.18     | Требования к видам обеспечения .....  | 13 |
| 3.2.18.1   | Требования к информационному обеспечению .....  | 13 |
| 3.2.18.1.1 | Требования к составу, структуре и способам организации данных в системе ..                        | 13 |
| 3.2.18.1.2 | Требования к информационному обмену между компонентами системы .....                              | 13 |
| 3.2.18.1.3 | Требования к информационной совместимости со смежными системами .....                             | 13 |
| 3.2.18.1.4 | Требования по применению систем управления базами данных .....                                    | 13 |
| 3.2.18.1.5 | Требования к защите данных от разрушений при авариях и сбоях в электропитании системы .....       | 13 |

|            |   |           |
|------------|---|-----------|
| 3.2.18.1.6 | Требования к контролю, хранению, обновлению и восстановлению данных ...                                     | 14        |
| 3.2.19     | Требования к лингвистическому обеспечению .....   | 14        |
| 3.2.20     | Требования к программному обеспечению .....   | 14        |
| 3.2.21     | Требования к техническому обеспечению .....   | 14        |
| 3.2.22     | Требования к организационному обеспечению .....   | 14        |
| 4          | Состав и содержание работ по ВНЕДРЕНИЮ системы .....  | 15        |
| 5          | Порядок контроля и приемки системы.....   | 15        |
| 6          | Требования к составу и содержанию работ по подготовке объекта автоматизации к вводу системы в действие..... | 16        |
| 7          | Требования к документированию .....   | 17        |
| 8          | Обязательства по технической поддержке и сопровождению до ввода в эксплуатацию                              | Ошибка! З |

# 1 ОБЩИЕ ПОЛОЖЕНИЯ

Настоящий документ представляет собой техническое задание (далее – ТЗ) на проведение работ по внедрению системы контроля над утечками данных в ОАО «Тюменьэнерго».

**Лот:** «Внедрение системы контроля над утечками данных в ОАО «Тюменьэнерго»

## **Наименование системы**

Полное наименование: Система контроля над утечками данных в ОАО «Тюменьэнерго».

Условное обозначение: СКЗУД.

## **Сроки оказания услуг**

Услуги по внедрению системы контроля над утечками данных в ОАО «Тюменьэнерго» проводятся в срок с 30 апреля по 30 июня 2015 года.

### **1.1.1. Назначение системы**

СКЗУД предназначена для автоматизации деятельности персонала Заказчика, направленной на обеспечение информационной безопасности, в части обнаружения и реагирования на события информационной безопасности (ИБ), возникающие в процессе обработки, хранения и перемещения конфиденциальной информации.

### **1.1.2. Цели создания системы**

Технические меры защиты от утечек, реализуемые в рамках СКЗУД, направлены на предотвращение утечек конфиденциальной информации в случае обнаружения нарушения политики информационной безопасности организации.

СКЗУД предназначена для решения следующих задач:

- безопасное хранение данных для анализа и проведения расследований;
- мониторинг и анализ данных, отправляемых за пределы корпоративной сети через почтовые системы, web, системы обмена сообщениями, распечатываемых на локальные и сетевые принтеры и копируемых на различные съёмные устройства;
- автоматическая классификация передаваемой информации;
- контроль информационных потоков внутри Общества;
- расследование инцидентов, связанных с попытками разглашения закрытой, конфиденциальной информации или информации ограниченного доступа;
- контроль соблюдения персоналом Заказчика установленных правил, норм и регламентов обращения с информацией;
- блокирование передачи конфиденциальной информации;
- соблюдение законодательных и отраслевых требований в области защиты информации.

# 2 ПЕРЕЧЕНЬ НОРМАТИВНЫХ ДОКУМЕНТОВ

1. Конституция Российской Федерации.
2. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ.
3. Федеральный закон «О персональных данных» от 27 июля 2006 г. № 152-ФЗ.
4. Федеральный закон «О коммерческой тайне» от 29 июля 2004 г. № 98-ФЗ.
5. Постановление Правительства Российской Федерации от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
6. Постановление Правительства Российской Федерации от 15 мая 2010 г. № 330 «Об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, относимых к охраняемой в соответствии с законодательством

Российской Федерации информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, а также процессов ее проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения, об особенностях аккредитации органов по сертификации и испытательных лабораториях (центров), выполняющих работы по подтверждению соответствия указанной продукции (работ услуг)».

7. Приказ ФСТЭК от 18 февраля 2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
8. ГОСТ 34.602-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы.
9. ГОСТ Р ИСО/МЭК 17799-2005. «Информационная технология. Практические правила управления информационной безопасностью» (утв. Приказом Ростехрегулирования от 29.12.2005 N 447-ст).
10. РД 50-34.698-90 Методические указания. Информационная технология. Комплекс стандартов и руководящих документов на автоматизированные системы. Автоматизированные системы. Требования к содержанию документов.
11. РД 50-34.698-90 Автоматизированные системы. Требования к содержанию документов
12. Политика информационной безопасности ОАО «Тюменьэнерго».

### **3 ХАРАКТЕРИСТИКИ ОБЪЕКТА АВТОМАТИЗАЦИИ**

#### **3.1 Перечень объектов защиты ОАО «Тюменьэнерго»**

ОАО «Тюменьэнерго» - крупнейшая распределительная электросетевая компания Западной Сибири, обеспечивающая электроснабжением объекты на территории более 1,4 млн. кв. км в трех субъектах РФ: Ханты-Мансийском автономном округе – Югре, Тюменской области, Ямало-Ненецком автономном округе, с численностью населения 3,4 млн. человек.

ОАО «Тюменьэнерго» является юридическим лицом и руководствуется в своей деятельности Уставом ОАО «Тюменьэнерго», Гражданским Кодексом Российской Федерации, Федеральным законом Российской Федерации «Об акционерных обществах», Федеральным законом Российской Федерации «Об электроэнергетике» и иными нормативными правовыми актами Российской Федерации.

ИТ-инфраструктура Заказчика представляет собой распределенную архитектуру.

В состав объектов информатизации входят исполнительный аппарат и 9 филиалов, обеспечивающих выполнение функций, связанных с передачей и распределением электроэнергии.

Объектом защиты является исполнительный аппарат ОАО «Тюменьэнерго» по адресу: Тюменская область, Ханты-Мансийский автономный округ - Югра, г Сургут, ул. Университетская, 4.

#### **3.2 Требования к системе**

##### **3.2.1 Требования к системе в целом**

Установка Системы в существующую вычислительную сеть Заказчика не должна накладывать ограничений на нормальное функционирование серверов и рабочих станций Заказчика.

### 3.2.2 Требования к структуре и функционированию Системы

Система должна выполнять следующие требования к структуре и функционированию:

- Иметь интерфейс централизованного управления и предоставления отчетности на русском языке;
- Функционировать в составе распределенной информационно-вычислительной сети;
- Функционировать по клиент-серверной схеме;
- Поддерживать кластерные технологии;
- Обеспечивать возможность отказоустойчивости;
- Получать данные с внешних систем по протоколу ICAP;
- Обеспечивать возможность модернизации путем замены технического и/или программного обеспечения;
- Обеспечивать возможность информирования администратора безопасности об инцидентах путем отправки письма-уведомления об инциденте на почтовый электронный адрес в режиме реального времени, а также выделением в системе инцидентов цветом, отличающимся от цвета корректных событий;
- Обеспечить возможность автоматического блокирования передачи информации в случае обнаружения нарушения политик безопасности;
- Обеспечивать возможность интеграции со следующими прокси-серверами: Cisco IronPort, Bluecoat ProxySG, Microsoft Forefront TMG, Squid 3.1, прокси-сервера с поддержкой ICAP;
- Обеспечивать возможность интеграции со следующими сторонними продуктами: Lumension Device Control, DeviceLock, Microsoft Lync Server, IBM Lotus Domino Server, Microsoft Exchange Server, ArcSight, Oracle IRM, IBM TSOM;
- Обеспечивать возможность интеграции и идентификации объектов с данными, полученными из Active Directory;
- Должна быть возможность использовать Систему в структуре ДЗО, соединенных любыми каналами связи, в том числе с низкой пропускной способностью;
- Для информационного обмена между компонентами системы должны использоваться только стандартные унифицированные протоколы семейства TCP/IP;
- Обеспечивать возможность контроля трафика удаленных элементов информационной системы;
- Обеспечивать управление загрузкой канала связи при взаимодействии с модулями Комплекса, расположенными в удаленных элементах информационной системы;
- Система должна функционировать в среде следующих операционных систем:
  - Microsoft Windows XP SP3 (32 bit);
  - Microsoft Windows 7 (32, 64 bit);
  - Microsoft Windows Server 2003 (32 bit);
  - Microsoft Windows Server 2008 (64 bit);
  - Microsoft Windows Server 2008 R2 (64 bit);
  - Microsoft Windows Server 2010 (64 bit);
  - Microsoft Windows Server 2012 (64 bit);
  - Microsoft Windows 8 (64 bit);
  - Red Hat Enterprise Linux 6.

### 3.2.3 Требования к функционалу

Система должна выполнять следующие требования к функционалу:

1. Система должна поддерживать каналы перехвата данных:
  - Электронная почта (SMTP-сообщения);
  - Интернет (в том числе web-почта, форумы, перехват HTTP(s)-запросов);
  - Системы мгновенных сообщений (ICQ, Skype, Mail.ru agent, Jabber);
  - Перехват SIP (сообщения Microsoft Lync);



2. Мониторинг распространения файлов по протоколу FTP;
3. Разграничение прав доступа к периферийным устройствам (например: flash, usb-hdd, т.д.);
4. Контроль копирования информации на периферийные устройства;
5. Контроль печати (локальная, сетевая);
6. Сканирование локальных дисков, сетевых папок, MS SharePoint на предмет наличия файлов нарушающих политики информационной безопасности. Сканирование вышеперечисленных объектов должно проводиться на сервере без увеличения нагрузки на рабочие станции сотрудников;
7. Предоставлять возможность блокировки данных, передаваемых по протоколам HTTP, HTTPS, SMTP;
8. Перехват данных, передаваемых по протоколам HTTP, HTTPS, SMTP, OSCAR не должен требовать установки клиентского программного обеспечения;
9. Система должна использовать единую точку съема почтового трафика. Для перечисленных в предыдущих пунктах поддерживаемых каналов перехвата должна быть обеспечена возможность автоматической рубрикации извлеченного из объектов текста, с учетом морфологии, опечаток, транслитерации;
10. Предоставлять возможность настраивать процесс рубрикации: задавать необходимые рубрики и их иерархию, а также признаки, по которым определяется релевантность анализируемого текста той или иной рубрике;
11. Содержать предустановленные рубрики «Гриффы конфиденциальности», «Структура компании», «Юридическая документация», «Финансовая служба» и др.;
12. Обеспечивать возможность автоматического создания описания рубрик на основе имеющихся примеров документов;
13. Обеспечивать поддержание следующих видов фильтрации контента в режиме реального времени:
  - классификация перехваченной информации путем лингвистического анализа в соответствии с перечнем сведений составляющих конфиденциальную информацию;
  - определение фактов передачи экземпляров конкретных текстовых и любых бинарных файлов/документов (предварительно определенных в Системе или цитат из них методом «Цифровых отпечаток»);
  - детектирование фактов передачи текстовых объектов, сложных алфавитно-цифровых объектов (номера паспортов, индивидуальные номера налогоплательщиков, номеров кредитных карт, договоров или счетов в случае детектирования банковских реквизитов, кодов классификаторов и т.п.);
  - автоматическое определение тематики текста на основании ключевых терминов и выражений;
  - готовые шаблоны политик;
  - детектирование фактов передачи изображений главной страницы внутреннего российского паспорта;
  - детектирование фактов передачи эталонных выгрузок из баз данных;
  - детектирование заполненных форм бланков, анкет, и т.п. типовых документов;
  - детектирование эталонных печатей на изображениях отсканированных документов;
14. Обеспечивать возможность распознавания текста в графических документах;
15. Обеспечивать возможность автоматической рубрикации извлеченного из изображений текста, с учетом морфологии;
16. Осуществлять фильтрацию «мусорного трафика» (бесполезных служебных http-запросов);
17. Обеспечить возможность оперативного оповещения (по электронной почте) ответственных сотрудников – офицеров безопасности о зафиксированных событиях ИБ, а так же сотрудников-отправителей данных событий. Сотрудник, отправитель, это сотрудник который отправил объект (письмо, печать, IM и т.д.) с нарушениями политик ИБ по результату анализа. То есть другими словами это отправитель;

18. Предоставлять возможности для автоматического вынесения вердикта по перехваченному объекту (выносимый вердикт должен трактовать, нарушает ли перехваченный объект политику безопасности или нет);
19. Предоставлять возможности для задания правил автоматического вынесения вердикта по объекту. Должна обеспечиваться возможность применять правила автоматического вынесения вердикта на основании:
- формальных признаков (контекста) перехваченного объекта (отправитель, получатель и т.д.), в том числе типа перехваченного объекта (SMTP, HTTP(S), ICQ, Skype);
  - результатов контентного анализа текста, извлеченного из перехваченного объекта (результаты рубрикации, сравнения с базой эталонных документов, поиска алфавитно-цифровых объектов и т.д.).
20. Обеспечить устойчивость к следующим видам манипуляции с информацией:
- импортирование фрагмента конфиденциальной информации в документы, не являющиеся конфиденциальными;
  - изменение порядка слов;
  - изменения расстояний между словами;
  - изменение форматирования документа;
  - изменение словоформ;
  - замены букв на символы другого алфавита;
  - использование цифр вместо букв;
  - изменение расширений файлов;
21. Предоставлять возможности для автоматического проставления перехваченным объектам дополнительных атрибутов (на основании правил) (к дополнительным атрибутам относятся пользовательские теги, а также цвет, комментарии);
22. Предоставлять возможности для детектирования и распаковки следующих типов объектов:
- детектирование форматов изображения (tiff, jpeg, gif, png, bmp, pbm, pgm, ppm, wmf), аудиофайлы (wma, flac, ogg, m4a, aac, ape, mp3, wav), видеофайлы (avi, mpg, wmv, mp4), MS Project (mpp), DjVu (djv, djvu), Adobe Photoshop (psd), Corel Draw (cdr), AutoCAD R14-2013 чертежи и шаблоны (dwg, dwt, dws), DXF (Drawing eXchange Format), Microsoft Publisher (pub), Scalable Vector Graphics (svg), библиотека Linux (so), пакет linux (rpm), OpenDocument Graphics (odg), файлы баз данных (mdb), исполняемые файлы (exe), библиотека Microsoft Windows (dll), документы (chm);
  - распаковка архивов gzip, bzip2, tar, arj, zip, rar, lzh, zlib, 7z, с глубиной вложения до 100, а также самораспаковывающихся архивов. В случае перехвата запароленного архива (зашифрованного файла) система должна детектировать его как Зашифрованный текст;
  - детектирование и извлечение текста из документов MS Office (doc, docx, xls,xlsx, ppt, pptx, pps, ppsx, vsd), шаблонов MS Office (dot, dotx, dotm, xlt, xltx, xltm, pot, potx, potm), документов Adobe Acrobat (pdf), документов Open Office (odt, ods, odp), сообщений MS Outlook, документы rtf, html, Windows icon (ico), изображения emf.
  - поддерживать кодировки: iso-8859-1, iso-8859-15, iso-8859-5, Windows-1251, Windows-1252, koi8-r, utf-8, utf-16;
23. Обеспечивать возможность хранения всей электронной корреспонденции (SMTP-сообщения электронной почты), сообщений и файлов, передаваемых через различные IM в том числе и сообщения MS Lync, POST-запросов, перехваченных файлов по протоколу FTP, перехваченных теневого копий файлов и заданий на печать в течение неограниченного срока;
24. Предоставлять возможность разнесения табличного пространства хранения перехваченной информации на оперативное хранение (6 месяцев) и на архив (2 года) с поддержкой подключения архивного пространства для проведения ретроспективного анализа (расследования);



25. Позволять выгружать сегменты базы данных почтового хранилища на сменные носители или в хранилища данных с возможностью их последующего подключения и поиска по ним;
26. Предоставлять возможности по разграничению доступа пользователей к перехваченным объектам (автоматическое отнесение перехваченного объекта к той или иной зоне ответственности на основании правил);
27. Предоставлять возможности для управления зонами ответственности пользователей системы (в том числе для настройки маршрутов перемещения объектов между зонами ответственности);
28. Предоставлять возможности управлять тегами и цветом, назначенными объекту (назначать/удалять);
29. Предоставлять возможности задать комментарий для перехваченного объекта;
30. Предоставлять возможности для подготовки статистических отчетов по перехваченным объектам в следующих форматах: xls,xlsx, pdf, csv, html, rtf, bmp, emf, wmf, gif, jpeg, png, tiff, txt;
31. Обеспечивать контроль доступа пользователей к периферийным устройствам;
32. Система должна предоставлять возможность настройки следующих правил для формирования политик безопасности:
  - правил записи в файл на съемном устройстве;
  - правил доступа к периферийным устройствам;
  - правил печати;
  - правил контроля сообщений, файлов и голоса, передаваемых с помощью Skype;
  - правил контроля сообщений mail.ru agent, Jabber;
  - правил передачи файлов по протоколу FTP;
  - контроль сетевых подключений при работе за пределами корпоративной сети;
33. Система должна предоставлять возможность создания белых списков устройств, доступ к которым разрешен;
34. Система должна предоставлять возможность удаленной установки/обновления/удаления клиентских приложений системы контроля печати, записи файлов, перехвата сообщений, вложений, голосового трафика Skype, FTP, Mail.ru Agent, Jabber, доступа пользователей к периферийным устройствам.

### **3.2.4 Требования к способам и средствам связи для информационного обмена**

В Системе должен быть организован информационный обмен между компонентами Системы, перечисленными в п. 3.1 на основе стандартных унифицированных протоколов семейства TCP/IP, работающие через IPv4.

### **3.2.5 Требования к характеристикам взаимосвязей со смежными системами**

Система должна функционировать в составе распределенной информационно-вычислительной сети Заказчика.

Для перехвата копии электронной почты Заказчика Система должна взаимодействовать со смежной системой Коммутатор, обеспечивающей зеркалирование трафика.

Для перехвата копии электронной почты Заказчика Система должна взаимодействовать со смежной системой Почтовый сервер, обеспечивающей передачу данных по протоколу SMTP.

Для перехвата копии POST-запросов Заказчика Система должна взаимодействовать со смежной системой Коммутатор, обеспечивающей зеркалирование трафика.

Для перехвата копии ICQ-сообщений Заказчика Система должна взаимодействовать со смежной системой Коммутатор, обеспечивающей зеркалирование трафика.

Система должна взаимодействовать с корпоративным сервером Active Directory, обеспечивающим передачу данных по протоколу LDAP.

Система должна взаимодействовать с корпоративным сервером Novell eDirectory.

Система должна взаимодействовать с корпоративным почтовым сервером Lotus Domino.

### **3.2.6 Требования к режимам функционирования Системы**

Система должна функционировать в автоматизированном режиме под управлением администратора.

Система должна обеспечивать возможность работы в следующих режимах:

- штатный режим (непрерывная круглосуточная работа);
- сервисный режим (для проведения обслуживания, реконфигурации и модернизации компонент);
- автономный режим (в случае отсутствия связи между компонентами Системы или с внешними сетями, для доступа к конфигурационной и архивной информации).

### **3.2.7 Требования по диагностированию системы**

Система должна обеспечивать возможность записи в журналы аудита информации по служебным событиям и сбоям. Записи в журналах должны содержать информацию, достаточную для установления причины неисправности.

### **3.2.8 Перспективы развития, модернизации системы**

В рамках дальнейшего развития Система должна предусматривать добавление следующих возможностей:

- Обеспечивать возможность масштабирования до 10 000 контролируемых рабочих станций.
- Обеспечивать возможность контроля трафика удаленных компонентов системы.

### **3.2.9 Требования к численности и квалификации персонала системы и режиму его работы**

Для обеспечения функционирования Системы в составе персонала должны быть предусмотрены следующие роли:

- администратор Системы;
- офицер безопасности.

Администратор Системы должен обладать знаниями в объеме, необходимом для выполнения штатного технического и аварийного обслуживания Системы:

- навыки работы с системным программным обеспечением, требования к которому перечислены в п. 3.2.20;
- знакомство с основами языка программирования Lua.

Офицер безопасности Системы должен обладать следующими знаниями и навыками:

- знакомство с основами работы в среде операционной системы Microsoft Windows;
- навыки работы с функцией Oracle Text для осуществления поиска по тексту объектов и вложений (руководство Oracle Text Reference, 11g Release 2).

Роли администратора Системы и офицера безопасности могут совмещаться и выполняться одним сотрудником ИБ-службы Заказчика, если это не противоречит политике информационной безопасности Заказчика.

### **3.2.10 Показатели назначения**

Действия по изменению настроек конфигурации Системы должны проводиться персоналом, квалификация которого соответствует требованиям п. 3.2.9 настоящего Технического задания.

Система должна обеспечивать возможность работы в следующих режимах:

Целевое назначение Системы должно сохраняться на протяжении всего срока эксплуатации системы. Срок эксплуатации Системы определяется сроком устойчивой работы технических средств вычислительных комплексов, своевременным проведением работ по замене (обновлению) технических средств, по сопровождению и обновлению программного обеспечения Системы (в рамках гарантийного и послегарантийного обслуживания) и его модернизации.

### **3.2.11 Требования к надежности**

Требования к надежности Системы определяют условия эффективного функционирования Системы, заключающиеся в своевременном решении всех задач и представлении результатов пользователям (без сбоев технических и программных средств, ошибок персонала и т.п.).

Надежность Системы определяется надежностью прикладного и системного программного обеспечения, комплексов технических и инженерных средств, организационного обеспечения.

Технические меры по обеспечению надежности должны предусматривать:

- использование технических средств, обеспечивающих непрерывность бизнес-процессов Заказчика в случае отказов Системы;
- использование технических средств, обеспечивающих штатное функционирование в случае одновременной работы всех пользователей Заказчика на объекте автоматизации;
- сохранение всей накопленной на момент отказа или выхода из строя информации при отказе одного из компонентов Системы не зависимо от его назначения, с последующим восстановлением после проведения ремонтных и восстановительных работ функционирования Системы.

Организационные меры по обеспечению надежности должны быть направлены на минимизацию ошибок персонала (пользователей), а также обслуживающего Систему персонала при эксплуатации и проведении работ по обслуживанию комплекса технических средств Системы, минимизацию времени ремонта или замену вышедших из строя компонентов за счет:

- достаточной квалификации персонала (пользователей);
- достаточной квалификации обслуживающего персонала;
- регламентации проведения работ и процедур по обслуживанию и восстановлению Системы;
- своевременного оповещения пользователей и обслуживающего персонала о случаях нештатной работы компонентов Системы;
- своевременной диагностики неисправностей;
- наличия договоров на сервисное обслуживание и поддержку компонентов комплекса технических средств.

### **3.2.12 Требования к эргономике и технической эстетике**

Система должна соответствовать следующим требованиям к графическому интерфейсу пользователя:

- должны использоваться стандартные системные диалоговые окна и управляющие элементы;
- экранные формы и меню должны иметь простую логическую организацию;
- графический интерфейс пользователя должен быть русскоязычным.

Для обеспечения комфортной работы пользователей все пиктограммы, присутствующие на рабочих окнах модулей, должны в обязательном порядке быть снабжены надписями, поясняющими их назначение.

### **3.2.13 Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов системы**

Для обеспечения использования технических средств Системы с заданными техническими показателями должны быть выполнены все условия и режимы эксплуатации оборудования, регламентируемые документацией производителей средств вычислительной техники (техническими паспортами и техническими требованиями на его установку и эксплуатацию), включая надежное и бесперебойное электропитание, защитное заземление.

Устойчивая и надежная работа Системы обеспечивается только при регулярном выполнении работ по техническому сопровождению Системы, при поддержании в работоспособном состоянии комплекса программно-аппаратных средств, а также при жестком соблюдении пользователями требований эксплуатационной документации и регламентов работы Системы.

Эксплуатация, техническое обслуживание, профилактические и ремонтные работы технических средств должны осуществляться в соответствии с требованиями технических паспортов на оборудование Системы и элементы вычислительной сети. Перечень работ по техническому обслуживанию технических средств Системы приводится в технической документации на конкретное оборудование.

### **3.2.14 Требования к защите информации от несанкционированного доступа**

Система должна обеспечивать защиту данных Системы от несанкционированного доступа. Управление доступом к Системе должно осуществляться на следующих уровнях:

Аутентификация пользователей при входе в Систему должна осуществляться с использованием индивидуального пароля пользователя. Система должна препятствовать доступу к защищаемым ресурсам неидентифицированных пользователей и пользователей, подлинность идентификации которых при аутентификации не подтвердилась.

Разграничение доступа пользователей к данным и функциям Системы. Доступ пользователей к функциям Системы должен определяться Администратором Системы в соответствии с принятым у Заказчика регламентом предоставления доступа к информационным ресурсам.

### **3.2.15 Требования по сохранности информации при авариях**

Система должна обеспечивать сохранность информации в следующих аварийных ситуациях:

- сбой аппаратуры или программного обеспечения серверов;
- сбой или выход из строя коммуникационного оборудования локальной вычислительной сети;
- аварийное отключение питания сервера.

Для обеспечения сохранности информации Системы в этих аварийных ситуациях требуется использовать средства резервирования БД Oracle. Частота резервирования должна определяться в соответствии с принятым у Заказчика регламентом.

### **3.2.16 Требования к патентной чистоте**

Проектные решения в рамках проектирования и внедрения Системы должны отвечать требованиям по патентной чистоте согласно действующему законодательству Российской Федерации.

### **3.2.17 Требования к стандартизации и унификации**

Разработчик Системы должен иметь действующие лицензии на деятельность по технической защите конфиденциальной информации.

Разработчик Системы должен иметь действующие лицензии на деятельность по разработке и (или) производству средств защиты конфиденциальной информации.

Разработчик должен по требованию Заказчика предоставить Заказчику лицензионные (сублицензионные) соглашения, подтверждающие права на обновление и поддержку (гарантийное сопровождение) программного обеспечения.

При создании Системы должно использоваться только лицензионное программное обеспечение.

### **3.2.18 Требования к видам обеспечения**

#### **3.2.18.1 Требования к информационному обеспечению**

##### **3.2.18.1.1 Требования к составу, структуре и способам организации данных в системе**

Состав данных, которыми оперирует Система, должен включать следующие основные группы:

- информация о перехваченных объектах;
- справочная информация (классификаторы, справочники и т.п.);
- служебная информация (состав пользователей, права пользователей, пароли, системные журналы и др.).

Структуризация информации в Системе должна осуществляться путем создания связанных реляционных таблиц данных (рабочих информационных массивов).

##### **3.2.18.1.2 Требования к информационному обмену между компонентами системы**

В общем случае информационный обмен между компонентами Системы должен осуществляться стандартными для выбранного прикладного программного обеспечения способами:

- обмен данными в виде XML-сообщений по протоколу SOAP;
- передача информации посредством локальных вызовов функций программных модулей;
- передача информации о перехваченных объектах посредством файловых очередей.

##### **3.2.18.1.3 Требования к информационной совместимости со смежными системами**

Информационная совместимость со смежными системами должна обеспечиваться за счет совместимости структур передаваемых данных.

Система принимает данные от внешних систем в виде сообщений, структура которых определяется протоколами HTTP, HTTPS, SMTP, OSCAR, ICAP и LDAP.

##### **3.2.18.1.4 Требования по применению систем управления базами данных**

Для хранения всех информационных массивов Системы должна использоваться система управления базами данных Oracle.

##### **3.2.18.1.5 Требования к защите данных от разрушений при авариях и сбоях в электропитании системы**

Защита данных от разрушения должна реализовываться средствами установленной СУБД и резервного копирования. В связи с этим специальные требования к защите данных от разрушения и сбоях в электропитании Системы не предъявляются.



### **3.2.18.1.6 Требования к контролю, хранению, обновлению и восстановлению данных**

Восстановление данных в случае их утраты должно производиться администратором Системы согласно регламенту проведения резервного копирования и восстановления данных с использованием технических средств и системных программных средств Системы.

Контроль данных должен происходить как на клиентском приложении при заполнении экранных форм и получении данных с сервера, так и на серверах Системы. При заполнении экранных форм должен производиться форматный контроль введенных данных. В случае обнаружения некорректных данных пользователю должно показываться сообщение об ошибке заполнения формы с указанием ошибочных полей и типов ошибок.

### **3.2.19 Требования к лингвистическому обеспечению**

Требования к использованию языков программирования не предъявляются.

Сценарии анализа объектов в подсистемах должны создаваться с использованием языка программирования Lua.

### **3.2.20 Требования к программному обеспечению**

Требования к программному обеспечению приведены в документе: «Система контроля над утечками данных ОАО «Тюменьэнерго». Пояснительная записка к техническому проекту».48957919.401240.026.П2.02.01.М.

### **3.2.21 Требования к техническому обеспечению**

Требования к техническому обеспечению приведены в документе «Система предотвращения утечек данных ОАО «Тюменьэнерго». Пояснительная записка к техническому проекту».48957919.401240.026.П2.02.01.М.

### **3.2.22 Требования к организационному обеспечению**

В структуре ИТ-служб Заказчика должен быть определен администратор Системы, обеспечивающий поддержку ее функционирования и восстановление в случае сбоев или отказов.

Для эксплуатации Системы Заказчик должен определить персонал, который будет отвечать за выполнение следующих задач:

- управление пользователями Системы (в частности, распределение прав на работу с Системой);
- управление настройками конфигурации (в частности подготовка сценария, в соответствии с которым Система будет выполнять анализ и принятие решения по объектам);
- анализ информации и формирование отчетов по выявленным фактам передачи конфиденциальной информации;
- принятие окончательного решения по выявленным фактам передачи конфиденциальной информации.

Персонал Заказчика, который эксплуатирует Систему, должен ознакомиться с правилами эксплуатации, изложенными в комплекте документации, прилагаемом к Системе (требования к документации перечислены в п.7 «Требования к документированию» настоящего ТЗ). Степень ознакомления с документами определяется ролью (а именно, набором задач), которую Заказчик определил конкретному сотруднику в эксплуатации Системы.

## 4 СОСТАВ УСЛУГ ПО ВНЕДРЕНИЮ СИСТЕМЫ

Таблица 1. Этапы выполнения работ

| №, №<br>п/п | Состав   | Результат услуг   | Отчетные документы  |
|-------------|--|---|---|
| 1.          | Развёртывание Системы                                | Установка технических и программных средств на объектах Заказчика                                     | Паспорт Системы; Формуляр Системы;<br>Руководство пользователя;<br>Руководство администратора;<br>Описание комплекса технических средств, включающих в себя схему автоматизации;<br>План расположения оборудования и проводок,<br>Схема подключений и соединений,<br>Инструкция по эксплуатации оборудования;<br>Ведомость оборудования и материалов. |
| 2.          | Разработка Программы и методики испытаний Системы.   | Утвержденная Программа и методики испытаний системы   | Утвержденная полномочными представителями Заказчика и Исполнителя Программа и методики испытаний системы;   |
| 3.          | Опытная эксплуатация системы, исправление замечаний. | Перечень выявленных замечаний в процессе проведения опытной эксплуатации и результаты их исправления. | Приказ о начале опытной эксплуатации;<br>Акт приемки в опытную эксплуатацию;<br>Протоколы испытаний, подписанный полномочными представителями Заказчика и Исполнителя;<br>Протокол согласования, подписанный полномочными представителями Заказчика и Исполнителя;  |
| 4.          | Приемка услуг  | Приемка в промышленную эксплуатацию   | Акт сдачи-приемки оказанных услуг, подписанный полномочными представителями Заказчика и Исполнителя;<br>Утвержденный Заказчиком и Исполнителем протокол приемочных испытаний.   |

## 5 ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ СИСТЕМЫ

Контроль и приемка Системы должны проводиться в соответствии с ГОСТ 34.601-90 «Автоматизированные системы. Стадии создания» и ГОСТ 34.603-92 «Информационная технология. Виды испытаний автоматизированных систем».

Контролю, испытаниям и приемке могут подвергаться как Система в целом, так и ее подсистемы и отдельные задачи.

Для планирования проведения испытаний разрабатывается документ «Программа и методики испытаний», который устанавливает необходимый и достаточный объем испытаний, обеспечивающий заданную достоверность получаемых результатов. Программа и методики испытаний могут разрабатываться на Систему в целом и (или) ее части. В качестве приложения могут включаться сценарии проверки (контрольные примеры).

При проведении испытаний Системы должны быть выполнены проверки на соответствие Техническому заданию на развитие Системы в следующем составе:

- качество выполнения комплексом программных и технических средств автоматизированных функций во всех режимах функционирования Системы;
- знание персоналом эксплуатационной документации и наличие у него навыков, необходимых для выполнения установленных функций во всех режимах функционирования Системы;
- полнота содержащихся в эксплуатационной документации указаний персоналу по выполнению им функций во всех режимах функционирования Системы;
- количественные и/или качественные характеристики выполнения автоматических и автоматизированных функций Системы;
- другие свойства Системы, которым она должна соответствовать согласно требованиям данного Технического задания.

В рамках опытной эксплуатации проводятся испытания Системы на объекте Заказчика. Между Заказчиком и Исполнителем согласовываются даты проведения и виды испытаний, Исполнителем разрабатывается и утверждается у Заказчика Программа и методики испытаний Системы, а также состав комиссии. Состав комиссии определяется Заказчиком.

По результатам испытаний составляются протоколы с перечнем замечаний и акты завершения испытаний, на основании которых принимается решение о возможности (или невозможности) перевода Системы в промышленную эксплуатацию. Виды испытаний могут повторяться до устранения всех замечаний к Системе и соответствующей корректировки эксплуатационной документации.

Испытания Системы выполняются после проведения отладки и тестирования поставляемых программных и технических средств Системы и представления Исполнителем соответствующих документов об их готовности к испытаниям, а также после ознакомления технических специалистов Заказчика с эксплуатационной документацией Системы.

В процессе опытной эксплуатации и испытаний проводится проверка готовности отдельных подсистем и задач Системы, а также предъявленной документации к функционированию в реальных условиях. Эксплуатация Системы и ее частей начинается с момента утверждения акта приемки Системы в промышленную эксплуатацию.

Возникшие в процессе предварительных испытаний и опытной эксплуатации дополнительные требования Заказчика, не предусмотренные в техническом задании, не являются основанием для отрицательной оценки результатов опытной эксплуатации и испытаний и могут быть удовлетворены по дополнительному соглашению в согласованные сроки.

## **6 ТРЕБОВАНИЯ К ПОДГОТОВКЕ ОБЪЕКТА АВТОМАТИЗАЦИИ К ВВОДУ СИСТЕМЫ В ДЕЙСТВИЕ**

Для подготовки объекта автоматизации к вводу Системы в действие Заказчику необходимо выполнить следующие мероприятия:

- принимать непосредственное участие специалистами подразделений и служб в качестве консультантов в выполнении работ по развитию Системы (подсистем) и осуществлять контроль за ходом услуг;
- предоставлять по запросу Исполнителя необходимую информацию для настройки Системы;
- предоставить доступ к комплексу технических средств специалистам

Исполнителя с целью оказания услуг по развертыванию Системы;

- обеспечить изучение пользователями эксплуатационной документации;
- провести предварительные и приемочные испытания Системы (подсистем) совместно с Исполнителем на рабочем месте пользователя.

Для подготовки объекта автоматизации к вводу Системы в действие Исполнитель обязан:

- разработать и обеспечить пользователей необходимой эксплуатационной документацией для работы с прикладным программным обеспечением Системы (☐Руководство пользователя);
- провести предварительные и приемочные испытания Системы (подсистем) совместно с Заказчиком на рабочем месте пользователя.

## 7 ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

В рамках оказания услуг по внедрению Системы Исполнителем должна быть разработана следующая техническая документация (в соответствии с ГОСТ 34, РД 50-34.698-90):

- Паспорт Системы;
- Формуляр Системы;
- Руководство пользователя;
- Руководство администратора;
- Руководство по развертыванию;
- Руководство по установке и конфигурированию;
- Описание комплекса технических средств, включающих в себя схему автоматизации;
- План расположения оборудования и проводок;
- Схема подключений и соединений;
- Инструкция по эксплуатации оборудования;
- Ведомость оборудования и материалов;
- Программа и методики испытаний Системы, протоколы испытаний;
- Документы на ввод в эксплуатацию Системы.

Согласовано:

Начальник службы  
информационной безопасности



О.М. Маслов