|  |  |
| --- | --- |
|  | Утверждаю  Управляющий ООО «РТМ Технологии»  ИП Царев Е.О. /\_\_\_\_\_\_\_\_\_\_\_\_\_\_  «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_20\_\_ г. |

заключение ЭКСПЕРТа №2022/716 от 11.07.2022

по результатам исследования отчета об аудите ИТ-инфраструктуры РАН

RTM Group

**ПОДПИСКА**

Я, Шпакова Екатерина Максимовна, эксперт ООО «РТМ ТЕХНОЛОГИИ», в связи с поручением произвести судебную экспертизу по материалам арбитражного дела № A40-190138/21-82-1344, на основании определения судьи Арбитражного суда города Москвы Абызовой Е.Р., об ответственности за дачу заведомо ложного заключения по ст.307 УК РФ предупреждена.

Права и обязанности, предусмотренные ст. 85 ГПК РФ мне разъяснены.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Оглавление

[На разрешение экспертам поставлены вопросы 4](#_Toc107910780)

[На исследование представлено 4](#_Toc107910781)

[Производство исследования поручено 5](#_Toc107910782)

[Использованы следующие материалы и справочно-нормативная литература 5](#_Toc107910783)

[При проведении работ использовались следующие программные и аппаратные средства 5](#_Toc107910784)

[Используемые сокращения 6](#_Toc107910785)

[Термины и определения 6](#_Toc107910786)

[МЕТОДИКА ИССЛЕДОВАНИЯ 6](#_Toc107910787)

[ИССЛЕДОВАНИЕ 8](#_Toc107910788)

[1. Обзор материалов исследования 8](#_Toc107910789)

[2. Исследование банк-клиентского взаимодействия 9](#_Toc107910790)

[3. Исследование мобильного телефона iPhone SE 14](#_Toc107910791)

[4. Исследование финансовых транзакций 16](#_Toc107910792)

[5. Исследование лог-файла входа в личный кабинет 19](#_Toc107910793)

[ВЫВОДЫ 23](#_Toc107910794)

Производство исследования начато в 10:00 «02» июля 2022 г.

Производство исследования завершено в 18:00 «11» июля 2022 г.

Основанием для производства исследования является определение судьи Арбитражного суда города Москвы Абызовой Е.Р. от «15» июня 2022 года о приостановлении производства по делу № A40-190138/21-82-1344 и назначении судебной экспертизы.

# На разрешение экспертам поставлены вопросы

1. Является ли отчет от 15.06.2021 г., представленный ООО «Виртуализация ИТ» комплексным аудитом ИТ-инфраструктуры РАН?
2. Соответствует ли отчет от 15.06.2021 г., представленный ООО «Виртуализация ИТ» перечню работ, их объему, требованиям и характеристикам работ, требованиям к качеству установленных Техническим заданием Контракта №4У-ЭА-201-20?

# На исследование представлено

* Копия определения суда от 15.06.2022 г.;
* Отчет об аудите средств информационных технологий ФГБУ РАН (1т, л.д. 82-155);
* Отчет об аудите средств информационных технологий ФГБУ РАН (2т, л.д. 1-5);
* Контракт №4У-ЭА-201-20 (идентификационный код закупки 201772509243577250100101450016209244) с приложением №1 к контракту от 09.02.2021 г. (2т, л.д. 66-83);
* Отчет по проведенному аудиту ИТ-инфраструктуры (3т, л.д. 33-142);
* Пример отчета о техническом обследовании информационной технологической инфраструктуры (4т, л.д. 25-52);
* Отчет об аудите средств информационных технологий ФГБУ РАН (5т, л.д. 6-39);
* Отчет об аудите средств информационных технологий ФГБУ РАН (5т, л.д. 52-118);
* Диск.

# Производство исследования поручено

* эксперту Шпаковой Екатерине Максимовне, уровень подготовки: высшее образование, квалификация - квалификация специалист по специальности «Безопасность информационных технологий в правоохранительной сфере». Стаж работы в области судебной экспертизы с 2017 года.

**Эксперту известно** о том, что данное заключение может быть использовано в качестве доказательства в суде и возможности его привлечения в судебный процесс в качестве специалиста.

**Эксперту известно** об ответственности, предусмотренной ст. 307 УК РФ за дачу заведомо ложного заключения.

# Использованы следующие материалы и справочно-нормативная литература

* Федеральный закон от 31 мая 2001 г. N 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации»;
* ГОСТ Р 57429-2017 Судебная компьютерно-техническая экспертиза. Термины и определения;
* ГОСТ 34.321-96 Информационные технологии. Система стандартов по базам данных. Эталонная модель управления данными;
* ГОСТ Р ИСО 19011-2021 Оценка соответствия. Руководящие указания по проведению аудита систем менеджмента; ГОСТ Р 58811-2020 Центры обработки данных. Инженерная инфраструктура. Стадии создания.
* Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 08.06.2020) «Об информации, информационных технологиях и о защите информации»;
* Россинская Е. Р., Усов А. И. Судебная компьютерно-техническая экспертиза. М., 2001;
* Судебная экспертиза: типичные ошибки, под редакцией Россинской Е.Р. –Москва: Проспект, 2016. 544 с;
* Нехорошев А.Б., Шухнин М.Н., Юрин И.Ю., Яковлев А.Н. Практические основы компьютерно-технической экспертизы: учебно-практическое пособие. Саратов: Издательство «Научная книга», 2007.

# При проведении работ использовались следующие программные и аппаратные средства

* Персональный компьютер Intel(R) Core(TM) i5–6400K 2.7GHz/DDR16Gb/SSD-120Gb/HDD-1000Gb/HDD-2Tb, DVD-ROM;
* ноутбук HP 250 G7, 15.6", Intel Core i5 1035G1 1.0ГГц, 8ГБ, 256ГБ SSD, Intel UHD Graphics , DVD-RW, Windows 10 Professional;
* пакет прикладных программ «Microsoft Office 2016»;
* браузер «Google Chrome версия 101.0.4951.67»;
* программа для просмотра PDF-документов «Foxit Reader Version: 10.0.0.35798»;
* файловый менеджер «Total Commander 10.0»;
* МФУ типа «HP LaserJet M1132 MFP».

# Используемые сокращения

|  |  |
| --- | --- |
| Сокращение | Определение |
| API | Application programming interface (программный интерфейс приложения) |
| HTTP | HyperText Transfer Protocol |
| HTTPS | Расширение [протокола](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%82%D0%BE%D0%BA%D0%BE%D0%BB_%D0%BF%D0%B5%D1%80%D0%B5%D0%B4%D0%B0%D1%87%D0%B8_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85) [HTTP](https://ru.wikipedia.org/wiki/HTTP) для поддержки [шифрования](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5) в целях повышения безопасности |
| IP | Internet Protocol (межсетевой протокол) |

# Термины и определения

|  |  |
| --- | --- |
| Термин | Определение |
| Клиент | компонент вычислительной системы, посылающий запросы серверу |
| Клиент-сервер | вычислительная архитектура, в которой задания распределены между поставщиками услуг (серверами) и заказчиками услуг (клиентами) |
| Микросервисная архитектура | вариант программного обеспечения, направленный на взаимодействие насколько это возможно небольших, слабо связанных и легко изменяемых модулей – микросервисов |
| Сервер | компонент вычислительной системы, выполняющий запросы клиента, путем предоставления доступа к ресурсам или услугам |

# МЕТОДИКА ИССЛЕДОВАНИЯ

Методика исследования отчетов об аудите средств информационных технологий включает в себя общенаучные и частнонаучные методы исследования. В данном случае методика будет пониматься как алгоритм действий, в итоге приводящий к выяснению фактических обстоятельств, необходимых для ответа на поставленный вопрос.

Используемые методы:

* документальный — применяется в рамках исследования содержания документов;
* аналогия – перенос знания, полученного при рассмотрении какого-либо одного объекта, на другой, менее изученный, но схожий с первым объектом по каким-то существенным свойствам.
* описание — применяется в рамках установления признаков и свойств объектов;
* формализация — применяется в рамках формулирования сжатого и ёмкого ответа на поставленный вопрос;
* сопоставление — применяется в рамках сравнения фактически имеющихся результатов с необходимыми;
* формирование таблицы соответствия — применяется для установления соответствия либо не соответствия между необходимыми требуемыми характеристиками объекта и фактически имеющимися.

При проведении исследований использовалась экспертная методика, в которую входит совокупность методов, приемов и технических средств, применяемых в определенной последовательности при исследовании объектов и их свойств. Исследование производились с использованием общих методик (анализ, синтез, описание), конкретных и частных методик, описанных в исследовательской части, а именно:

* соответствие отчета об аудите требованиям к комплексному аудиту ИТ-инфраструктуры;
* сопоставление отчета об аудите требованиям технического задания.

# ИССЛЕДОВАНИЕ

Обработка результатов и исследование проводилось по месту нахождения обособленного подразделения экспертного учреждения по адресу город Воронеж, ул. Промышленная дом 4, офис 210.

## Обзор материалов исследования

Материалы, переданные на исследование, содержат:

1. Копия определения суда от 15.06.2022 г. содержит вопросы, поставленные на разрешение эксперта.
2. Контракт №4У-ЭА-201-20 на проведение комплексного аудита ИТ-инфраструктуры между ФБГУ РАН и ООО «Виртуализация ИТ» (идентификационный код закупки 201772509243577250100101450016209244) с приложением №1 «Техническая часть» к контракту от 09.02.2021 г. В приложении №1 изложены требования к технологии проведения аудита ИТ-инфраструктуры РАН, форме, структуре, содержанию, срокам.
3. Отчет об аудите средств информационных технологий ФГБУ РАН (1т, л.д. 82-155) и Отчет по проведенному аудиту ИТ-инфраструктуры (3т, л.д. 33-142) содержат электронную переписку и отчеты об аудите, что дает эксперту основания считать отчеты представленные в 1т, л.д. 82-155 и 3т, л.д. 33-142, промежуточными.
4. Отчет об аудите средств информационных технологий ФГБУ РАН (2т, л.д. 1-5) представляет собой последние 9 стр. Отчета об аудите средств информационных технологий ФГБУ РАН (1т, л.д. 82-155);
5. Пример отчета о техническом обследовании информационной технологической инфраструктуры (4т, л.д. 25-52) содержит шаблон отчета по оформлению отчета об аудите. Данный документ не фигурирует ни в Контракте, ни в Отчете об аудите.
6. Отчет об аудите средств информационных технологий ФГБУ РАН (5т, л.д. 52-118) и Отчет об аудите средств информационных технологий ФГБУ РАН (5т, л.д. 6-39) по оглавлению идентичны;
7. Диск (CD-диск) cодержит файл «Отчет по аудиту РАН финал.pdf» (MD5 - c48b999292e2846e250ddb598c41a4de), по оглавлению идентичный Отчету об аудите средств информационных технологий ФГБУ РАН (5т, л.д. 6-39).

Материалы, переданные на исследование содержат несколько вариантов отчета об аудите ИТ-инфраструктуры ФБГУ РАН c названиями «Отчет по проведенному аудиту ИТ инфраструктуры» и «Отчет об аудите средств информационных технологий ФБГУ РАН». Представленные варианты Отчета об аудите не содержат даты.

Отчет об аудите средств информационных технологий ФГБУ РАН (5т, л.д. 6-39) на тыльной стороне последнего листа содержит бумажную наклейку (фото 1.1). Данная наклейка позволяет сделать заключение о том, что это «Отчет от 15.06.2021 г., представленный ООО «Виртуализация ИТ», фигурирующий в определении суда.

Таким образом, объектами исследования являются:

1. Отчет об аудите средств информационных технологий ФГБУ РАН (5т, л.д. 6-39), (далее – Отчет об аудите).
2. Контракт №4У-ЭА-201-20 на проведение комплексного аудита ИТ-инфраструктуры между ФБГУ РАН и ООО «Виртуализация ИТ» (идентификационный код закупки 201772509243577250100101450016209244) с приложением №1 «Техническая часть» к контракту от 09.02.2021 г. (далее – Контракт).

|  |
| --- |
|  |
| Фото 1.1 – Наклейка с тыльной стороны листа 5т, л.д.39 |

## Исследование по вопросу, Является ли отчет от 15.06.2021 г., представленный ООО «Виртуализация ИТ» комплексным аудитом ИТ-инфраструктуры РАН?

В отечественной нормативно-справочной литературе отсутствует понятие «комплексный аудит ИТ-инфраструктуры», поэтому эксперт считает необходимым воспользоваться источниками из смежных отраслей знаний, а именно:

* ГОСТ Р ИСО 19011-2021 Оценка соответствия. Руководящие указания по проведению аудита систем менеджмента.
* ГОСТ Р 58811-2020 Центры обработки данных. Инженерная инфраструктура. Стадии создания.

В соответствии с ГОСТ Р ИСО 19011-2021 аудит – это систематический, независимый и документированный процесс установления объективного свидетельства и его объективного оценивания для получения степени соответствия совокупности требований, используемых как основа для сравнения с ними объективного свидетельства.

Независимость проведенного аудита (специалисты, проводящие аудит, не должны отвечать за результаты той работы, которую они проверяют) подтверждается выполнением аудита сторонней организацией.

Документируемость проведенного аудита подтверждается Отчетом об аудите.

При осуществлении внешнего аудита его периодичность устанавливается правилами органа по сертификации или заказчиком. В этой связи свойство систематичности не нарушено.

Совокупность требований, используемых как основа для сравнения с ними объективного свидетельства, представлена в п.4.1 Приложения №1 Контракта: «Анализ представленной информации выполняется для оценки следующих факторов:

* достаточности технических средств;
* достаточности программных средств;
* достаточности штатной численности сотрудников;
* достаточности методической, организационно-распорядительной и нормативно-справочной информации;
* степени соответствия ИТ-инфраструктуры основным задачам, стоящим перед Заказчиком.»

Анализ Отчета по аудиту показывает, что он содержит описание текущего состояния средств информационных технологий РАН, недостатки текущего состояния и/или замечания, соответствие бизнес-задачам Заказчика, рекомендации, т.е. подходит под определение аудита по ГОСТ Р ИСО 19011-2021.

В соответствии с ГОСТ Р 58811-2020 «ИТ-инфраструктура – это совокупность комплексов аппаратных, программных и телекоммуникационных средств автоматизированных информационных систем, размещенных в центре обработки данных и обеспечивающих предоставление информационных, вычислительных и телекоммуникационных ресурсов, возможностей и услуг потребителям». При этом ГОСТ Р 58811-2020 выделяет инженерную инфраструктуру центра обработки данных, как «комплекс систем и их оборудования, обеспечивающий бесперебойное функционирование систем и оборудования ИТ-инфраструктуры».

Проведенный аудит включает себя анализ ИТ-инфраструктуры, инженерной инфраструктуры, организационной структуры, документации, средств информационной безопасности. Таким образом, данное исследование шире, чем аудит ИТ-инфраструктуры, но с учетом наличия в определении ИТ-инфраструктуры таких широких понятий, как «комплексы аппаратных, программных и телекоммуникационных средств автоматизированных информационных систем», можно сказать, что охват исследования достаточен, для классификации его в качестве аудита ИТ-инфраструктуры РАН.

Так же в ГОСТ Р ИСО 19011-2021 содержится определение комплексного аудита, как аудита, проводимого в одной проверяемой организации для двух и более систем менеджмента одновременно. Под системой менеджмента понимается совокупность взаимосвязанных или взаимодействующих элементов организации для разработки политик, целей, и процессов для достижения этих целей.

Контракт в п.4.2 Приложения №1 содержит компоненты ИТ-инфраструктуры, которые должны быть обследованы:

1. Организационная структура ИТ-служб;
2. Информационные системы (в рамках требований обследуемых информационных систем к ИТ-инфраструктуре);
3. Вычислительное оборудование;
4. Системы хранения данных;
5. Оборудование сети хранения данных;
6. Оборудование резервного копирования и восстановления;
7. Оборудование сети передачи данных;
8. Средства информационной безопасности;
9. Оборудование и ПО видеоконференцсвязи (ВКС);
10. Инженерная инфраструктура (системы электропитания и кондиционирования серверных комнат);
11. Системное программное обеспечение (в рамках оценки текущей нагрузки);
12. Автоматизированные рабочие места пользовательского сегмента (проводится выборочно для некоторого количества пользователей).

Перечисленные в п.2-9, 11-12 компоненты являются взаимосвязанными и взаимодействующими элементами (в терминах теории систем – подсистемами) ИТ-инфраструктуры РАН. Применяя метод аналогии, можно заключить, что обследуется более 2 подсистем, что соответствует свойству «комплексности» аудита.

Таким образом, эксперт приходит к выводу, что отчет от 15.06.2021 г., представленный ООО «Виртуализация ИТ» является комплексным аудитом ИТ-инфраструктуры РАН.

## Исследование по вопросу, Соответствует ли отчет от 15.06.2021 г., представленный ООО «Виртуализация ИТ» перечню работ, их объему, требованиям и характеристикам работ, требованиям к качеству установленных Техническим заданием Контракта №4У-ЭА-201-20?

Исследование по данному вопросу проводится:

* методом документирования – изучается Приложения №1 Контракта и Отчет по аудиту;
* методом сопоставления – сравнивается перечень работ, их объем, требования и характеристики работ, требования к качеству, установленные Приложением №1 Контракта с информацией Отчета по аудиту;
* методом формирования таблиц соответствия – каждому пункту требующихся по Контракту работ, на основе анализа Отчета об аудите и опыта эксперта сопоставляется оценка степени выполнения;
* методом формализации – оценка степени выполнения представляет собой значение качественной шкалы «выполнено, выполнено частично, не выполнено».

В контексте реализации принципа «от анализа к синтезу», исследование целесообразно проводить в следующей последовательности:

* Анализ выполнения Требований к документированию, изложенных в п.7 Приложения №1 к Контракту;
* Анализ выполнения Требований к составу и содержанию работ, изложенных в п.4 Приложения №1 к Контракту;
* Анализ выполнения задач и достижения целей аудита, изложенных в п.2 Приложения №1 к Контракту.

### Анализ выполнения Требований к документированию

Оценка результатов работ по документированию аудита приведена в таблице 3.1. Эксперт понимает пункты требований, как объекты проверки аудитором, и считает выявление отсутствия объекта выполнением пункта. Эксперт считает, что аудитор предпринял все действия, предусмотренные Контрактом по получению информации для аудита. Эксперт оценивает выполнение пунктов формально, т.к. не имеет доступа к исходным данным для аудита.

При этом эксперт считает, что аудитор должен дополнять недостающие свойства объектов, если эта информация находится в свободном доступе (например, тип оборудования в п.4.4 таблицы 3.1).

В столбце Примечания таблицы 3.1 эксперт дополняет оценку. Термин «отсутствует» означает, что эксперт считает, что данный объект аудита не был предоставлен. Термин «пометка об отсутствии» означает, что эксперт считает, что данная и информация объективно существует и причины, по которым она отсутствует у Аудитора эксперту не понятны.

Также эксперт считает необходимым отметить, что Контракт не содержит ссылок на ГОСТы и каких-либо требований к глубине анализа достаточности средств информационных технологий и рекомендаций по устранению недостатков, что позволяет аудитору выполнять данные пункты исходя из своих представлений.

Таблица 3.1

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Наименование работ** | **Оценка** | **Примечания** |
|  | **Существующая документация Заказчика:** |  |  |
|  | информация о предоставленной методической, организационно-распорядительной и нормативно-справочной информации (схемы, регламенты, журналы обслуживания, инструкции и пр.) | выполнено | предоставлено 5% от необходимой документации |
|  | результаты анализа достаточности представленной документации для решения текущих задач Заказчика | выполнено |  |
|  | рекомендации по устранению обнаруженных недостатков | выполнено |  |
|  |  |  |  |
|  | **Общая информация:** |  |  |
|  | Состав(ведомость) технических средств | выполнено |  |
|  | общая архитектурная схема | выполнено |  |
|  | результаты анализа достаточности общей информации и ее соответствие бизнес-задачам Заказчика | выполнено |  |
|  | рекомендации по устранению обнаруженных недостатков | выполнено |  |
|  |  |  |  |
|  | **Информационные системы (ИС):** |  |  |
|  | функциональная схема | выполнено | отсутствует |
|  | название ИС | выполнено |  |
|  | назначение ИС | выполнено |  |
|  | возможное и текущее количество пользователей | выполнено частично | не расписано по ИС |
|  | технические требования ИС к ИТ-инфраструктуре | выполнено | отсутствует |
|  | политики хранения резервных и архивных копий ИС | выполнено | отсутствует |
|  | окна резервного копирования, требования RTO (recovery time objective) и RPO (гесоvеrу point objective) для ИС | выполнено | отсутствует |
|  | процедуры восстановления ИС и их компонентов при сбоях | выполнено | отсутствует |
|  | результаты анализа достаточности используемых архитектурных решений, политик и соответствия требований ИС к ИТ-инфраструктуре | выполнено |  |
|  | рекомендации по устранению обнаруженных недостатков | выполнено |  |
|  |  |  |  |
|  | **Вычислительное оборудование:** |  |  |
|  | схемы расположения оборудования в монтажных шкафах серверных комнат | выполнено | отсутствует |
|  | имя устройства (уникальный идентификатор) | выполнено | отсутствует |
|  | таблица IР адресации | выполнено | отсутствует |
|  | тип устройства | выполнено частично | в п.3,-5,7,9 тип не указан |
|  | производитель устройства | выполнено | пометка об отсутствии |
|  | серийный номер | выполнено | пометка об отсутствии |
|  | наличие и тип внутренней дисковой подсистемы | выполнено | отсутствует |
|  | конфигурация жестких дисков | выполнено | пометка об отсутствии |
|  | функциональное назначение устройства | выполнено | отсутствует |
|  | уровень производственной критичности устройства | выполнено | отсутствует |
|  | тип и версия операционной системы | выполнено | пометка об отсутствии |
|  | тип и количество адаптеров ввода/вывода | выполнено | пометка об отсутствии |
|  | результаты анализа достаточности используемого вычислительного оборудования и его соответствия бизнес-задачам Заказчика | выполнено |  |
|  | рекомендации по устранению обнаруженных недостатков | выполнено |  |
|  |  |  |  |
|  | **Системы хранения данных** |  |  |
|  | схема разбиения и презентации разделов СХД серверам | выполнено | отсутствует |
|  | схемы расположения оборудования в монтажных шкафах серверных комнат | выполнено | отсутствует |
|  | имя устройства (уникальный идентификатор) | выполнено | отсутствует |
|  | таблица IР адресации | выполнено | отсутствует |
|  | тип устройства | выполнено |  |
|  | производитель оборудования | выполнено |  |
|  | общее дисковое пространство | выполнено |  |
|  | используемый объем дискового пространства | выполнено | пометка об отсутствии |
|  | неиспользуемый объем дискового пространства | выполнено | пометка об отсутствии |
|  | конфигурация жестких дисков | выполнено | пометка об отсутствии |
|  | тип и количество внешних портов | выполнено | пометка об отсутствии |
|  | результат анализа достаточности используемых систем хранения данных и их соответствие бизнес-задачам Заказчика | выполнено |  |
|  | рекомендации по устранению обнаруженных недостатков | выполнено |  |
|  |  |  |  |
|  | **Оборудование сети хранения данных:** |  |  |
|  | схема подключения к сети хранения данных компонентов ИТ-инфраструктуры | выполнено | отсутствует |
|  | схемы расположения оборудования в монтажных шкафах серверных комнат | выполнено | отсутствует |
|  | имя устройства (уникальный идентификатор) | выполнено | отсутствует |
|  | таблица IР адресации | выполнено | отсутствует |
|  | тип устройства | выполнено | пометка об отсутствии |
|  | производитель оборудования | выполнено | пометка об отсутствии |
|  | тип и количество внешних портов | выполнено | пометка об отсутствии |
|  | результат анализа достаточности используемого оборудования сети хранения данных и его соответствие бизнес-задачам Заказчика | выполнено |  |
|  | рекомендации по устранению обнаруженных недостатков | выполнено |  |
|  |  |  |  |
|  | **Оборудование резервного копирования и восстановления:** |  |  |
|  | схемы расположения оборудования в монтажных шкафах серверных комнат | выполнено | отсутствует |
|  | имя устройства (уникальный идентификатор) | выполнено | отсутствует |
|  | таблица IР адресации | выполнено | отсутствует |
|  | тип устройства | выполнено | пометка об отсутствии |
|  | производитель оборудования | выполнено |  |
|  | число и тип лентопротяжных устройств (для ленточных библиотек) | выполнено | пометка об отсутствии |
|  | число и тип оптических накопителей (для оптических библиотек) | выполнено | пометка об отсутствии |
|  | число слотов для размещения носителей (для ленточных и оптических библиотек) | выполнено | пометка об отсутствии |
|  | число и тип используемых носителей (для ленточных и оптических библиотек) | выполнено | пометка об отсутствии |
|  | тип и версия ПО резервного копирования (для устройств резервного копирования) | выполнено |  |
|  | результат анализа достаточности используемого оборудования резервного копирования и их соответствие бизнес-задачам Заказчика | выполнено |  |
|  | рекомендации по устранению обнаруженных недостатков | выполнено |  |
|  |  |  |  |
|  | **Оборудование сети передачи данных:** |  |  |
|  | схемы сети передачи данных, подключения к провайдерам сети Интернет, построение сети WAN | выполнено |  |
|  | схемы расположения оборудования в монтажных шкафах серверных комнат | выполнено |  |
|  | обозначение устройства (идентификатор в инфраструктуре Заказчика) | выполнено | отсутствует |
|  | таблица IР адресации | выполнено | отсутствует |
|  | производитель оборудования | не выполнено | пометка об отсутствии |
|  | модель оборудования | выполнено | пометка об отсутствии |
|  | назначение оборудования | не выполнено | пометка об отсутствии |
|  | результат анализа достаточности используемого оборудования сети передачи данных и их соответствие бизнес-задачам Заказчика | выполнено |  |
|  | рекомендации по устранению обнаруженных недостатков | выполнено |  |
|  |  |  |  |
|  | **Средства информационной безопасности:** |  |  |
|  | схемы расположения оборудования в монтажных шкафах серверных комнат | выполнено | отсутствует |
|  | схемы взаимодействия средств информационной безопасности | выполнено | отсутствует |
|  | обозначение устройства /ПО (идентификатор в инфраструктуре Заказчика) | выполнено | отсутствует |
|  | таблица IP адресации | выполнено | отсутствует |
|  | производитель оборудования /ПО | выполнено | пометка об отсутствии |
|  | модель оборудования /ПО | выполнено | пометка об отсутствии |
|  | назначение оборудования /ПО | выполнено | пометка об отсутствии |
|  | политики и контуры безопасности | выполнено | отсутствует |
|  | ролевая модель и права доступа | выполнено | отсутствует |
|  | модели угроз | выполнено | отсутствует |
|  | результат достаточности используемых средств безопасности и их соответствие бизнес-задачам Заказчика, описывающий: |  |  |
|  | правила работы персонала с информацией | выполнено | отсутствует |
|  | внутреннюю нормативную базу, определяющую тайну и конфиденциальную информацию | выполнено | отсутствует |
|  | управление доступом к данным | выполнено | отсутствует |
|  | организацию защиты от вредоносного ПО | выполнено | отсутствует |
|  | организацию мониторинга событий в сфере информационной безопасности и реагирования на данные события | выполнено | отсутствует |
|  | используемые политики (шифрование, управление паролями, обработки данных и пр.) | выполнено | отсутствует |
|  | использование различных носителей информации | выполнено |  |
|  | порядок и требования предоставления доступа пользователям к каналам обмена информацией | выполнено | отсутствует |
|  | порядок предоставления доступа к информации третьим лицам, не являющихся сотрудниками Заказчика | выполнено | отсутствует |
|  | порядок мониторинга и контроля доступа к сети компании | выполнено |  |
|  | рекомендации по устранению обнаруженных недостатков | выполнено |  |
|  |  |  |  |
|  | **Средства видеоконференцсвязи (ВКС):** |  |  |
|  | схема взаимодействия компонентов ВКС | выполнено | отсутствует |
|  | схемы расположения оборудования в монтажных шкафах серверных комнат | выполнено | отсутствует |
|  | обозначение устройства /ПO (идентификатор в инфраструктуре Заказчика) | выполнено | отсутствует |
|  | таблица IР адресации | выполнено | отсутствует |
|  | производитель оборудования /ПО | выполнено |  |
|  | модель оборудования / ПО | выполнено |  |
|  | назначение оборудования /ПО | выполнено |  |
|  | результат анализа достаточности используемых средств ВКС и их соответствие бизнес-задачам Заказчика | выполнено |  |
|  | рекомендации по устранению обнаруженных недостатков | выполнено |  |
|  |  |  |  |
|  | **Средства инженерной инфраструктуры:** |  |  |
|  | схемы организации электропитания и кондиционирования | выполнено | отсутствует |
|  | обозначения устройства (идентификатор инфраструктуре Заказчика) | выполнено | отсутствует |
|  | производитель оборудования | выполнено | отсутствует |
|  | модель оборудования | выполнено | отсутствует |
|  | назначение оборудования | выполнено | отсутствует |
|  | средства мониторинга и управления оборудованием | выполнено | отсутствует |
|  | результат анализа достаточности используемых средств их соответствие бизнес-задачам Заказчика | выполнено |  |
|  | рекомендации по устранению обнаруженных недостатков | выполнено |  |
|  |  |  |  |
|  | **Выводы по итогам аудита (отчет для руководителей), включающий оценку текущей ситуации, с перечислением существующих рисков** | выполнено |  |
|  |  |  |  |
|  | **Рекомендации:** |  |  |
|  | рекомендации по устранению обнаруженных недостатков и рисков | выполнено |  |
|  | рекомендации по повышению надежности, производительности и эффективности функционирования информационных систем | выполнено |  |
|  | рекомендации по дальнейшему развитию информационных систем | выполнено | в виде концепции развития IT инфраструктуры |
|  | рекомендации по актуализации методической и нормативно-справочной информации | выполнено |  |

Таким образом, по документированию аудита из 117 пунктов не выполнены – 2, выполнены частично – 2. При этом информация по 72 пунктам аудитору не предоставлена, из них по 23 пунктам информация объективно существует и должна быть доступна заказчику аудита.

Также, эксперт считает необходимым отметить, что в Отчете по аудиту присутствуют дополнительные разделы, не заявленные в Требованиях к документированию: Организационная структура и Пользовательские АРМ.

### Анализ выполнения Требований к составу и содержанию работ

Требования к содержанию работ изложены в п.4.2 Приложения №1 к Контракту. Оценка соответствия содержания результатов работ приведена в таблице 3.2:

Таблица 3.2

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Содкржание работ** | **Оценка** | **Примечания** |
|  | Организационная структура ИТ-служб | выполнено | стр.52-53 Отчета |
|  | Информационные системы (в рамках требований обследуемых информационных систем к ИТ-инфраструктуре) | выполнено | стр.13-14 Отчета |
|  | Вычислительное оборудование | выполнено | стр.15-17 Отчета |
|  | Системы хранения данных | выполнено | стр.18-19 Отчета |
|  | Оборудование сети хранения данных | выполнено | стр.20-21 Отчета |
|  | Оборудование резервного копирования и восстановления | выполнено | стр.22-23 Отчета |
|  | Оборудование сети передачи данных | выполнено | стр.24-28 Отчета |
|  | Средства информационной безопасности | выполнено | стр.29-45 Отчета |
|  | Оборудование и ПО видеоконференцсвязи (ВКС) | выполнено | стр.46 Отчета |
|  | Инженерная инфраструктура (системы электропитания и кондиционирования серверных комнат) | выполнено | стр.47-51 Отчета |
|  | Системное программное обеспечение (в рамках оценки текущей нагрузки) |  |  |
|  | программное обеспечение операционных систем | выполнено | стр.13 Отчета |
|  | программное обеспечение виртуализации | выполнено | стр.13,22 Отчета |
|  | программное обеспечение платформы корпоративных коммуникаций | не выполнено |  |
|  | программное обеспечение СУБД | выполнено | стр.13,14 Отчета |
|  | программное обеспечение системы управления и мониторинга | выполнено | стр.54 Отчета |
|  | программное обеспечение системы поддержки пользователей | выполнено | стр.13,14 Отчета |
|  | Автоматизированные рабочие места пользовательского сегмента (проводится выборочно для некоторого количества пользователей) | выполнено | стр.54 Отчета |

Таким образом, по содержанию работ из 17 пунктов выполнены 16.

Требования к составу работ изложены в п.4.1 Приложения №1 к Контракту. Оценка соответствия содержания результатов работ приведена в таблице 3.3:

Таблица 3.3

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Состав работ** | **Оценка** | **Примечания** |
|  | Организационная структура ИТ-служб | выполнено | стр.52-53 Отчета |
|  | Информационные системы (в рамках требований обследуемых информационных систем к ИТ-инфраструктуре) | выполнено | стр.13-14 Отчета |
|  | Вычислительное оборудование | выполнено | стр.15-17 Отчета |
|  | Системы хранения данных | выполнено | стр.18-19 Отчета |
|  | Оборудование сети хранения данных | выполнено | стр.20-21 Отчета |
|  | Оборудование резервного копирования и восстановления | выполнено | стр.22-23 Отчета |
|  | Оборудование сети передачи данных | выполнено | стр.24-28 Отчета |

и включают 3 раздела:

Сбор информации

Анализ представленной информации о компонентах ИТ-инфраструктуры и ее дополнение.

Разработка отчетного документа

Оценка результатов работ по документированию аудита приведена в таблице 3.1. Эксперт понимает пункты требований, как объекты проверки аудитором, и считает выявление отсутствия объекта выполнением пункта. Эксперт считает, что аудитор предпринял все действия, предусмотренные Контрактом по получению информации для аудита. Эксперт оценивает выполнение пунктов формально, т.к. не имеет доступа к исходным данным для аудита.

# ВЫВОДЫ

По результатам проведенного исследования эксперты приходят к следующим выводам:

-----------------------

1. Является ли отчет от 15.06.2021 г., представленный ООО «Виртуализация ИТ» комплексным аудитом ИТ-инфраструктуры РАН?
2. Соответствует ли отчет от 15.06.2021 г., представленный ООО «Виртуализация ИТ» перечню работ, их объему, требованиям и характеристикам работ, требованиям к качеству установленных Техническим заданием Контракта №4У-ЭА-201-20?

-----------------------