СОГЛАСОВАНО

Заместитель генерального директора
ОАО РТИ по безопасности

С.И. Смоленцев

«15» апреля 2014 г.

УТВЕРЖДАЮ

Генеральный директор
ОАО РТИ

В.П. Савченко

«15» апреля 2014 г.

# ТЕХНИЧЕСКОЕ ЗАДАНИЕ

## СИСТЕМА ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

в автоматизированной системе

«Интегрированная информационная среда электронного документооборота WindChill Радиотехнического института имени академика А.Л. Минца»

СОГЛАСОВАНО

Заместитель генерального директора
ОАО РТИ по качеству

К.И. Сучков

«18» апреля 2014 г.

СОГЛАСОВАНО

Директор центра развития информационных технологий
ОАО РТИ

В.В. Кабанов

«15» апреля 2014 г.

СОГЛАСОВАНО

Начальник сектора ПДИТР
ОАО РТИ

А.Н. Бабушкин

«14» апреля 2014 г.

Москва, 2014

## Перечень сокращений

| | |
|---|---|
| АРМ | Автоматизированное рабочее место |
| ИИС | Интегрированная информационная среда |
| ИС | Информационная система |
| ЛВС | Локальная вычислительная сеть |
| НСД | Несанкционированный доступ |
| РД | Руководящий документ |
| СЗИ | Средство защиты информации |
| СиЗИ | Система защиты информации |

# 1. Общие сведения

## *1.1 Полное наименование системы*

– Система защиты конфиденциальной информации в автоматизированной системе «Интегрированная информационная среда электронного документооборота WindChill Радиотехнического института имени академика А.Л. Минца» (ИИС WindChill ОАО РТИ).

## *1.2 Наименование заказчика*

– Открытое акционерное общество «Радиотехнический институт имени академика А.Л. Минца».

– Место нахождения: 127083, г. Москва, ул. 8-го Марта, д. 10, стр. 1.

## *1.3 Перечень документов, на основании и в соответствии с которыми создается СиЗИ*

– Федеральный закон РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации»;

– Федеральный закон РФ от 27.12.2002 № 184-ФЗ «О техническом регулировании»;

– Указ Президента РФ от 17 мая 2008 года № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;

– «Положение по аттестации объектов информатизации по требованиям безопасности информации», Гостехкомиссия России, 1994 г.;

– «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)», (утверждено приказом Гостехкомиссии России от 30.08.2002 г. № 282);

– Извещение № 1-2008 о корректировке «Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К)»;

– Руководящий документ Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации (РД АС) Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г;

– Руководящий документ Средства вычислительной техники. Межсетевые экраны Защита от несанкционированного доступа к информации Показатели защищенности от несанкционированного доступа к информации (РД МЭ) Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25 июля 1997 г;

– Руководящий документ Средства вычислительной техники Защита от несанкционированного доступа к информации Показатели защищенности от несанкционированного доступа к информации (РД СВТ) Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.

### *1.4 Плановые сроки начала и окончания работ*

Сроки начала и окончания работ по разработке СиЗИ определяются договором на выполнение работ, заключенным между Заказчиком и Разработчиком.

### *1.5 Сведения об источнике и порядке финансирования работ*

Источники и порядок финансирования работ по разработке СиЗИ определяются договором на выполнение работ, заключенным между Заказчиком и Разработчиком.

### *1.6 Порядок оформления и предъявления результатов работ по разработке СиЗИ*

Установка и настройка средств защиты информации происходит в процессе работ по разработке СиЗИ. Документально оформленные результаты работ по разработке СиЗИ передаются Заказчику после выполнения всех работ. Передача оформляется актом сдачи-приемки работ.

## 2. Назначение и цели создания системы

### *2.1 Назначение СиЗИ*

Обеспечение конфиденциальности, доступности, целостности и защищённости от уничтожения конфиденциальной информации, обрабатываемой в ИИС ОАО РТИ.

### *2.2 Цели создания СиЗИ*

– обеспечение безопасности конфиденциальной информации, обрабатываемой в АС, от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, распространения, а также иных неправомерных действий;

– выполнение требований нормативных правовых актов Российской Федерации, руководящих документов ФСТЭК России, регламентирующих вопросы защиты конфиденциальной информации.

## 3. Характеристика объекта защиты

***3.1*** По структуре ИИС ОАО РТИ представляет собой локальную вычислительную сеть в составе 5 серверов и 300 автоматизированных рабочих мест. По территориальному размещению – ИИС ОАО РТИ развернута в пределах 3 (трёх) корпусов. ИИС ОАО РТИ имеет подключение к сетям связи общего пользования.

***3.2*** По результатам анализа исходных данных и сведений, в соответствии с требованиями к защите конфиденциальной информации, а также учитывая особенности технологического процесса обработки информации (многопользовательский режим с разными правами доступа пользователей к защищаемой информации) АС присвоен класс **1Г**.

***3.3*** В АС функционирует ИИС электронного документооборота Windchill.

***3.4*** Имеющиеся средства защиты информации:

3.4.1 в АС имеются межсетевые экраны Cisco 5510 – 1 шт., 5520 – 2 шт. (сертификат соответствия ФСТЭК по 4 классу МЭ);

3.4.2 для обмена конфиденциальной информацией с удаленными системами в АС имеются криптографические шлюзы CSP VPN Gate 100, 1000 и 3000 (имеются сертификаты ФСТЭК по 3 классу МЭ и сертификаты ФСБ на криптографическое средство).

## 4. Требования к системе защиты конфиденциальной информации

### *4.1 Требования к системе в целом*

*4.1.1 Требования к структуре и функционированию системы*

СиЗИ должна обеспечивать:

- защиту конфиденциальной информации от несанкционированного доступа;
- защиту конфиденциальной информации от вирусной угрозы;
- защиту конфиденциальной информации от утечки по техническим каналам.

Указанные функции должны реализовываться:

- комплексом средств защиты информации;
- документированными организационно-техническими мерами.

Комплекс программно-технических средств и организационных (процедурных) решений по защите информации от НСД должен быть реализован в рамках системы защиты информации, условно состоящей из следующих четырех подсистем:

- подсистема управления доступом;
- подсистема регистрации и учета;
- подсистема обеспечения целостности;
- подсистема антивирусной защиты;
- подсистема межсетевого экранирования.

Требования к каждой подсистеме определяются:

– требованиями руководящего документа «Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации» к автоматизированным системам класса 1Г;

– требованиями руководящего документа «Средства вычислительной техники. Межсетевые экраны Защита от несанкционированного доступа к информации Показатели защищенности от несанкционированного доступа к информации» к межсетевым экранам 4 класса

– требованиями других законодательных актов и нормативно методических документов, действующими на момент начала проектирования СиЗИ.

Требования к структуре и функционированию СиЗИ могут быть уточнены в ходе выполнения работ по согласованию с Заказчиком.

*4.1.2 Требование к надежности*

Комплекс программно-технических средств СиЗИ должен быть рассчитан для функционирования в режиме круглосуточной работы и позволять осуществлять выполнение процедур резервирования и восстановления системы после сбоев.

*4.1.3 Требования безопасности*

В процессе обслуживания и эксплуатации комплекса программно-технических средств СиЗИ должны выполняться требования по обеспечению безопасности обслуживающего персонала, предъявляемые к техническим средствам АС в целом.

*4.1.4 Требования к патентной чистоте и сертификации*

Все программное обеспечение и аппаратные средства, используемые в составе СиЗИ, должны иметь возможность легального использования на территории Российской Федерации.

Средства защиты информации, используемые в составе СиЗИ, должны иметь действующие сертификаты ФСТЭК России, удостоверяющие их соответствие требованиям по защите сведений конфиденциального характера.

Антивирусное программное обеспечение должно иметь действующий сертификат ФСТЭК России, удостоверяющий его соответствие требованиям по защите сведений конфиденциального характера.

*4.1.5 Требования по стандартизации и унификации*

Все элементы СиЗИ должны производиться из серийно поставляемых аппаратных средств и программного обеспечения. Если в процессе выполнения работ выявится необходимость доработки программного обеспечения и/или аппаратных средств, планируемых к включению в состав СиЗИ, то решение по проведению необходимых доработок должно приниматься по согласованию с Заказчиком.

### *4.2 Требования к функциям, выполняемым системой защиты конфиденциальной информации*

Реализация функций СиЗИ от утечки по техническим каналам должна обеспечиваться размещением устройств вывода информации средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической видео- и буквенно-цифровой информации, входящих в состав АС, в помещениях, в которых они установлены, таким образом, чтобы была исключена возможность просмотра посторонними лицами текстовой и графической видовой информации, содержащей конфиденциальную информацию.

### *4.3 Требования к видам обеспечения*

#### *4.3.1 Требования к техническому и программному обеспечению*

Средства защиты информации от НСД должны обеспечивать:

– аутентификацию пользователей;

– разграничение доступа пользователей к информации и ресурсам автоматизированной системы;

– доверенную информационную среду;

– контроль утечек и каналов распространения конфиденциальной информации;

– контроль устройств компьютера и отчуждаемых носителей информации на основе централизованных политик, исключающих утечки конфиденциальной информации;

– централизованное управление системой защиты, оперативный мониторинг, аудит безопасности;

– масштабируемость системы защиты, возможность дальнейшего расширения ЛВС в составе АС.

Средства защиты информации должны предусматривать сетевой режим работы, средства управления должны предоставлять возможности для настройки системы и изменения состояния объектов, а также для контроля функционирования защищаемых компьютеров. Для управления защищаемыми компьютерами и контроля их функционирования должна быть предусмотрена программа оперативного управления.

СЗИ от НСД должны иметь возможность централизованного конфигурирования, позволяющую с рабочего места администратора производить:

– настройку централизованного сбора локальных журналов безопасности;

– настройку автоматического архивирования журналов безопасности;

– настройку уведомлений об НСД, фильтрация событий;

– настройку защитных подсистем, локальной политики безопасности. Удаленное управление работой механизмов защиты и настройка параметров, применяемых на отдельных компьютерах или группах компьютеров;

– управление лицензированием;

– редактирование структуры и изменение подчиненности объектов.

СЗИ от НСД должно обеспечивать мониторинг и оперативное управление программным обеспечением СЗИ на всех АРМ и серверах АС. Мониторинг должен осуществляться в режиме реального времени и обеспечивать:

– визуализацию защищаемой сети компьютеров;

– мониторинг текущего состояния защищаемых компьютеров;

– мониторинг событий НСД в защищаемой сети;

– выполнение действий с защищаемыми компьютерами при возникновении угроз для безопасности системы;

– утверждение изменений в аппаратной конфигурации АС;

– обновление групповых политик на компьютерах;

– формирование отчетов.

*4.3.2 Требования к организационному обеспечению*

В качестве организационного обеспечения СиЗИ должны быть разработаны (доработаны) Разработчиком (в виде проектов) и внедрены Заказчиком организационно-распорядительные документы, регламентирующие организационные вопросы обеспечения безопасности конфиденциальной информации при её обработке в АС.

## 5. Состав и содержание работ по созданию системы

Состав и содержание работ по разработке СиЗИ должны включать в себя:

- работы по проектированию СиЗИ, работы по установке и настройке необходимых средств защиты информации;
- разработку проектов организационно-распорядительной документации по обеспечению безопасности конфиденциальной информации в объеме, предусмотренным руководящими документами ФСТЭК России;
- разработку проекта технического паспорта АС;
- проведение аттестационных испытаний АС;
- выдачу отчетных документов по результатам аттестации.

Сроки выполнения этапов работы устанавливаются в договоре на выполнение работ и составляют не более 50 рабочих дней.

## 6. Порядок контроля и приемки системы

Порядок контроля и приемки СиЗИ определяется договором на выполнение работ, заключенным между Заказчиком и Разработчиком.

## 7. Требования к составу и содержанию работ по подготовке объекта к вводу системы в действие

Для подготовки к вводу СиЗИ в действие необходимо проведение следующих работ:

– выполнение Заказчиком мероприятий, обеспечивающих условия функционирования АС, при которых Разработчик сможет беспрепятственно выполнить требования настоящего технического задания (в том числе, предоставление запрашиваемой Разработчиком документации, обеспечение доступа для специалистов Разработчика в помещения, в которых расположены технические средства АС, обеспечение возможности установки в АС необходимых средств защиты информации и т.п.);

– создание рабочей группы из представителей Заказчика и Разработчика для выполнения работ в соответствии с настоящим Техническим заданием;

– подготовка рабочей группой организационно-распорядительных документов, регламентирующих организационные вопросы обеспечения безопасности конфиденциальной информации при ее обработке в АС;

– назначение со стороны Заказчика лиц, ответственных за эксплуатацию СиЗИ и, при необходимости, их обучение по направлению обеспечения безопасности конфиденциальной информации.

## 8. Требования к исполнителю

Исполнитель (аттестационный центр) **обязан** иметь следующие лицензии:

- лицензия ФСБ на осуществление работ, связанных с использованием сведений, составляющих государственную тайну;
- лицензия Минобороны России на деятельность в области создания средств защиты информации;
- лицензия ФСБ на осуществление разработки и производства средств защиты конфиденциальной информации;
- лицензия ФСТЭК России на проведение работ, связанных с созданием средств защиты информации;
- лицензия ФСТЭК России на деятельность по разработке и (или) производству средств защиты конфиденциальной информации;
- лицензия ФСТЭК России на деятельность по технической защите конфиденциальной информации.

Ведущий инженер сектора ПДИТР М. Калюжный