Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Южно-Уральский государственный университет
(национальный исследовательский университет)»

Высшая школа электроники и компьютерных наук

Кафедра «Защита информации»

ДОПУСТИТЬ К ЗАЩИТЕ
Заведующий кафедрой,
к.т.н., доцент
_____ А.Н. Соколов
_____ 2017 г.

Аттестация ГИС "Аэропорт" Челябинского филиала "Аэронавигация Урала" ФГУП "Госкорпорация по ОрВД"

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ

Автор проекта,
студент группы КЭ- 501
_____ Овчинникова, Л. О.
_____ 2017 г.

Нормоконтролер,
к.т.н., доцент
_____ В.П. Мартынов
_____ 2017 г.

Челябинск 2017

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В реалиях современного мира остро стоит вопрос обеспечения информационной безопасности (ИБ). [1] Одним из отличительных признаков развития информационного пространства в России является его стремительный рост и увеличение числа угроз ИБ, что приводит к необходимости защищать информационные активы как государства, так и гражданина.

Важной составляющей безопасности информационного пространства является обеспечение безопасности информационных систем. [2]

Государственные информационные автоматизированные системы играют ключевую роль в жизни человека, государств и общества, поэтому для этих систем должны быть обеспечены непрерывная работа и безопасность на всех этапах их функционирования.

Активно государственные информационные системы используются для организации безопасного воздушного движения на территории Российской Федерации. На данных системах должна обеспечиваться безопасность информации во всех режимах работы и на всех этапах разработки, функционирования и вывода из эксплуатации.

Для государственных информационных систем мероприятием по контролю соответствия системы защиты информации требованиям является аттестация. Аттестация объектов информатизации – комплекс организационно-технических мероприятий, в результате которых посредством специального документа – «Аттестата соответствия» подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных Гостехкомиссией России. [3]

Единая система организации воздушного движения Российской Федерации имеет стратегическое государственное значение, является важнейшим компонентом сохранения национальной безопасности государства, обеспечения безопасности использования воздушного пространства и приемлемого уровня безопасности полетов при обслуживании воздушного движения.

1 ПОНЯТИЕ АТТЕСТАЦИИ И ЕЕ МЕСТО В СИСТЕМЕ ЗАЩИТЫ ИНФОРМАЦИИ

1.1 Обеспечение информационной безопасности в Российской Федерации

Под информационной безопасностью Российской Федерации понимают состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства, а под обеспечением информационной безопасности – осуществление взаимоувязанных правовых, организационных, оперативно-розыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления. [1]

Информационная система – совокупность содержащихся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств [2]. Защищаемая информационная система – информационная система, предназначенная для обработки защищаемой информации с требуемым уровнем ее защищенности [4].

На законодательном уровне проблема обеспечения безопасности информации не осталась без внимания. Доктрина информационной безопасности Российской Федерации, утвержденная Президентом Российской Федерации в 09.09.2000 № Пр-1895 уже не отражала в полной мере цели, задачи, принципы и основные направления обеспечения информационной безопасности, поэтому была принята новая Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 5 декабря 2016 г. № 646, которая представляет собой актуальную систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере. [1]

Принципами обеспечения информационной безопасности являются:

1) Системность и комплексность – это принцип обеспечения безопасности информационных ресурсов, содержащих информацию с ограниченным доступом, в течение всего их жизненного цикла на всех этапах и режимах обработки информации, а также анализ конфиденциальности информации и защита от угроз всеми возможными методами.

2) Своевременность – принцип реализации системы информационной безопасности на основе актуальных данных о состоянии информационных технологий, угроз информационной безопасности, а также разработка эффективных мер предупреждения посягательств на интересы заказчика в информационной сфере.

3) Законность – принцип обеспечения информационной безопасности на основе федерального законодательства в области информатизации и защиты информации и других нормативных правовых актов по безопасности информации.

4) Научно-техническая обоснованность и реализуемость – принцип использования технических и программных средств, информационных технологий, средств защиты информации реализованных на современном уровне развития науки и техники, научно и технически обоснованных с точки зрения достижения заданного уровня безопасности информации и соответствия установленным нормам и требованиям по безопасности информации.

5) Экономическая целесообразность – принцип адекватности уровня затрат на обеспечение безопасности информационных ресурсов.

6) Специализация и профессионализм – принцип привлечения к разработке и внедрению мер и средств защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности информационных ресурсов, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области.

7) Взаимодействие и координация – принцип выполнения комплекса мер по обеспечению информационной безопасности на основе взаимодействия и координации всех лиц и органов, участвующих в разработке и создании системы защиты информации.

8) Обязательность и эффективность контроля – принцип обязательности и своевременности выявления и пресечения попыток нарушения требований по обеспечения информационной безопасности.

9) Преемственность и непрерывность совершенствования – принцип постоянного совершенствования мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового аппарата, анализа функционирования системы защиты информации с учетом изменений в методах и средствах перехвата информации, нормативных требований по ее защите, достигнутого отечественного и зарубежного опыта в этой области.

10) Эффективность управления – принцип создания и постоянной актуализации данных о состоянии технической защиты информации в информационной системе. [5]

Актуальность данной темы в области воздушного транспорта обусловлена возрастающей ролью авиационной отрасли в современной системе грузовых и пассажирских перевозок. Интенсивность воздушного движения имеет четкую тенденцию роста не только на внутренних авиалиниях страны, но и на международных воздушных трассах. Авиация – наукоемкая отрасль, использующая новейшие технические и технологические достижения в приборостроении, а также средства телерадиокоммуникаций, в оснащении аэропортов и аэродромных комплексов.

Увеличение значимости авиаперевозок предполагает развитие автоматизированных систем, способствующих нормальной работе системы организации и контроля воздушного движения. Они создаются как стратегическая система обеспечения безопасного и эффективного использования воздушного пространства страны в интересах решения экономических и оборонных задач в условиях мирного и военного времени.

Постоянный процесс обновления программных и аппаратных средств предполагает наличие постоянного контроля за правильностью функционирования автоматизированных систем, который является гарантом безопасности воздушного движения. [6]

Филиал «Аэронавигация Урала» ФГУП «Госкорпорация по ОрВД» осуществляет деятельность по организации воздушного движения в границах воздушного пространства Екатеринбургского зонального центра единой системы организации воздушного движения (ЗЦ ЕС ОрВД) на территории шести субъектов Российской Федерации: Удмуртской Республики, Свердловской, Челябинской, Курганской, Пермской и Кировской областей.

В состав филиала входят семь центров обслуживания воздушного движения, расположенные в городах Екатеринбурге, Челябинске, Кургане, Магнитогорске, Перми, Кирове и Ижевске. В границах ответственности филиала семь аэропортов, в их числе четыре международных: а/п «Кольцово» (Екатеринбург), а/п «Баландино» (Челябинск), а/п «Большое Савино» (Пермь), а/п Магнитогорск.

Основные усилия руководящего состава аппарата управления филиала и центров всегда были направлены в первую очередь на обеспечение безопасности воздушного движения, повышение качества радиотехнического обслуживания полетов, поддержание практической и теоретической подготовки специалистов служб движения и ЭРТОС на высоком профессиональном уровне. Созданы и эффективно работают отделы и службы обеспечения жизнедеятельности филиала и центров: финансовые, планово-экономические, кадровые, обеспечения делопроизводства и другие.

1.2 Понятие государственной информационной системы и этапы ее построения

Информационные системы включают в себя:

1) государственные информационные системы – федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов;

2) муниципальные информационные системы, созданные на основании решения органа местного самоуправления;

3) иные информационные системы.

Государственные информационные системы создаются в целях реализации полномочий государственных органов и обеспечения обмена информацией между этими органами, а также в иных установленных федеральными законами целях. [2]

Ввод в действие государственной информационной системы осуществляется в соответствии с федеральным законом «Об информации, информационных технологиях и о защите информации», с учетом ГОСТ 34.601 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания» и при наличии аттестата соответствия. [7]

Жизненный цикл создания (разработки) и использования информационной автоматизированной системы представляет собой последовательность стадий работ, включающих однородные по содержанию и результатам этапы работ. Стадии работы, этапы жизненного цикла работы, а также документация, в которой фиксируются результаты и содержание работ приведены в Таблице 1. [8]

Таблица 1.

Стадия жизненного цикла АИС	Этап	Комплектность документов
1	2	3
1 Разработка аванпроекта	Научные исследования	Научный отчет, включающий проект технического задания
2 Разработка технического задания	Разработка, согласование, утверждение ТЗ	Техническое задание
3 Проектирование	3.1 Эскизное проектирование	1 Конструкторские документы (описание эскизного проекта ИВС - принятых технических решений) 2 Откорректированное ТЗ (при необходимости)
	3.2 Техническое проектирование	1 Конструкторские документы (описание технического проекта как доработанного эскизного проекта ИВС - принятых технических решений), ТЗ на программирование 2 Откорректированное ТЗ (при необходимости)
	3.3 Рабочее проектирование: программирование, отладка, тестирование	1 Конструкторские документы (описание принятых технических решений ИВС, текст программы на языке программирования) 2 Эксплуатационные документы

Продолжение Таблицы 1

1	2	3
3 Проектирование	3.3 Рабочее проектирование: программирование, отладка, тестирование	3 Откорректированное ТЗ (при необходимости)
	3.4 Приемо-сдаточные испытания	1 Откорректированные конструкторские документы 2 Откорректированные эксплуатационные документы 3 Протоколы испытаний 4 Технические условия (для тиражирования ИВС) 5 Акты сдачи и приемки
4 Внедрение	4.1 Адаптация на конкретные условия применения	1 Откорректированные конструкторские документы 2 Откорректированные эксплуатационные документы
	4.2 Эксплуатация	-
5 Сопровождение	5.1 Анализ проблем и разработка предложений по изменениям	1 ТЗ на внесение изменений 2 Рабочие проекты изменений
	5.2 Внесение изменений	1 Откорректированные конструкторские документы 2 Откорректированные эксплуатационные документы
	5.3 Проверка и приемка изменений	1 Протокол проверки изменений 2 Протоколы испытаний 3 Откорректированные ТУ 4 Акты сдачи и приемки работ
6 Снятие с эксплуатации	Утилизация	Протоколы об архивировании программ утилизации аппаратных средств

1.3 Организация системы защиты информации, содержащейся в ГИС

Одной из важнейших составляющих защищенности информационного пространства является обеспечение безопасности информационных систем.

В ГИС должна обеспечиваться защита информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, а также для защиты общедоступной информации, в целях обеспечения защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования,

предоставления, распространения, а также от иных неправомерных действий в отношении такой информации, а также в целях реализации права на доступ к информации. [7]

Для этих целей для каждой отдельно взятой системы разрабатывается система защиты информации.

Обязательные требования к обеспечению защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, от утечки по техническим каналам, несанкционированного доступа, специальных воздействий на такую информацию или ее носителей при обработке указанной информации в государственных информационных системах, функционирующих на территории Российской Федерации, устанавливает Приказ Федеральной службы по техническому и экспортному контролю России «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (№ 17 от 11 февраля 2013 г.). Данный приказ был редактирован Приказом ФСТЭК России № 27 от 15 февраля 2017 и претерпел существенное изменение.

При принятии решения о необходимости защиты информации, содержащейся в информационной системе, осуществляется:

– анализ целей создания информационной системы и задач, решаемых этой информационной системой;

– определение информации, подлежащей обработке в информационной системе;

– анализ нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать информационная система;

– принятие решения о необходимости создания системы защиты информации информационной системы, а также определение целей и задач защиты информации в информационной системе, основных этапов создания системы защиты информации информационной системы и функций по обеспечению защиты информации, содержащейся в информационной системе, обладателя информации (заказчика), оператора и уполномоченных лиц.

Организационные и технические меры защиты информации, реализуемые в ее рамках, в зависимости от информации, содержащейся в информационной системе, целей создания информационной системы и задач, решаемых этой информационной системой, должны быть направлены на сохранение:

– конфиденциальности информации (исключение неправомерных доступа, копирования, предоставления или распространения информации);

– целостности информации (исключение неправомерных уничтожения или модифицирования информации);

– доступности информации (исключение неправомерного блокирования информации). [7]

Основные этапы создания системы защиты информации представляют собой:

– аудит информационной системы;

– классификация информационной системы;

– моделирование угроз безопасности;

– проектирование и разработка системы защиты информации;

– реализация проекта системы защиты информации;

– мероприятие по контролю соответствия системы защиты информации требованиям законодательства в сфере защиты информации (персональных данных). [9]

Первостепенной задачей при создании системы защиты информации и контроле ее функционирования является определение класса информационной системы, так как выбранный класс устанавливает набор требований к системе защиты информации. Классификация необходима для более детальной, дифференцированной разработки требований по защите информации с учетом специфических особенностей этих систем. Требование к классу защищенности изначально включается в техническое задание на создание информационной системы или системы защиты информации.

Для определения класса защищенности ГИС необходимы два параметра – уровень значимости информации и масштаб ГИС. Класс защищенности определяется по формуле:

Класс защищенности (*К*) = [уровень значимости информации;
масштаб системы]

Уровень значимости информации определяется степенью возможного ущерба для обладателя информации (заказчика) и (или) оператора от нарушения конфиденциальности, целостности или доступности информации. Уровень значимости определяется по формуле:

УЗ = [(конфиденциальность, степень ущерба) (целостность, степень ущерба) Х
Х (доступность, степень ущерба)]

Степень возможного ущерба характеризуется негативным воздействием, оказанным на область деятельности (социальную, политическую, международную, экономическую, финансовую и иные) и возможностью выполнения информационной системой или оператором своих функций. Степень возможного ущерба определяется обладателем информации или оператором самостоятельно экспертным или иными методами и может быть:

- высокой;
- средней;
- низкой.

Информация имеет высокий уровень значимости (УЗ 1), если хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена высокая степень ущерба. Информация имеет средний уровень значимости (УЗ 2), если хотя бы для одного из свойств безопасности информации (конфиденциальности, целостности, доступности) определена средняя степень ущерба и нет ни одного свойства, для которого определена высокая степень ущерба. Информация имеет низкий уровень значимости (УЗ 3), если для всех свойств безопасности информации (конфиденциальности, целостности, доступности) определены низкие степени ущерба.

Информационная система имеет федеральный масштаб, если она функционирует на территории Российской Федерации (в пределах федерального округа) и имеет сегменты в субъектах Российской Федерации, муниципальных образованиях и (или) организациях.

Информационная система имеет региональный масштаб, если она функционирует на территории субъекта Российской Федерации и имеет сегменты в одном или нескольких муниципальных образованиях и (или) подведомственных и иных организациях.

Информационная система имеет объектовый масштаб, если она функционирует на объектах одного федерального органа государственной власти, органа государственной власти субъекта Российской Федерации, муниципального образования и (или) организации и не имеет сегментов в территориальных органах, представительствах, филиалах, подведомственных и иных организациях. [7]

При изменении масштаба системы или уровня значимости информации производят повторную классификацию объекта информатизации.

Класс защищенности государственной информационной системы определяется согласно Таблицы 2.

Таблица 2. Определение класса ГИС

Уровень значимости информации	Масштаб информационной системы		
	Федеральный	Региональный	Объектовый
УЗ 1	К1	К1	К1
УЗ 2	К1	К2	К2
УЗ 3	К2	К3	К3

Результаты установления класса объекта информатизации фиксируется в акте классификации.

Угрозы безопасности информации определяются по результатам оценки возможностей (потенциала) внешних и внутренних нарушителей, анализа возможных уязвимостей информационной системы, возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

В качестве исходных данных для определения угроз безопасности информации используется банк данных угроз безопасности информации, ведение которого осуществляется ФСТЭК России, а также иные источники, содержащие сведения об уязвимостях и угрозах безопасности информации.

При определении угроз безопасности информации учитываются структурно-функциональные характеристики информационной системы, включающие структуру и состав информационной системы, физические, логические, функциональные и технологические взаимосвязи между сегментами информационной системы, с иными информационными системами и информационно-телекоммуникационными сетями, режимы обработки информации в информационной системе и в ее отдельных сегментах, а также иные характеристики информационной системы, применяемые информационные технологии и особенности ее функционирования.

По результатам определения угроз безопасности информации при необходимости разрабатываются рекомендации по корректировке структурно-функциональных характеристик информационной системы, направленные на блокирование (нейтрализацию) отдельных угроз безопасности информации.

Модель угроз безопасности информации должна содержать описание информационной системы и ее структурно-функциональных характеристик, а также описание угроз безопасности информации, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей информационной системы, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

По результатам определения класса защищенности информационной системы и угроз безопасности информации, которые описываются в модели угроз создаются требования к системе защиты информации.

Требования должны содержать:

– цель и задачи обеспечения защиты информации в информационной системе;

– класс защищенности информационной системы;

– перечень нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать информационная система;

– перечень объектов защиты информационной системы;

– требования к мерам и средствам защиты информации, применяемым в информационной системе;

– стадии создания системы защиты информационной системы;

– требования к поставляемым техническим средствам, программному обеспечению, средствам защиты информации;

– функции заказчика и оператора по обеспечению защиты информации в информационной системе;

– требования к защите средств и систем, обеспечивающих функционирование информационной системы (обеспечивающей инфраструктуре);

– требования к защите информации при информационном взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями, в том числе с информационными системами уполномоченного лица, а также при применении вычислительных ресурсов (мощностей), предоставляемых уполномоченным лицом для обработки информации.

Разработка системы защиты информации информационной системы осуществляется в соответствии с техническим заданием на создание информационной системы или ее системы защиты информации и включает:

– проектирование системы защиты информации информационной системы;

– разработку эксплуатационной документации на систему защиты информации информационной системы;

– макетирование и тестирование системы защиты информации информационной системы (при необходимости).

Система защиты информации информационной системы не должна препятствовать достижению целей создания информационной системы и ее функционированию.

При разработке системы защиты информации информационной системы учитывается ее информационное взаимодействие с иными информационными системами и информационно-телекоммуникационными сетями.

При проектировании системы защиты информации информационной системы:

– определяются объекты и субъекты доступа;

– определяются методы разграничения доступом и управления им;

– выбираются меры защиты информации которые будут реализованы в данной информационной системе;

– определяются виды и типы средств защиты информации, обеспечивающие реализацию технических мер защиты информации;

– определяется структура системы защиты информации информационной системы, включая состав (количество) и места размещения ее элементов;

– осуществляется выбор средств защиты информации;

– определяются требования к параметрам настройки программного обеспечения;

– определяются меры защиты информации при информационном взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями.

Субъектами доступа могут являться:

– пользователи;

– процессы;

– иные субъекты доступа.

Объектами доступа, которые являются объектами защиты могут выступать:

– устройства;

– объекты файловой системы;

– запускаемые и исполняемые модули;

– объекты системы управления базами данных;

– объекты, создаваемые прикладным программным обеспечением;

– иные объекты доступа.

Метод управления доступом может быть:

– дискреционным, предусматривающим управление доступом субъектов доступа к объектам доступа на основе идентификационной информации субъекта и для каждого объекта доступа – списка, содержащего набор субъектов доступа (групп субъектов) и ассоциированных с ними типов доступа;

– ролевым, предусматривающим управление доступом субъектов доступа к объектам доступа на основе ролей субъектов доступа (совокупность действий и обязанностей, связанных с определенным видом деятельности);

– мандатным, предусматривающим управление доступом субъектов доступа к объектам доступа на основе сопоставления классификационных меток каждого субъекта доступа и каждого объекта доступа, отражающих классификационные уровни субъектов доступа и объектов доступа, являющиеся комбинациями иерархических и неиерархических категорий [10];

– иным (комбинацией из вышеперечисленных методов).

Типы доступа должны включать в себя операции по:

– чтению;

– записи;

– удалению;

– выполнению;

– иные типы доступа, разрешенные к выполнению пользователем или запускаемому от его имени процессу.

Выбор средств защиты информации должен осуществляться из списка сертифицированного на соответствие требованиям безопасности информации для данного класса защищенности информационной системы, должны учитываться стоимость средства защиты, совместимость с программно-аппаратными компонентами защищаемой информационной системы, а также их особенностей данного средства защиты.

Результаты проектирования системы защиты информации информационной системы отражаются в проектной документации на информационную систему (систему защиты информации информационной системы).

Эксплуатационная документация на систему защиты информации информационной системы разрабатывается с учетом ГОСТ 34.601, ГОСТ 34.201 и ГОСТ Р 51624 в соответствии с техническим заданием и должна в том числе содержать описание:

– структуры системы защиты информации информационной системы;

– состава, мест установки, параметров и порядка настройки средств защиты информации, программного обеспечения и технических средств;

– правил эксплуатации системы защиты информации информационной системы.

При макетировании и тестировании системы защиты информации информационной системы осуществляются проверка работоспособности и совместимости выбранных средств защиты информации с информационными технологиями и техническими средствами, выполнение выбранными средствами защиты информации требований к системе защиты информации информационной системы, а также корректировка проектных решений, разработанных при создании информационной системы и (или) системы защиты информации информационной системы.

1.4 Внедрение, эксплуатация и вывод из работы государственной информационной системы

Внедрение системы защиты информации информационной системы осуществляется в соответствии с проектной и эксплуатационной документацией и включает:

– установку и настройку средств защиты информации в информационной системе;

– разработку документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации (далее - организационно-распорядительные документы по защите информации);

– внедрение организационных мер защиты информации;

– предварительные испытания системы защиты информации информационной системы;

– опытную эксплуатацию системы защиты информации информационной системы;

– анализ уязвимостей информационной системы и принятие мер защиты информации по их устранению;

– приемочные испытания системы защиты информации информационной системы.

Разрабатываемые организационно-распорядительные документы по защите информации должны определять правила и процедуры:

– управления (администрирования) системой защиты информации информационной системы;

– выявления инцидентов, которые могут привести к сбоям или нарушению функционирования информационной системы или к возникновению угроз безопасности информации, и реагирования на них;

– управления конфигурацией аттестованной информационной системы и системы защиты информации информационной системы;

– контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе;

– защиты информации при выводе из эксплуатации информационной системы или после принятия решения об окончании обработки информации.

При внедрении организационных мер защиты информации осуществляются:

– реализация правил разграничения доступа, регламентирующих права доступа субъектов доступа к объектам доступа, и введение ограничений на действия пользователей, а также на изменение условий эксплуатации, состава и конфигурации технических средств и программного обеспечения;

– проверка полноты и детальности описания в организационно-распорядительных документах по защите информации действий пользователей и администраторов информационной системы по реализации организационных мер защиты информации;

– отработка действий должностных лиц и подразделений, ответственных за реализацию мер защиты информации.

Предварительные испытания системы защиты информации информационной системы проводятся с учетом ГОСТ 34.603 «Информационная технология. Виды испытаний автоматизированных систем» и включают проверку работоспособности

системы защиты информации информационной системы, а также принятие решения о возможности опытной эксплуатации системы защиты информации информационной системы.

Опытная эксплуатация системы защиты информации информационной системы проводится с учетом ГОСТ 34.603 и включает проверку функционирования системы защиты информации информационной системы, в том числе реализованных мер защиты информации, а также готовность пользователей и администраторов к эксплуатации системы защиты информации информационной системы.

Анализ уязвимостей информационной системы проводится в целях оценки возможности преодоления нарушителем системы защиты информации информационной системы и предотвращения реализации угроз безопасности информации и включает в себя анализ уязвимостей средств защиты информации, технических средств и программного обеспечения информационной системы.

Приемочные испытания системы защиты информации информационной системы включают проверку выполнения требований к системе защиты информации информационной системы в соответствии с техническим заданием.

Обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы осуществляется заказчиком в соответствии с эксплуатационной документацией на систему защиты информации и организационно-распорядительными документами по защите информации и в том числе включает:

– управление (администрирование) системой защиты информации информационной системы;

– выявление инцидентов и реагирование на них;

– управление конфигурацией аттестованной информационной системы и ее системы защиты информации;

– контроль (мониторинг) за обеспечением уровня защищенности информации, содержащейся в информационной системе.

Организационные и технические меры защиты информации, реализуемые в информационной системе в рамках ее системы защиты информации, в зависимости от угроз безопасности информации, используемых информационных технологий и

структурно-функциональных характеристик информационной системы должны обеспечивать:

– идентификацию и аутентификацию субъектов доступа и объектов доступа;

– управление доступом субъектов доступа к объектам доступа;

– ограничение программной среды;

– защиту машинных носителей информации;

– регистрацию событий безопасности;

– антивирусную защиту;

– обнаружение (предотвращение) вторжений;

– контроль (анализ) защищенности информации;

– целостность информационной системы и информации;

– доступность информации;

– защиту среды виртуализации;

– защиту технических средств;

– защиту информационной системы, ее средств, систем связи и передачи данных.

Состав мер защиты информации определяется выбранным классом защищенности информационных систем.

Общий порядок действий по выбору мер защиты информации для их реализации в информационной системе описан в Таблице 3. [10]

Таблица 3 – Набор мер ЗИ

Набор мер	Основание
1	2
Базовый набор мер защиты информации	Установленный класс защищенности информационной системы
Адаптированный базовый набор мер защиты информации	Особенности функционирования информационной системы, структурно-функциональные характеристики, информационные технологии
Уточненный адаптированнный базовый набор мер защиты информации	Угрозы безопасности информации, включенные в модель угроз безопасности информации

Продолжение Таблицы 3

1	2
Дополненный уточненный адаптированный базовый набор мер защиты информации	Выполнение требований о защите информации, установленными иными нормативными правовыми актами в области защиты информации

При невозможности принятия отдельных мер защиты информации могут применяться компенсирующие меры защиты информации, в полной мере нейтрализующие угрозу информационной безопасности, для которых должно быть приведено обоснование их применения, а также их достаточность и адекватность.

Организационные меры и средства защиты информации, применяемые в информационной системе, должны обеспечивать:

– защиту от угроз безопасности информации, связанных с действиями нарушителей с высоким потенциалом (в информационных системах 1 класса защищенности);

– защиту от угроз безопасности информации, связанных с действиями нарушителей с потенциалом не ниже усиленного базового (в информационных системах 2 класса защищенности);

– защиту от угроз безопасности информации, связанных с действиями нарушителей с потенциалом не ниже базового (в информационных системах 3 класса защищенности).

Обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации осуществляется оператором в соответствии с эксплуатационной документацией на систему защиты информации информационной системы и организационно-распорядительными документами по защите информации и в том числе включает:

– архивирование информации, содержащейся в информационной системе (при необходимости использования заказчиком этой информации в своей работе);

– уничтожение (стирание) данных и остаточной информации с машинных носителей информации (при передаче их сторонним организациям) или физическое уничтожение машинных носителей информации.

1.5 Правовая основа аттестации государственной информационной системы

Для государственных информационных систем мероприятием по контролю соответствия системы защиты информации требованиям является аттестация, которая характеризуется рядом признаков:

– регламентирована «Положением по аттестации объектов информатизации», рядом ГОСТов и руководящими документами ФСТЭК;

– проводится организациями, имеющими лицензию на деятельность по технической защите конфиденциальной информации;

– периодичность проведения – один раз в 3 года (для ГИС – раз в 5 лет), также проводится ежегодный инструментальный контроль.

Органы по аттестации аккредитуются Гостехкомиссией России и получают от нее лицензию. Правила аккредитации определяются действующим в системе «Положением об аккредитации испытательных лабораторий и органов по сертификации средств защиты информации по требованиям безопасности информации». Гостехкомиссия России может передавать права на аккредитацию отраслевых (ведомственных) органов по аттестации другим органам государственной власти. Проведение аттестационных испытаний информационной системы должностными лицами, осуществляющими проектирование и (или) внедрение системы защиты информации информационной системы, не допускается.

Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации представлена в Таблице 4.

Таблица 4. Структурообразующие органы и лица

Орган	Выполняемые функции
1	2
Гостехкомиссия России – федеральный орган по сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации	- организация обязательной аттестации объектов информатизации; - создание системы аттестации объектов информатизации и установление правил для проведения аттестации в этих системах; - установление правил аккредитации и выдачи лицензий на проведение работ по обязательной аттестации; - организация, финансирование разработки и утверждение нормативных и методических документов по аттестации объектов

Продолжение Таблицы 4

1	2
Гостехкомиссия России – федеральный орган по сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации	информатизации; - аккредитация органов по аттестации объектов информатизации и выдача им лицензии на проведение определенных видов работ; - осуществление государственного контроля и надзора за соблюдением правил аттестации и эксплуатацией аттестованных объектов информатизации; - рассмотрение апелляций, возникающих в процессе аттестации объектов информатизации и контроля за эксплуатацией аттестованных объектов информатизации; - организация периодической публикации информации по функционированию системы аттестации объектов информатизации по требованиям безопасности информации
Органы по аттестации объектов информатизации по требованиям безопасности информации	- аттестация объектов информатизации и выдача «Аттестатов соответствия»; - осуществление контроля за безопасностью информации, циркулирующей на аттестованных объектах информатизации, и за их эксплуатацией; - отмена и приостановка действия выданных этим органом «Аттестатов соответствия»; - формирование фонда нормативной и методической документации, необходимой для аттестации конкретных типов объектов информатизации, участие в их разработке; - ведение информационной базы аттестованных этим органом объектов информатизации; - осуществление взаимодействия с Гостехкомиссией России и ежеквартального информирования его о своей деятельности в области аттестации.
Испытательные центры (лаборатории) по сертификации продукции по требованиям безопасности информации	Проведение испытания несертифицированной продукции, используемой на объекте информатизации, подлежащем обязательной аттестации, в соответствии с «Положением о сертификации средств защиты информации по требованиям безопасности информации».
Заявители (заказчики, владельцы, разработчики аттестуемых объектов информатизации)	- проведение подготовки объекта информатизации для аттестации путем реализации необходимых организационно-технических мероприятий по защите информации; - привлечение органов по аттестации для организации и проведения аттестации объекта информатизации; - предоставление органам по аттестации необходимых документов и условий для проведения аттестации;
Заявители (заказчики, владельцы, разработчики аттестуемых объектов информати-	- привлечение, в необходимых случаях, для проведения испытаний несертифицированных средств защиты информации, используемых на аттестуемом объекте информатизации, испытательных центров (лабораторий) по сертификации;

Окончание Таблицы 4

1	2
зации)	- осуществление эксплуатации объекта информатизации в соответствии с условиями и требованиями, установленными в «Аттестате соответствия»; - извещение органа по аттестации, выдавшего «Аттестат соответствия», обо всех изменениях в информационных технологиях, составе и размещении средств и систем информатизации, условиях их эксплуатации, которые могут повлиять на эффективность мер и средств защиты информации (перечень характеристик, определяющих безопасность информации, об изменениях которых требуется обязательно извещать орган по аттестации, приводится в «Аттестате соответствия»); - предоставление необходимых документов и условий для осуществления контроля и надзора за эксплуатацией объекта информатизации, прошедшего обязательную аттестацию.

Порядок проведения аттестации объектов информатизации по требованиям безопасности информации включает следующие действия:

– подачу и рассмотрение заявки на аттестацию (заявитель отправляет в орган по аттестации заявку, которую орган по аттестации рассматривает в месячный срок, а также составляет план аттестации на основании исходных данных);

– предварительное ознакомление с аттестуемым объектом (проводится до начала аттестационных испытаний при недостаточности исходных данных об объекте);

– испытание несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте (при необходимости), по итогам испытаний выдаются соответствующие заключения;

– разработка программы и методики аттестационных испытаний (включает в себя виды аттестационных работ, сроки их выполнения, состав комиссии по аттестации, используемое оборудование и программные средства и т.д.), которая согласуется с заявителем;

– заключение договоров на аттестацию между заявителем и органом по аттестации;

– проведение аттестационных испытаний объекта информатизации;

– оформление, регистрация и выдача «Аттестата соответствия»;

– осуществление государственного контроля и надзора, инспекционного контроля за проведением аттестации и эксплуатацией аттестованных объектов информатизации (включает проверку правильности и полноты проводимых мероприятий по аттестации объектов информатизации, оформления и рассмотрения органами по аттестации отчетных документов и протоколов испытаний, своевременное внесение изменений в нормативную и методическую документацию по безопасности информации, инспекционный контроль за эксплуатацией аттестованных объектов информатизации);

– рассмотрение апелляций, которые подаются в вышестоящий орган по аттестации или непосредственно в Гостехкомиссию России, где она рассматривается в месячный срок.

При составлении заявки на аттестацию рассматриваются следующие исходные данные:

1) Полное наименование объекта информатизации и выполняемые им функции.

2) Характер (научно-техническая, экономическая, производственная, финансовая, военная, политическая) и уровень конфиденциальности обрабатываемой информации, а также документ, на основании которого эта информация отнесена к информации ограниченного доступа.

3) Организационная структура объекта информатизации.

4) Перечень помещений, состав комплекса основных и вспомогательных технических средств.

5) Схема расположения объекта информатизации с указанием границ контролируемой зоны.

6) Структура программного обеспечения (общесистемного и прикладного), используемого на аттестуемом объекте информатизации и предназначенного для обработки защищаемой информации, используемые протоколы обмена информацией.

7) Общая функциональная схема объекта информатизации, в которой указаны информационные потоки и режимы обработки защищаемой информации.

8) Характер взаимодействия с другими объектами информатизации (при наличии).

9) Характеристика системы защиты информации на аттестуемом объекте информатизации.

10) Перечень технических и программных средств в защищенном исполнении, средств защиты и контроля, используемых на аттестуемом объекте информатизации и имеющих соответствующий сертификат, предписание на эксплуатацию.

11) Сведения о разработчиках системы защиты информации, наличие у сторонних разработчиков лицензий на проведение подобных работ.

12) Наличие на объекте информатизации службы безопасности информации, службы администратора.

13) Наличие и основные характеристики физической защиты объекта информатизации (помещений, где обрабатывается защищаемая информация и хранятся информационные носители).

14) Наличие и готовность проектной и эксплуатационной документации на объект информатизации и другие исходные данные по аттестуемому объекту информатизации, влияющие на безопасность информации.

В качестве исходной документации, необходимой для аттестации информационной системы, выступают:

- модель угроз безопасности информации;
- акт классификации информационной системы;
- техническое задание на создание информационной системы;
- техническое задание (частное техническое задание) на создание системы защиты информации информационной системы;
- проектная и эксплуатационная документация на систему защиты информации информационной системы;
- организационно-распорядительные документы по защите информации,
- результаты анализа уязвимостей информационной системы;
- материалы предварительных и приемочных испытаний системы защиты информации информационной системы;

– и др. [7]

Аттестация предусматривает комплексную проверку (аттестационные испытания) защищаемого объекта информатизации в реальных условиях эксплуатации с целью оценки соответствия применяемого комплекса мер и средств защиты требуемому уровню безопасности информации. Аттестация проводится органом по аттестации в установленном «Положением по аттестации объектов информатизации по требованиям безопасности информации» порядке в соответствии со схемой, выбираемой этим органом на этапе подготовки к аттестации из основного перечня работ, указанного ниже.

На этапе аттестационных испытаний объекта информатизации осуществляется анализ организационной структуры объекта информатизации, информационных потоков, состава и структуры комплекса технических средств и программного обеспечения, системы защиты информации на объекте. Проводится экспертное обследование объекта информатизации и анализ разработанной документации по защите информации на этом объекте с точки зрения ее соответствия требованиям нормативной и методической документации.

Важным этапом является определение правильности классификации автоматизированной системы, работы средств и систем защиты информации.

Проверяется уровень подготовки кадров (образование, стаж работы, право работы с информацией ограниченного доступа) и соответствие лиц, ответственных за защиту информации на объекте, указанным в организационно-распорядительной документации.

После проверки соответствия документации требованиям, в режиме работы проводится комплекс аттестационных испытаний, описанный в «Программе и методике…», на всех этапах его технологического процесса, где проверяется правильность выполнения мер и требований по защите информации. Проведение испытаний отдельных средств и систем защиты информации на аттестуемом объекте информатизации осуществляется с помощью специальной контрольной аппаратуры и тестовых средств. При необходимости проводятся испытания несертифицирован-

ных средств и систем защиты информации непосредственно на объекте информатизации или анализ результатов их испытаний в испытательных центрах (лабораториях) по сертификации. [3]

При проведении аттестационных испытаний должны применяться следующие методы проверок (испытаний):

– экспертно-документальный метод, предусматривающий проверку соответствия системы защиты информации информационной системы установленным требованиям по защите информации, на основе оценки эксплуатационной документации, организационно-распорядительных документов по защите информации, а также условий функционирования информационной системы;

– анализ уязвимостей информационной системы, в том числе вызванных неправильной настройкой (конфигурированием) программного обеспечения и средств защиты информации;

– испытания системы защиты информации путем осуществления попыток несанкционированного доступа (воздействия) к информационной системе в обход ее системы защиты информации. [7]

По итогам проверки оформляются протоколы испытаний и заключение по результатам аттестации, в котором указываются рекомендации по устранению выявленных нарушений (если таковые имеются), по приведению объекта информатизации в соответствие с требованиями и по возможному усовершенствованию системы, а также рекомендации по контролю за эксплуатацией объекта информатизации.

Заключение по результатам аттестации, в котором описывается степень защищенности объекта информатизации, степень соответствия требованиям по безопасности информации, а также вывод о возможности выдачи «Аттестата соответствия» и необходимые рекомендации, подписывается членами аттестационной комиссии, утверждается органом по аттестации, проводившим проверку, и выдается заявителю. К заключению прилагаются протоколы испытаний, подтверждающие полученные при испытаниях результаты и обосновывающие приведенный в заключении вывод.

После утверждения положительного заключения по результатам аттестационных испытаний заявителю выдается «Аттестат соответствия».

Органами по аттестации ведется информационная база объектов информатизации, которые имеют «Аттестат соответствия». Сводную информационную базу обрабатывает Гостехкомиссия России или один из органов надзора.

«Аттестат соответствия» выдается заявителю на время, за которое обеспечивается неизменность условий функционирования информационной системы, но не более, чем на 3 года (для государственных информационных систем данный срок составляет 5 лет).

Владелец аттестованного объекта информатизации несет ответственность за выполнение установленных условий функционирования объекта информатизации, технологии обработки защищаемой информации и требований по безопасности информации.

В случае изменения условий и технологии обработки защищаемой информации владельцы аттестованных объектов обязаны известить об этом орган по аттестации, который принимает решение о необходимости проведения дополнительной проверки эффективности системы защиты объекта информатизации.

При несоответствии аттестуемого объекта требованиям по безопасности информации и невозможности оперативно устранить отмеченные аттестационной комиссией недостатки орган по аттестации принимает решение об отказе в выдаче «Аттестата соответствия». [3]

Выводы по первому разделу

Обеспечение информационной безопасности в государственных информационных системах – важная часть функционирования организаций и предприятий, которая регулируется целым комплексом нормативно-правовых актов. Для государственных информационных систем мероприятием по контролю соответствия системы защиты информации требованиям является аттестация, регламентированая

«Положением по аттестации объектов информатизации», рядом ГОСТов и руководящими документами ФСТЭК.

2 АТТЕСТАЦИЯ ГОСУДАРСТВЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ «АЭРОПОРТ»

2.1 Составление заявки на аттестацию и предварительное ознакомление с аттестуемым объектом

В рамках аттестационных мероприятий специалистами ЗАО «Гранит Информ» было проведено обследование государственной информационной системы «Аэропорт» Челябинского центра ОВД филиала «Аэронавигация Урала» ФГУП «Госкорпорация по ОрВД» (далее ГИС), обрабатывающей информацию ограниченного доступа. Исходные данные были использованы для составления заявки на аттестацию и дальнейшего проведения аттестационных испытаний.

Обследование проводилось путем:

– определения перечня информации ограниченного доступа, подлежащих защите;

– определения условий расположения ГИС относительно границ контролируемой зоны;

– определения конфигурации и топологии ГИС в целом и ее отдельных компонент, физических, функциональных и технологических связей как внутри ГИС, так и с другими системами различного уровня и назначения;

– определения режимов обработки информации в ГИС в целом и в ее отдельных компонентах;

– определения степени участия персонала в обработке информации ограниченного доступа, характер его взаимодействия между собой;

– определения уровня защищенности ГИС.

Предпроектное обследование проводилось путем:

– устного опроса лиц, ответственных за обработку информации ограниченного доступа;

– сбора информации о рабочих станциях, входящих в информационную систему, с использованием специального программного обеспечения;

– заполнения форм сбора информации об ГИС.

Общие сведения об учреждении:

1) Реквизиты учреждения:

– полное наименование – Челябинский центр ОВД филиала «Аэронавигация Урала» ФГУП «Госкорпорация по ОрВД»;

– адрес учреждения: г. Челябинск, Аэропорт, 2 этаж, кабинет № 202.

Расположение здания Уралаэронавигации относительно зданий других организаций указано на Рисунке 1.

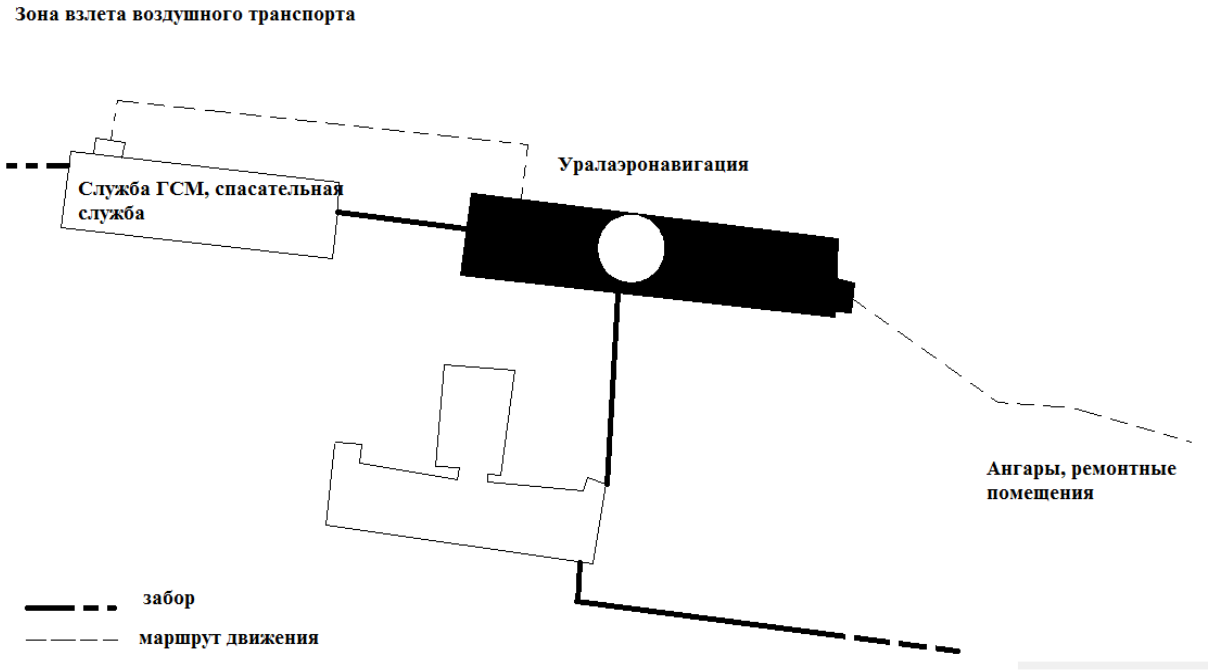

Рисунок 1 – положение здания Уралэронавигации

2) Ответственный за обеспечение безопасности информации ограниченного доступа: Олейников С.В., Главный инспектор по информационной безопасности и технической защите информации, администратор безопасности на ОИ: Родионов Д.А., Главный инженер.

Общая характеристика учреждения:

Челябинский центр ОВД филиала «Аэронавигация Урала» ФГУП «Госкорпорация по ОрВД» характеризуется проведением аэропортовой деятельности, связанной с обслуживанием воздушных судов, пассажиров и груза, деятельность по техническому обслуживанию воздушного движения.

Организационно-штатная структура Филиала «Аэронавигация Урала» ФГУП «Госкорпорация по ОрВД» представлена на Рисунке 2.

Рисунок 1 – Структура Челябинского филиала «Аэронавигация Урала»

*ОВД - Организация воздушного движения

ЭРТОС - Эксплуатации радиотехнического оборудования и связи

Сведения об АС:

– Территориальное размещение ГИС: объектовая ГИС в пределах одного здания, все компоненты находятся на территории РФ;

– Перечень информации ограниченного доступа:

1) перечень объектов РТОП и АЭС;

2) аэронавигационная информация (планируемое и фактическое движение ВС, маршруты и участки полетов);

3) справочные данные и метеорологическая информация;

4) нормативно-техническая баз;

5) анализ летно-технических характеристик ВС;

6) анализ хода процессов эксплуатации АТ и их результатов.

– Масштаб информационной системы: объектовый;

– Структура информационной системы: локальная вычислительная сеть;

– Наличие соединения с сетями общего пользования и международного информационного обмена (МИО): ГИС имеет соединение с сетями общего пользования;

– Режим обработки информации ограниченного доступа: многопользовательский, без разграничения прав доступа;

– Хранение информации ограниченного доступа: хранение информации ограниченного доступа осуществляется на НЖМД системного блока АРМ, а также на учтенных носителях информации;

– Информация о физической охране ГИС: в здании имеется пропускной режим, средства охранной и пожарной сигнализации.

2.2 Разработка программы и методики аттестационных испытаний

Программа и методика определяет цели, задачи, методы, условия, объем, порядок и методики проведения аттестационных испытаний автоматизированной системы – «Аэропорт» на соответствие требованиям по обеспечению безопасности конфиденциальной информации.

Аттестационная комиссия назначается генеральным директором из числа штатных сотрудников АО «Гранит Информ», лицензия на деятельность по технической защите конфиденциальной информации № 2125 от 29 октября 2013 г.

Целью аттестационных испытаний является комплексная проверка защищаемого объекта информатизации в реальных условиях эксплуатации с целью оценки соответствия применяемого комплекса мер и средств защиты требуемому уровню безопасности информации.

Испытания проводятся в эксплуатационных режимах работы объекта с использованием тестирующих программных средств, приведенных в Таблице 5.

В случае выявления по результатам испытаний несоответствия АС установленным требованиям по защите информации комиссия может рассмотреть предложения заявителя по оперативному устранению выявленных недостатков и нарушений. При этом могут рекомендоваться следующие меры:

– доработка организационно-распорядительной документации;

– снижение класса объекта информатизации;

– исключение отдельных средств из состава средств объекта информатизации;

– применение дополнительных организационно-технических мер защиты;

– применение дополнительных сертифицированных средств защиты информации.

Таблица 5 – Перечень программного обеспечения

Наименования средств измерений и вспомогательного оборудования	Тип	Заводской номер	Сертификат
Программа поиска и гарантированного уничтожения информации на дисках	«TERRIER» (версии 3.0)	Голограмма № А 293818	Сертификат ФСТЭК № 1193, действ. до 16.05.2018 г.
Программа фиксации и контроля исходного состояния программного комплекса	«ФИКС» (версия 2.0.1)	Голограмма № А 267757	Сертификат ФСТЭК № 913, действ. до 01.06.2019 г.
Средство создания модели системы разграничения доступа	«Ревизор 1 XP»	Голограмма № А 296220	Сертификат ФСТЭК № 989, действ. до 08.02.2017 г.
Программа контроля полномочий доступа к информационным ресурсам	«Ревизор 2 XP»	Голограмма № А 268720	Сертификат ФСТЭК № 990, действ. до 08.02.2017 г.

Методики аттестационных испытаний автоматизированной системы на соответствие требованиям безопасности информации включают в себя мероприятия, указанные в Таблице 6.

Таблица 6 – Мероприятия, определенные ПиМ

Мероприятие	Состав мероприятия
1	2
Анализ полноты исходных данных, проверка их соответствия реальным условиям размещения, монтажа и эксплуатации технических средств АС	Приведенный перечень исходных данных и документации может уточняться по результатам анализа и проверки, в зависимости от особенностей объекта информатизации, по согласованию с аттестационной комиссией
Исследование процесса обработки информации	Исследование технологического процесса обработки и хранения информации, анализ информационных потоков, определение состава использованных для обработки информации технических средств
Проверка состояния организации работ и выполнения организационно-технических требований по защите информации	- Проверка достаточности представленных документов и соответствия их содержания требованиям по безопасности информации; - Проверка правильности категорирования КИ и классификации ИС;

Продолжение Таблицы 6

1	2
Проверка состояния организации работ и выполнения организационно-технических требований по защите информации	- Проверка уровня подготовки кадров и распределения ответственности персонала; - Проверка наличия сертификатов соответствия на технические средства и средства защиты информации, экспертиза отчетов и протоколов по специальным исследованиям технических средств, предписаний на эксплуатацию технических средств; - Проверка выполнения требований к помещениям, в которых производится обработка информации
Производится проверка достаточности соответствия требованиям стандартов и иным руководящим документам на соответствие требованиям по защите информации от НСД	- Анализ и оценка технологического процесса обработки информации; - Выбор инструментальных средств и методики испытаний; - Испытания подсистемы управления доступом; - Испытания подсистемы регистрации и учета; - Испытания подсистемы обеспечения целостности; - Проверка наличия необходимых сертификатов; - Испытания подсистемы антивирусной защиты

2.3 Заключение договора на аттестацию

Заключение договора на аттестацию подразумевает под собой фиксирование между сторонами правил и соглашений о деятельности по аттестации.

АО «Гранит Информ» оказывает комплекс услуг:

– по проведению аттестационных испытаний объекта информатизации, а Заказчик оплачивает Исполнителю оказанные услуги в соответствии с условиями настоящего Договора;

– по разработке комплекта проектов документов на объект информатизации Заказчика.

Заказчик предоставляет Исполнителю необходимые для оказания услуг документы, обеспечивает доступ представителю Исполнителя на создаваемый объект информатизации, к необходимым средствам информатизации, схемам и документам.

Правомочность оказания услуг по настоящему Договору гарантируется Исполнителем наличием у него лицензии ФСТЭК России и Аттестата аккредитации.

Указывается стоимость проведения аттестационных испытаний с учетом спецификации, а также порядок проведения аттестационных испытаний, указанная в программе и методике аттестационных испытаний, которая должна быть предварительно согласована с Челябинским центром ОВД филиала «Аэронавигация Урала» ФГУП «Госкорпорация по ОрВД».

Фиксируются права и обязанности Сторон.

Заказчик обязан:

– Предоставить Исполнителю необходимые документы и доступ членов аттестационной комиссии на аттестуемый объект и к средствам информатизации;

– После получения «Аттестата соответствия» осуществлять эксплуатацию объекта информатизации в соответствии с условиями и требованиями, установленными в «Аттестате соответствия»;

– Извещать в письменной форме орган по аттестации, выдавший «Аттестат соответствия», обо всех изменениях на объекте информатизации, которые могут повлиять на эффективность мер и средств защиты информации (перечень характеристик, определяющих безопасность информации, приводится в «Аттестате соответствия»).

Исполнитель обязан:

– Оказать Заказчику услуги по проведению аттестационных испытаний объекта информатизации в точном соответствии с действующими нормативно-правовыми, техническими актами и условиями настоящего договора;

– В течение пяти рабочих дней после завершения аттестации независимо от результатов аттестационных испытаний стороны подписывают Акт сдачи - приемки услуг. В Акте стороны фиксируют результат проведенных аттестационных испытаний и факт выдачи (невыдачи) Аттестата соответствия.

За невыполнение или ненадлежащее выполнение обязательств по настоящему Договору Стороны несут ответственность в соответствии с действующим законодательством Российской Федерации.

Каждая Сторона по договору с момента подписания настоящего Договора несет ответственность за выполнение возложенных на нее функций, обеспечение сохран-

ности сведений, содержащихся в ГИС.

Отдельными пунктами вынесены форс-мажорные и особые обстоятельства, а также порядок разрешения споров.

2.4 Проведение аттестационных испытаний и оформление аттестационной документации

Аттестация проводится в соответствии с «Программой и методикой…», согласованной с Заказчиком.

Для проведения испытаний заявитель представляет аттестационной комиссии следующие исходные данные и документацию:

- технический паспорт на АС (в соответствии с приложением В СТР-К);
- акт присвоения класса защищенности информации;
- сертификаты соответствия требованиям по безопасности информации на программные и технические средства АС, используемые средства защиты;
- состав технических и программных средств, входящих в АС;
- планы размещения ОТСС и ВТСС;
- план контролируемой зоны;
- схемы прокладки линий передачи данных ОТСС и ВТСС;
- состав и схемы размещения средств защиты информации;
- организационно-распорядительную документацию разрешительной системы доступа персонала к защищаемым ресурсам АС;
- описание технологического процесса обработки информации;
- требования к системе защиты;
- технологические инструкции пользователям АС;
- инструкции по эксплуатации средств защиты информации;
- документы, регламентирующие порядок и правила парольной защиты, антивирусной защиты, восстановления конфиденциальной информации;
- данные по уровню подготовки кадров, обеспечивающих защиту информации.

Состав и размещение основных и вспомогательных технически средств приведены в техническом паспорте (Приложение 1).

Документом, необходимым для проведения аттестации является частная модель угроз безопасности информации при ее обработке в государственной информационной системе.

При определении угроз безопасности информации учитываются характеристики информационной системы, режимы обработки информации, а также иные характеристики информационной системы.

С применением Модели угроз решается задача разработки системы защиты ГИС, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты информации, предусмотренных для соответствующего класса защищенности.

Модель определяет угрозы безопасности персональных данных, обрабатываемых в государственной информационной системе «Аэропорт».

Потенциальную опасность безопасности данных при их обработке в ГИС представляют:

- несанкционированный доступ к данным, обрабатываемым в ГИС;
- утечка информации по техническим каналам;
- несанкционированный доступ к рабочим станциям пользователей;
- несанкционированный доступ к серверам;
- утечка данных с использованием внешних носителей информации;
- утечка данных по сетям связи общего пользования.

Уровень исходной защищенности ГИС определен экспертным методом. Результаты анализа исходной защищенности приведены в Таблице 7.

Таблица 7 – Результаты анализа

Технические и эксплуатационные характеристики ГИС	Уровень защищенности		
	Высокий	Средний	Низкий
1	2	3	4
1 По территориальному размещению:			
Локальная ГИС в пределах одного здания	+		
2 По наличию соединения с сетями общего пользования:			
ГИС с одноточечным выходом в сеть		+	

Продолжение Таблицы 7

1	2	3	4
3 По встроенным (легальным) операциям с записями баз ГИС:			
Запись, удаление, сортировка		+	
4 По разграничению доступа к ГИС:			
Определенный перечень сотрудников		+	
5 По наличию соединений с другими базами ГИС:			
С одной БД	+		
6 По уровню обработки данных:			
Не передаются в сторонние организации	+		
7 По объему данных, которые предоставляются сторонним пользователям ГИС без предварительной обработки:			
Предоставляется часть БД		+	
Характеристики ГИС	42,86%	57,14%	0%

Таким образом, ГИС имеет средний (Y_1=5) уровень исходной защищенности, т.к. не менее 70% характеристик ГИС соответствуют уровню защищенности не ниже «средний».

Определение актуальных угроз безопасности данных.

Частота реализации, опасность и актуальность угроз безопасности ГИС определена экспертным методом и на основании результатов обследования. Перечень актуальных угроз приведены в Таблице 8.

Таблица 8 – Актуальные угрозы

Наименование угрозы	Y2	Y	Возможность реализации угрозы	Опасность угрозы
Компьютерные вирусы	2	0,35	Средняя	Средняя
Несанкционированный доступ через сети международного обмена	2	0,35	Средняя	Средняя
Кража технических средств, носителей информации (в т.ч. сервера БД)	2	0,35	Средняя	Средняя
Порча или уничтожение технических средств, носителей информации	2	0,35	Средняя	Средняя
Внедрение по сети вредоносных программ	2	0,35	Средняя	Средняя

Была проведена проверка соответствия действительности класса защищенности объекта.

При вводе системы в эксплуатацию, комиссия, назначенная Начальником Челябинского центра ОВД филиала «Аэронавигация Урала» ФГУП «Госкорпора-ция по

ОрВД», провела работу по определению и присвоению класса защищенности государственной информационной системы «Аэропорт», расположенной по адресу: г. Челябинск, Аэропорт.

Рассмотрев исходные данные о государственной информационной системе, определила:

1) Масштаб информационной системы: объектовый (информационная система функционирует на объектах Челябинского центра ОВД филиала «Аэронавигация Урала» ФГУП «Госкорпорация по ОрВД» и не имеет сегментов в территориальных органах, представительствах, филиалах, подведомственных и иных организациях);

2) Степень ущерба от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности): низкая.

В соответствии с приказом ФСТЭК России № 17 от 11 февраля 2013 г. «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и на основании анализа исходных данных, комиссия решила:

Государственной информационной системе «Аэропорт» Челябинского центра ОВД филиала «Аэронавигация Урала» ФГУП «Госкорпорация по ОрВД» присвоить:

1) уровень значимости информации – УЗ 3;
2) класс защищенности информационной системы – К3.

Результаты отражены в Акте присвоения класса защищенности государственной информационной системы «Аэропорт».

Перечисленные выше актуальные угрозы нейтрализуются с помощью организационно-технических мер и использования средств защиты информации, сертифицированных на соответствия требованиям безопасности информации (Приложение 2).

На объект информатизации разработан технический паспорт, соответствующий требованиям приложения В СТР-К. Состав ОТСС и ВТСС, установленных на объекте, соответствует указанному в техническом паспорте.

В организации приняты меры по ограничению доступа посторонних лиц к техническим средствам обработки защищаемой информации. Визуальный просмотр обрабатываемой на объекте информации посторонними лицами невозможен. Окно помещения, в котором расположен объект информатизации, оборудовано шторами-жалюзи. Помещения, в которых установлены ОТСС и хранятся машинные носители информации, оборудованы надежными замками, используются технические средства охраны и сигнализации. Допуск посторонних лиц в помещение ограничен и без контроля невозможен.

Допуск сотрудников к обработке конфиденциальной информации обеспечивается в рамках действующей в организации разрешительной системы и в соответствии с возложенными на персонал функциями.

На объекте имеются инструкции, на основании которых осуществляется работа пользователей, администраторов и обслуживающего персонала. Имеется эксплуатационная документация на используемые средства защиты информации.

Используемые средства защиты информации позволяют выполнить требования по защите информации ограниченного доступа.

Требования руководящих документов по защите информации от несанкционированного доступа к классу защищенности ГИС «К3» в части подсистем управления доступом, регистрации событий, обеспечения целостности и антивирусной защите выполнены.

Сертификаты соответствия на используемые средства защиты информации подтверждают возможность использования СЗИ в ГИС класса защищенности «К3».

Выводы по второму разделу

В процессе аттестационных испытаний были проведены мероприятия организационно-технического характера, результаты зафиксированы в Заключении (Приложение 3), принято решение о возможности выдачи Аттестата соответствия (Приложение 4).

3 ВЫБОР СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

3.1 Общие положения

Одним из основным этапом проведения аттестации является проверка полноты и достаточности выбранных мер защиты информации. Все СЗИ, согласно Приказу ФСТЭК № 17 от 11 февраля 2013 г. имеют действующие сертификаты соответствия требованиям безопасности информации.

Технические меры защиты информации реализуются посредством применения средств защиты информации, в том числе программных (программно-аппаратных) средств, в которых они реализованы, имеющих необходимые функции безопасности. В данной информационной системе 3 класса защищенности применяются средства защиты информации 6 класса, а также средства вычислительной техники не ниже 5 класса. [7]

Выбор СЗИ проводился по нескольким параметрам: стоимость, простота в администрировании, популярность в использовании и иные.

3.2 Выбор средств защиты информации от несанкционированного доступа

В связи с наличием подтвержденной уязвимости в СЗИ от НСД Secret Net 5.1 (идентификатор уязвимости 2016-00436). Уязвимости присвоен средний уровень опасности, а ее описание включено в Банк данных угроз безопасности информации, размещенный на сайте bdu.fstec.ru.

ООО «Код Безопасности» прекратил техническую поддержку средств защиты информации Secret Net версии 5.1. Выпуск соответствующих обновлений для данных средств защиты информации не предусмотрен. [10] В связи с этим необходимо осуществить перевод информационной системы на иное сертифицированное средство защиты. Екатеринбургским зональным центром единой системы организации воздушного движения была произведена закупка СЗИ от НСД Secret Net 7 (сертификат соответствия ФСТЭК № 2707, действительный до 07.09.2018 года). В целях

унификации средств защиты данное программное обеспечение было внедрено в ГИС «Аэропорт».

3.3 Выбор антивирусной защиты

Выбор средства антивирусной защиты осуществлялся с учетом стоимости, наличию документации в открытом доступе, оперативно работающей технической поддержки и регулярности обновлений банка уязвимостей.

Выбор проводился из трех средств антивирусной защиты:

– Dr.Web Enterprise Security Suite (сертификат ФСТЭК № 3509, действительный до 27.01.2019 г.);

– Kaspersky Endpoint Security 10 для Windows (сертификат ФСТЭК № 3025, действительный до 25.11.2019 г.);

– ESET NOD32 Secure Enterprise Pack (версия 5.0) (сертификат ФСТЭК № 3243 действительный до 13.10.2017 г.).

Сравнительный анализ приведен в Таблице 9.

Таблица 9 – Сравнение СВАЗ

Наименование	Стоимость	Наличие документации и техподдержка	Регулярное обновление
Dr.Web Enterprise Security Suite	6 000 р.	+	+/-
Kaspersky Endpoint Security 10 для Windows	4 000 р.	+	+
ESET NOD32 Secure Enterprise Pack (версия 5.0)	7000 р.	+/-	-

Помимо вышеперечисленных критериев был рассмотрен факт совместимости со средством защиты он несанкционированного доступа, и на основании анализа САВЗ было выбрано средство антивирусной защиты «Kaspersky Endpoint Security 10 для Windows». Kaspersky Endpoint Security 10 обеспечивает комплексную защиту конечных точек от известных и новых угроз, сетевых и мошеннических атак и другой нежелательной информации.

Компоненты защиты:

– Файловый Антивирус;

– Мониторинг системы;
– Почтовый Антивирус;
– Веб-Антивирус;
– IM-Антивирус;
– Сетевой экран;
– Мониторинг сети;
– Защита от сетевых атак.

3.4 Выбор межсетевого экрана и средства криптографической защиты

На объекте информатизации установлен аппаратно-программный комплекс шифрования «Континент» Версия 3.7, действующие сертификаты которого приведены в Таблице 10. Установленное средство защиты удовлетворяет необходимым требованиям по защите информации и может использоваться на объекте информатизации.

Таблица 10

Назначение	Сертификат ФСТЭК	Сертификат ФСБ
Криптографическая защита информации, передаваемой по открытым каналам связи. Фильтрация принимаемых и передаваемых пакетов по различным критериям (адресам отправителя и получателя, протоколам, номерам портов, дополнительным полям пакетов и т.д.).	№ 3008 действителен до 01.11.2019 г.	№ СФ/124-2918 действителен до 07.07.2019 г.

Функции:

- Межсетевое экранирование;
- Создание VPN-каналов между сетями предприятия;
- Маршрутизация трафика: статическая, динамическая и Multicast.
- Обеспечение работы в режиме повышенной безопасности;
- Обеспечение отказоустойчивости.

Выводы по третьему разделу

После осуществления мониторинга СЗИ, имеющих сертификаты соответствия по требованиям безопасности информации, были выбраны средства, оптимально удовлетворяющие потребностям Челябинского центра ОВД филиала «Аэронавигация Урала» ФГУП «Госкорпорация по ОрВД».

4. БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ

4.1 Общие положения

При проведении аттестации сотрудникам АО «Гранит Информ» необходимо взаимодействовать с ПЭВМ для ввода, обработки, передачи и хранения информации о результатах аттестационных испытаний, что накладывает определенные требования к персональным компьютерам и помещениям в которых происходит работа с ПЭВМ: пожарные требования, требования к климату и требования при работе с электроаппаратурой.

В Российской Федерации, нормативно-правовыми актами, регулирующими данный вопрос, являются:

– «Трудовой кодекс Российской Федерации» № 197-ФЗ от 30.12.2001 г.,

– «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы» (СанПиН 2.2.2/2.4.1340-03),

– «Типовая инструкция по охране труда при работе на персональном компьютере» (ТОИ Р-45-084-01).

Государственными нормативными требованиями охраны труда устанавливаются правила, процедуры, критерии и нормативы, направленные на сохранение жизни и здоровья работников в процессе трудовой деятельности.

Статья 209 ТК РФ формулирует основные понятия, используемые при обеспечении охраны труда.

Охрана труда - система сохранения жизни и здоровья работников в процессе трудовой деятельности, включающая в себя правовые, социально-экономические, организационно-технические, санитарно-гигиенические, лечебно-профилактические, реабилитационные и иные мероприятия.

Условия труда - совокупность факторов производственной среды и трудового процесса, оказывающих влияние на работоспособность и здоровье работника.

Безопасные условия труда - условия труда, при которых воздействие на работающих вредных и (или) опасных производственных факторов исключено либо

уровни их воздействия не превышают установленных нормативов.

Рабочее место - место, где работник должен находиться или куда ему необходимо прибыть в связи с его работой и которое прямо или косвенно находится под контролем работодателя.

Требования охраны труда - государственные нормативные требования охраны труда, в том числе стандарты безопасности труда, а также требования охраны труда, установленные правилами и инструкциями по охране труда.

Для доведения до сведения требований по охране труда все работники обязаны проходить обучение по охране труда и проверку знания требований охраны труда. Для всех поступающих на работу лиц, а также для работников, переводимых на другую работу, должен быть проведен инструктаж по охране труда, а также организовано обучение безопасным методам и приемам выполнения работ и оказания первой помощи пострадавшим.

Предусмотрены пять видов инструктажей (вводный, первичный, повторный, внеплановый и целевой) которые формулируют требования и порядок действия работника для обеспечения безопасного труда. В общем случае работник обязан:

– Выполнять только ту работу, которая определена его должностной инструкцией;

– Содержать в чистоте рабочее место;

– Соблюдать режим труда и отдыха в зависимости от продолжительности, вида и категории трудовой деятельности (Таблица 11);

– Соблюдать меры пожарной безопасности.

При работе с ПЭВМ в целях осуществления аттестационной деятельности категория трудовой деятельности соответствует категории «1а».

Риск – вероятность причинения вреда жизни или здоровью граждан, имуществу физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде, жизни или здоровью животных и растений с учетом тяжести этого вреда [20].

Вредный производственный фактор - производственный фактор, воздействие которого на работника может привести к его заболеванию.

Опасный производственный фактор - производственный фактор, воздействие которого на работника может привести к его травме. [16]

Таблица 11 – Время регламентированных перерывов при работе с ПЭВМ

Категория работы с ПЭВМ	Уровень нагрузки за рабочую смену при видах работы с ПЭВМ по группам			Суммарное время регламентированных перерывов, мин	
	А количество знаков	Б количество знаков	В часов	при 8-часовой смене	при 12-часовой смене
I	до 20 000	до 15 000	до 2,0	30	70
II	до 40 000	до 30 000	до 4,0	50	90
III	до 60 000	до 40 000	до 6,0	70	120

Вредными факторами могут быть:

– физические факторы - температура, влажность, скорость движения воздуха, тепловое излучение, электромагнитные поля (ЭМП) и излучения, производственный шум, вибрация, аэрозоли, освещение - естественное, искусственное;

– химические факторы - химические вещества, смеси;

– биологические факторы - микроорганизмы, живые клетки и споры;

– факторы трудового процесса. [21]

При эксплуатации персонального компьютера на работника могут оказывать действие следующие опасные и вредные производственные факторы:

– повышенное значение напряжения в электрической сети, замыкание которой может привести к поражению электрическим током;

– повышенный уровень напряженности электромагнитного поля;

– пониженный или повышенный уровень освещенности;

– не соответствующие нормам параметры микроклимата;

– повышенный уровень шума. [19]

4.2. Требования к помещениям для работы с ПЭВМ

Перечень продукции и контролируемых гигиенических параметров вредных и опасных факторов представлены в Таблице 12.

Временные допустимые уровни электромагнитных полей, создаваемых ПЭВМ,

а также допустимые визуальные параметры устройств отображения информации не должны превышать значений, указанных в СанПиН 2.2.2/2.4.1340-03.

Таблица 12 – Используемая продукция при аттестации

Вид продукции	Код ОКП	Контролируемые гигиенические параметры
Машины вычислительные электронные цифровые, машины вычислительные электронные цифровые персональные (включая портативные ЭВМ)	40 1300	Уровни электромагнитных полей (ЭМП), акустического шума, концентрация вредных веществ в воздухе, визуальные показатели ВДТ
Устройства периферийные: принтеры, сканеры, модемы, сетевые устройства, блоки бесперебойного питания и т.д.	40 3000	Уровни ЭМП, акустического шума, концентрация вредных веществ в воздухе
Устройства отображения информации	40 3200	Уровни ЭМП, визуальные показатели, концентрация вредных веществ в воздухе

Временные допустимые уровни электромагнитных полей, создаваемых ПЭВМ, а также допустимые визуальные параметры устройств отображения информации не должны превышать значений, указанных в СанПиН 2.2.2/2.4.1340-03.

При размещении рабочих мест с ПЭВМ расстояние между рабочими столами с видеомониторами (в направлении тыла поверхности одного видеомонитора и экрана другого видеомонитора), должно быть не менее 2,0 м, а расстояние между боковыми поверхностями видеомониторов – не менее 1,2 м. [22]

Рабочая мебель для пользователей компьютерной техникой должна отвечать следующим требованиям:

– высота рабочей поверхности стола должна регулироваться в пределах 680 - 800 мм; при отсутствии такой возможности высота рабочей поверхности стола должна составлять 725 мм;

– рабочий стол должен иметь пространство для ног высотой не менее 600 мм, глубиной на уровне колен не менее 450 мм и на уровне вытянутых ног не менее 650 мм;

– рабочий стул (кресло) должен быть подъемно - поворотным и регулируемым по высоте и углам наклона сиденья и спинки, а также - расстоянию спинки от переднего края сиденья;

– рабочее место должно быть оборудовано подставкой для ног, имеющей ширину не менее 300 мм, глубину не менее 400 мм, регулировку по высоте в пределах до 150 мм и по углу наклона опорной поверхности подставки до 20 градусов; поверхность подставки должна быть рифленой и иметь по переднему краю бортик высотой 10 мм. [18]

Экран монитора находиться от глаз пользователя на расстоянии 600-700 мм, но не ближе 500 мм с учетом размеров алфавитно-цифровых знаков и символов.

Площадь на одно рабочее место пользователей ПЭВМ должна составлять не менее 4,5 м^2.

Клавиатуру следует располагать на поверхности стола на расстоянии 100 - 300 мм от края, обращенного к пользователю, или на специальной регулируемой по высоте рабочей поверхности, отделенной от основной столешницы. [22]

Естественное и искусственное освещение должно соответствовать требованиям действующей нормативной документации. Окна в помещениях, где эксплуатируется вычислительная техника, преимущественно должны быть ориентированы на север и северо-восток.

Оконные проемы должны быть оборудованы регулируемыми устройствами типа: жалюзи, занавесей, внешних козырьков и др.

Для внутренней отделки интерьера помещений, где расположены ПЭВМ, должны использоваться диффузно отражающие материалы с коэффициентом отражения для потолка – 0,7-0,8; для стен – 0,5-0,6; для пола – 0,3-0,5.

Помещения, где размещаются рабочие места с ПЭВМ, должны быть оборудованы защитным заземлением (занулением) в соответствии с техническими требованиями по эксплуатации.

4.3. Требования к микроклимату, уровню шума и освещению

В производственных помещениях должны обеспечиваться оптимальные параметры микроклимата в соответствии с нормативами микроклимата производственных помещений (СанПиН 2.2.4.3359-16).

Показателями, характеризующими микроклимат в производственных помещениях, являются:

1) температура воздуха;

2) температура поверхностей;

3) относительная влажность воздуха;

4) скорость движения воздуха;

5) интенсивность теплового облучения.

Оптимальные величины параметров микроклимата на рабочих местах применительно к выполнению работ категории 1а в холодный и теплый периоды года приведены в Таблице 13. [23] В помещениях, оборудованных ПЭВМ, проводится ежедневная влажная уборка и систематическое проветривание после каждого часа работы на ПЭВМ. [22]

Таблица 13 – Оптимальные величины параметров микроклимата

Период года	Температура воздуха, ^{0}C	Температура поверхностей, ^{0}C	Относительная влажность воздуха, %	Скорость движения воздуха, м/с, не более
Холодный	22-24	21-25	60-40	0,1
Теплый	23-25	22-26	60-40	0,1

По характеру спектра шума выделяют:

1) тональный шум;

2) широкополосный шум, не содержащий выраженных тонов.

По временным характеристикам шума выделяют:

1) постоянный шум;

2) непостоянный шум, уровень звука которого за 8-часовой рабочий день изменяется более чем на 5 дБА;

3) импульсный шум. [23]

Основными источниками шума в помещениях, оборудованных вычислительной техникой, являются принтеры, плоттеры, копировальные аппараты и оборудование для кондиционирования воздуха, вентиляторы систем охлаждения, трансформаторы.

Нормативным эквивалентным уровнем звука на рабочих местах, согласно СанПиН 2.2.4.3359-16, является 80 дБА. [23]

Рабочие места, оборудованные ПЭВМ, должны быть обеспечены как искусственным, так и естественным светом.

Рабочие столы следует размещать таким образом, чтобы мониторы ПЭВМ были ориентированы боковой стороной к световым проемам, а естественный свет падал преимущественно слева.

Искусственное освещение в помещениях для эксплуатации ПЭВМ для проведения работ по аттестации должно осуществляться системой комбинированного освещения (к общему освещению дополнительно устанавливаются светильники местного освещения, предназначенные для освещения зоны расположения документов).

Освещенность на поверхности стола в зоне размещения рабочего документа должна быть 300-500 лк. Освещение не должно создавать бликов на поверхности экрана. Освещенность поверхности экрана не должна быть более 300 лк.

Следует ограничивать прямую блёскость от источников освещения (не более 200 кд/м^2), а также отраженную блёскость на рабочих поверхностях (не более 40 кд/м^2). Яркость потолка не должна превышать 200 кд/м^2.

Яркость светильников общего освещения должна составлять не более 200 кд/м^2, защитный угол светильников должен быть не менее 40^0.

Применение светильников без рассеивателей и экранирующих решеток не допускается.

Общее освещение при использовании люминесцентных светильников следует выполнять в виде сплошных или прерывистых линий светильников, расположенных сбоку от рабочих мест, параллельно линии зрения пользователя при рядном расположении мониторов. При периметральном расположении компьютеров линии светильников должны располагаться локализовано над рабочим столом ближе к его переднему краю, обращенному к оператору.

Для обеспечения нормируемых значений освещенности в помещениях для использования ПЭВМ следует проводить чистку стекол оконных рам и светильников не реже двух раз в год и проводить своевременную замену перегоревших ламп. [22]

4.4. Обеспечение пожарной и электробезопасности

Степень опасного и вредного воздействия на человека электрического тока, электрической дуги и электромагнитных полей зависит от:

– рода и величины напряжения и тока;

– частоты электрического тока;

– пути тока через тело человека;

– продолжительности воздействия электрического тока или электромагнитного поля на организм человека;

– условий внешней среды.

Электробезопасность должна обеспечиваться:

– конструкцией электроустановок;

– техническими способами и средствами защиты;

– организационными и техническими мероприятиями.

Электроустановки и их части должны быть выполнены таким образом, чтобы работающие не подвергались опасным и вредным воздействиям электрического тока и электромагнитных полей, и соответствовать требованиям электробезопасности.

Для обеспечения защиты от случайного прикосновения к токоведущим частям необходимо применять следующие способы и средства:

– защитные оболочки;

– защитные ограждения (временные или стационарные);

– защитные барьеры;

– безопасное расположение токоведущих частей;

– изоляция токоведущих частей (основная, дополнительная, усиленная, двойная);

– изоляция рабочего места;

– малое напряжение;

– защитное отключение;

– электрическое разделение;

– предупредительная сигнализация, блокировки, знаки безопасности.

Технические способы и средства применяют раздельно или в сочетании друг с другом так, чтобы обеспечивалась оптимальная защита при нормальном функционировании электроустановок и при возникновении аварийных ситуаций. [24]

Сформулирован ряд требований к работе за ПЭВМ с целью обеспечения электробезопасности.

Пред началом работ:

– Проверить правильность подключения оборудования к электросети.

– Проверить исправность проводов питания и отсутствие оголенных участков проводов.

– Убедиться в наличии заземления системного блока, монитора и защитного экрана.

– Протереть антистатической салфеткой поверхность экрана монитора и защитного экрана.

Во время работы запрещается:

– прикасаться к задней панели системного блока (процессора) при включенном питании;

– переключать разъемы интерфейсных кабелей периферийных устройств при включенном питании;

– допускать попадание влаги на поверхность системного блока (процессора), монитора, рабочую поверхность клавиатуры, дисководов, принтеров и других устройств;

– производить самостоятельное вскрытие и ремонт оборудования;

– работать на компьютере при снятых кожухах;

– отключать оборудование от электросети и выдергивать электровилку, держась за шнур.

Требования безопасности в аварийных ситуациях:

– Во всех случаях обрыва проводов питания, неисправности заземления и других повреждений, появления гари, немедленно отключить питание и сообщить об аварийной ситуации руководителю.

– Не приступать к работе до устранения неисправностей.

– При получении травм или внезапном заболевании немедленно известить своего руководителя, организовать первую доврачебную помощь или вызвать скорую медицинскую помощь. [18]

Помещение, в котором располагается ПЭВМ, должно иметь систему обеспечения пожарной безопасности с целью предотвращение пожара, обеспечения безопасности людей и защиты имущества при пожаре.

Возможными классам пожаров при работе с ПЭВМ могут быть:

– А – пожары твердых горючих веществ и материалов (огнетушащие вещества: вода, пена, порошок, углекислота);

– В – пожары горючих жидкостей или плавящихся твердых веществ и материалов (пена, порошок, асбестовое полотно, песок, огнетушащие составы на основе фтора и брома для ингибирования);

– Е – пожары горючих веществ и материалов электроустановок, находящихся под напряжением (углекислота, хладон, порошки, вода и пена, если оборудование обесточено);

К опасным факторам пожара, воздействующим на людей и имущество, относятся:

– пламя и искры;

– тепловой поток;

– повышенная температура окружающей среды;

– повышенная концентрация токсичных продуктов горения и термического разложения;

– пониженная концентрация кислорода;

– снижение видимости в дыму.

Защита людей и имущества от воздействия опасных факторов пожара и (или) ограничение последствий их воздействия обеспечиваются одним или несколькими из следующих способов:

1) применение объемно-планировочных решений и средств, обеспечивающих ограничение распространения пожара за пределы очага;

2) устройство эвакуационных путей, удовлетворяющих требованиям безопасной эвакуации людей при пожаре;

3) устройство систем обнаружения пожара (установок и систем пожарной сигнализации), оповещения и управления эвакуацией людей при пожаре;

4) применение систем коллективной защиты (в том числе противодымной) и средств индивидуальной защиты людей от воздействия опасных факторов пожара;

5) применение огнестойких строительных конструкций;

6) применение огнезащитных составов;

7) применение первичных средств пожаротушения;

8) применение автоматических и (или) автономных установок пожаротушения;

9) организация деятельности подразделений пожарной охраны. [10]

Выводы по четвертому разделу

В данном разделе были рассмотрены вредные производственные факторы, которые могут стать угрозой безопасности проведения работ по аттестации объектов информатизации сотрудниками АО «Гранит Информ». Для данных факторов были приведены допустимые значения, установленные нормами СанПин, а также меры по снижению негативного влияния вредных факторов на организм человека.

ЗАКЛЮЧЕНИЕ

В данной работе было освещено понятие аттестации объектов информатизации, ее место в системе обеспечения информационной безопасности автоматизированных систем, а также особенности проведения аттестационных испытаний в государственных информационных системах.

Проведена аттестация государственной информационной системы «Аэропорт» Челябинского центра ОВД филиала «Аэронавигация Урала» ФГУП «Госкорпорация по ОрВД». Были реализованы следующие этапы аттестационной деятельности:

– Составление заявки на аттестацию и предварительное ознакомление с аттестуемым объектом;

– Разработка программы и методики аттестационных испытаний;

– Заключение договора на аттестацию;

– Проведение аттестационных испытаний и оформление аттестационной документации.

Был произведен выбор средств защиты информации: от несанкционированного доступа, средство антивирусной защиты и межсетевой экран. Также были рассмотрены вредные производственные факторы, оказывающие влияние на организм человека при проведении аттестации.

Данная работа была практически реализована на базе АО «Гранит Информ», имеющего лицензию на осуществление аттестационной деятельности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1) Об утверждении Доктрины информационной безопасности Российской Федерации [Текст] : указ Президента РФ от 5 декабря 2016 г. № 646 // Собрание законодательства РФ – 2016. – № 50. – ст. 7074.

2) Об информации, информационных технологиях и о защите информации [Текст] : федер. закон от 27.07.2006 № 149-ФЗ // Собрание законодательства РФ – 2006. – № 31 (1 ч.). – ст. 3448.

3) Положение по аттестации объектов информатизации по требованиям безопасности информации [Электронный ресурс] : утв. Гостехкомиссией РФ 25.11.1994 г. // ФСТЭК России. – http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/112-polozheniya/375-polozhenie-ot-25-noyabrya-1994-g.

4) ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. – М.: Стандартинформ, 2008. – 7 с.

5) Остапенко В.С. Информационная безопасность региональных органов исполнительной власти / В.С. Остапенко //Государственное и муниципальное управление. Ученые записки СКАГС. – 2009. – № 1. – С. 160-169.

6) Асташова, Г.В. Дидактические условия интенсификации процесса обучения авиадиспетчеров профессионально-ориентированному английскому языку : дис…. канд. пед. наук / Г.В. Асташова. – М., 2001. – 232 с.

7) Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах [Текст] : приказ ФСТЭК России от 11.02.2013 г. № 17 // Российская газета. - 2013. - 26 июня. - С. 10.

8) ГОСТ Р 53622-2009 Информационные технологии (ИТ). Информационно-вычислительные системы. Стадии и этапы жизненного цикла, виды и комплектность документов. – М.: Стандартинформ, 2011. – 7 с.

9) Березов, А.А. Аттестация информационных систем. Понятие. Назначение. Процесс. Проблемы / А.А. Берёзов // ООО «Информационный центр». – http://www.ic-dv.ru/files/News/sem/Sem18_06_2015/8.pdf.

10) Методический документ. Меры защиты информации в государственных информационных системах [Электронный ресурс] : утв. ФСТЭК России 11.02.2014 г. // ФСТЭК России. – http:// http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/805-metodicheskij-dokument.

11) Вопросы Федеральной службы по техническому и экспортному контролю (Выписка) [Текст] : указ Президента РФ от 16.08.2004 г. № 1085 // Собрание законодательства РФ. – 2004. – № 34. – ст. 3541.

12) О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена [Текст] : указ Президента РФ от 17.03.2008 г. № 351 // Собрание законодательства РФ. – 2008. - №12. – ст. 1110.

13) Об утверждении Положения о Министерстве транспорта Российской Федерации [Текст] : постановление правительства Рос. Федерации от 30.07.2004 г. № 395 // Собрание законодательства РФ. – 2004. - № 32. – ст. 3342.

14) Лукацкий, А.В. Что такое государственная информационная система? – https://www.slideshare.net/CiscoRu/what-is-gis-43818277?next_slideshow=1.

15) Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения [Электронный ресурс] : утв. Гостехкомиссией РФ 30.03.1992 г. // ФСТЭК России. – http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/386-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g3.

16) Трудовой кодекс Российской Федерации [Текст] : федер. конституц. закон от 30.12.2001 № 197-ФЗ // Собрание законодательства РФ – 2002. – № 1 (1 ч.). – ст. 3.

17) Об утверждении Типового положения о системе управления охраной труда [Текст] : приказ М-ва труда Рос. Федерации от 19.08.2016 г. № 438н // Рос. газ. - 2016. - 01 ноября.

18) ТОИ Р-45-084-01. Типовая инструкция по охране труда при работе на персональном компьютере [Текст] : утв. приказом Минсвязи РФ от 02.07.2001 г. № 162 // Консультант Плюс. – http://www.consultant.ru/document/cons_doc_LAW_79762/

19) РД 153-34.0-03.298-2001. Типовая инструкция по охране труда для пользователей ПЭВМ в электроэнергетике [Текст] : утв. М-во энергетики РФ 17.05.2001 г. // Издательство НЦ ЭНАС. – 2002.

20) О техническом регулировании [Текст] : федер. закон от 27.12.2002 г. № 184-ФЗ // Собр. законодательства РФ. - 2002. - № 52 (ч. 1). - ст. 5140.

21) Р 2.2.2006-05.2.2. Гигиена труда. Руководство по гигиенической оценке факторов рабочей среды и трудового процесса. Критерии и классификация условий труда [Текст] : утв. Главным государственным санитарным врачом РФ 29.07.2005 г. // Бюллетень нормативных и методических документов Госсанэпиднадзора. – 2005. - № 3.

22) СанПиН 2.2.2/2.4.1340-03. Гигиенические требования к персональным электронно-вычислительным машинам и организации работы: санитар.-эпидемиол. правила и нормативы : утв. 24.07.03 : введ. в д. 30.07.03. – Москва : [б. и.], 2003. – 24 с.

23) СанПиН 2.2.4.3359-16. Санитарно-эпидемиологические требования к физическим факторам на рабочих местах: санитар.-эпидемиол. правила и нормативы : утв. 21.06.16 : введ. в д. 01.01.17. – Москва : [б. и.], 2016. – 24 с.

24) ГОСТ Р 12.1.019-2009 Система стандартов безопасности труда (ССБТ). Электробезопасность. Общие требования и номенклатура видов защиты. – М.: Стандартинформ, 2010. – 27 с.

25) Технический регламент о требованиях пожарной безопасности [Текст] : федер. закон от 22.07.2008 г. № 123-ФЗ // Собр. законодательства РФ. - 2008. - № 30 (ч. 1). - ст. 3579.

26) ФГУП «Государственная корпорация по организации воздушного движения в Российской Федерации». – https://gkovd.ru/.

27) О внесении изменений в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных

системах, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. N 17 [Электронный ресурс] : приказ ФСТЭК России от 15.02.2017 г. № 27 // ФСТЭК России. – http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/110-prikazy/1268-prikaz-fstek-rossii-15-fevralya-2017-g-n-27

28) ГОСТ 34.601-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания. – М.: Стандартинформ, 2009. – 5 с.

29) Информационное сообщение об уязвимостях в сертифицированных средствах защиты информации Secret Net и мерах по их нейтрализации. – http://fstec.ru/normotvorcheskaya/informatsionnye-i-analiticheskie-materialy/1136-informatsionnoe-soobshchenie-fstek-rossii-ot-12-aprelya-2016-g-240-24-1649.

ПРИЛОЖЕНИЯ

ПРИЛОЖЕНИЕ А
Технический паспорт

УТВЕРЖДАЮ
Начальник Челябинского центра ОВД
филиала «Аэронавигация Урала»
ФГУП «Госкорпорация по ОрВД»
_____ В.П. Ковалев
«_____»_____ 2017 г.

ТЕХНИЧЕСКИЙ ПАСПОРТ
на объект информатизации
«Аэропорт»
Челябинского центра ОВД филиала «Аэронавигация Урала»
ФГУП «Госкорпорация по ОрВД»

СОСТАВИЛ
Техник АО «Гранит Информ»
_____ Л.О. Овчинникова
«____» _____ 2017 г.

2017 г.

УСЛОВНЫЕ СОКРАЩЕНИЯ:

ОТСС – основные технические средства и системы;
АС – автоматизированная система;
ВТСС – вспомогательные технические средства и системы;
АРМ – автоматизированное рабочее место;
ЛВС – локальная вычислительная сеть;
ПО – программное обеспечение;
ВТ – вычислительная техника;

1 ОБЩИЕ СВЕДЕНИЯ ОБ ОБЪЕКТЕ

1.1 Наименование объекта: «Аэропорт» Челябинского центра ОВД «Аэронавигация Урала» ФГУП «Госкорпорация по ОрВД».

1.2 Расположение объекта: г. Челябинск, Аэропорт, второй этаж здания УралАэронавигации, кабинет № 202.

1.3 Классификация объекта.

Класс защищенности государственной информационной системы – «К3».

2 СОСТАВ ОБОРУДОВАНИЯ ОБЪЕКТА

2.1 Состав основных технических средств и систем (ОТСС) объекта информатизации отражен в таблице 2.1.

Таблица 2.1 - **Перечень ОТСС, входящих в состав ОИ «Аэропорт»**

№	Тип	Модель	Заводской / инвентаризационный номер
АРМ 1			
	Системный блок	InWin	инв. № 01010400779
	НЖМД	ST500DM002-1BD142	Z3TA3B6B
	Монитор	ViewSonic	S72103502117, инв. № 0000773
	Клавиатура	Genius KB-200	XECC04004974
	Мышь	Genius NetScroll 110X	X81145402338
	Принтер	HP LaserJet 1020	CNC9402074, инв. № 000.011101040000581
	Флешкарта	Transcend TS4GJF500 USB2 4Gb	инв. № 11013400017
АРМ 2			
	Системный блок	InWin	инв. № 1010400728
	НЖМД	ST500DM002-1BD142	Z3T35TM1
	Монитор	Acer V193	ETLHW0016623416DBC8504
	Клавиатура	Microsoft Basic Keyboard 1.0A	6968200981240
	Компьютерные колонки	Genius SP-G16	KA10057342
	Мышь	Oklick 105M	612852
	Принтер	Samsung ML-3310ND	Z5TPBUGBC00618L
	Флешкарта	Transcend TS4GJF500 USB2 4Gb	инв. № 11013400016
	ИБП	APC Back-UPS CS500	4B1223P48041, инв. № 1101040752
Сервер			
	Системный блок	Kraftway Express 200ED12	0010192060, инв. № 0040000334
	НЖМД	WDC WD3200JS-00P	0M21
	Монитор	Samsung SyncMaster 740N	344.011101040000334
	Клавиатура	Genius KB-110X	XP128S891287
	Мышь	Genius NetScroll 110X	X75892508894
	Флешкарта	Transcend TS4GJF500 USB2 4Gb	инв. № 1101340000012
	Коммутатор	D-Link DES-1005D	DL1E179000427

2.2 Состав вспомогательных технических средств и систем (ВТСС) объекта, установленных в помещении объекта информатизации отражен в таблице 2.2.

Таблица 2.2 – **Перечень ВТСС ОИ «Аэропорт»**

№	Тип	Модель	Заводской номер
1	Магнитофон	LG CD-321AX	б/н
2	Телефон	Panasonic KX-TS2350RUB	1DBKH219024
3	Телефон	Panasonic KX-TS2350RUW	7GPFD948672
4	Телефон	Panasonic KX-TS2350RUW	0FUKF039138
5	Кулер	AquaWell BH-YLR-QK	BH201408013171
6	Часы кварцевые	ANLIDA	инв. № 00671
7	Лампа светодиодная потолочная	Ledel	б/н
8	Люстра потолочная	б/н	б/н
9	Датчик пожарный	ИП 212-45	инв. № 000781
10	Датчик пожарный	ИП 212-45	инв. № 1034684
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			
25			
26			
27			
28			

2.3 Схема размещения и расположения ОТСС на объекте с привязкой к границам контролируемой зоны.

Структура, топология и размещение ОТСС и ВТСС объекта относительно границ контролируемой зоны объекта приведены на рисунках 2.1 – 2.3.

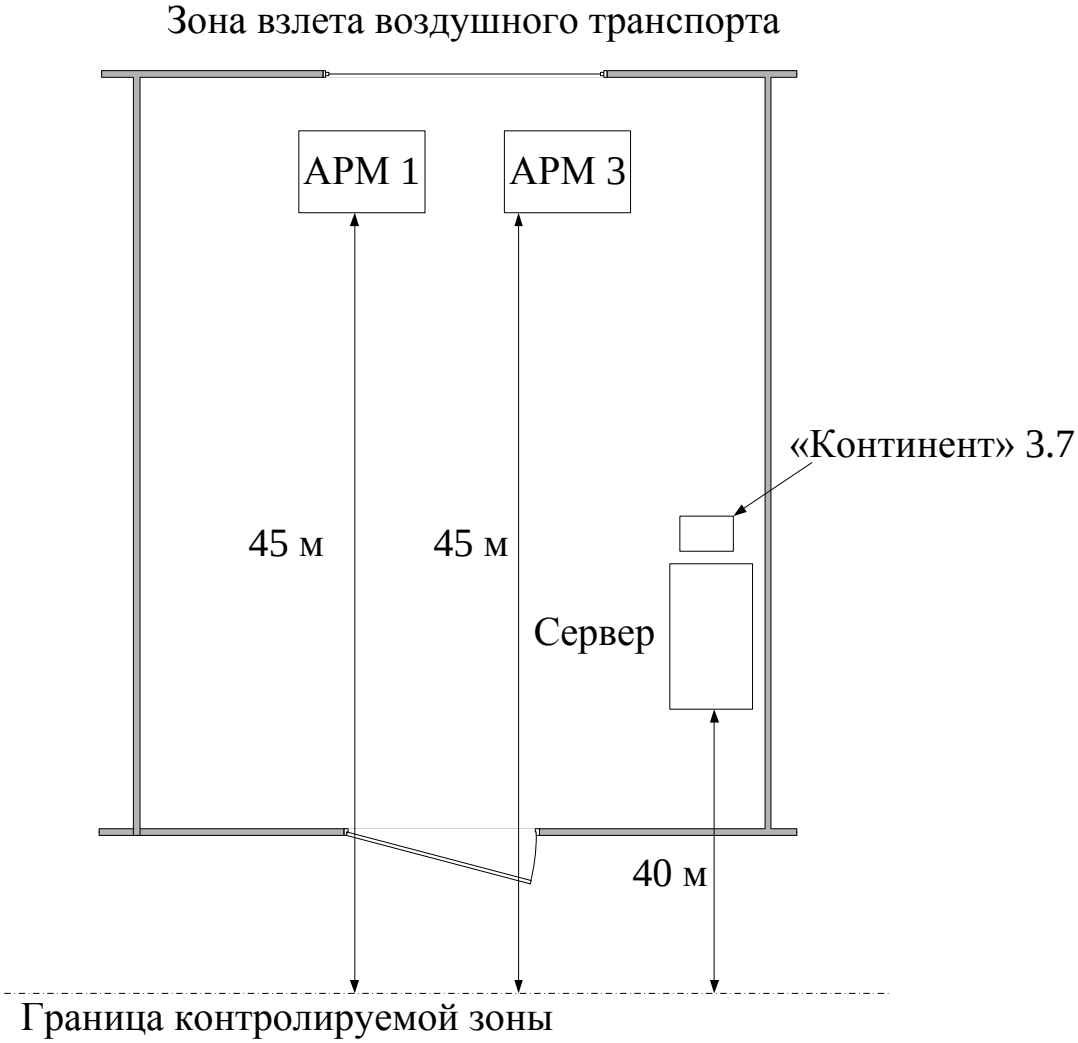

Рисунок 2.1 – Размещение ОТСС и средства защиты информации «Аэропорт»

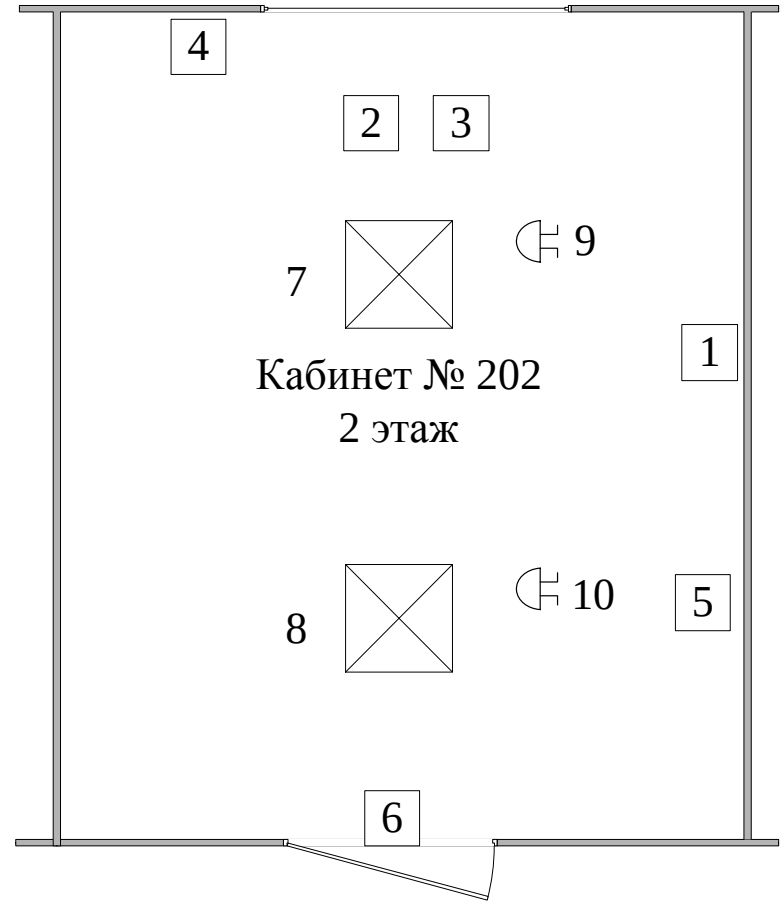

Рисунок 2.2 – Размещение ВТСС «Аэропорт»
*Примечание: Обозначения 1-10 приведены в Таблице 2.2 основной части технического паспорта.

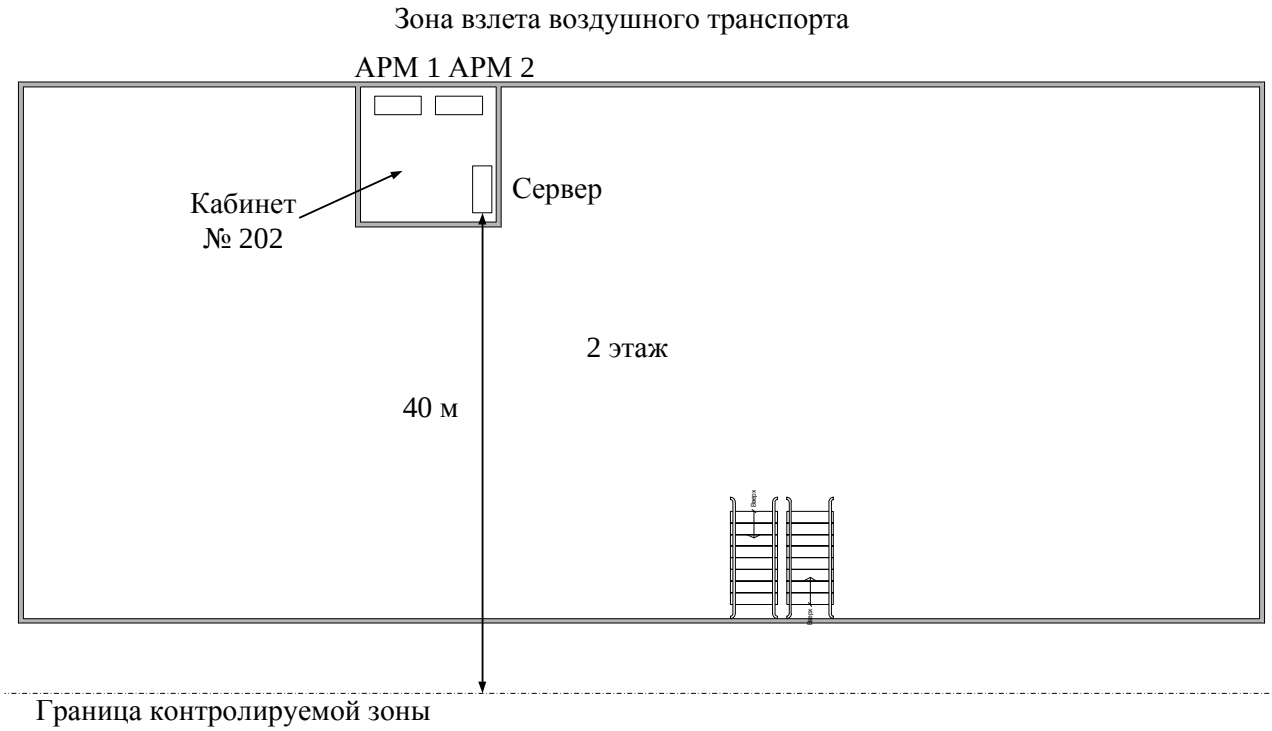

Рисунок 2.3 – Размещение ОТСС относительно границ контролируемой зоны

Контролируемой зоной является охраняемая территория Челябинского центра ОВД «Аэронавигация Урала» ФГУП «Госкорпорация по ОрВД». Граница контролируемой зоны определена приказом «Об определении границ контролируемой зоны Челябинского центра ОВД «Аэронавигация Урала» ФГУП «Госкорпорация по ОрВД».

Минимальное расстояние от ОТСС до КЗ составляет 40 метров.

2.5 Размещение ВТСС, линий приведено на рисунке 2.4.

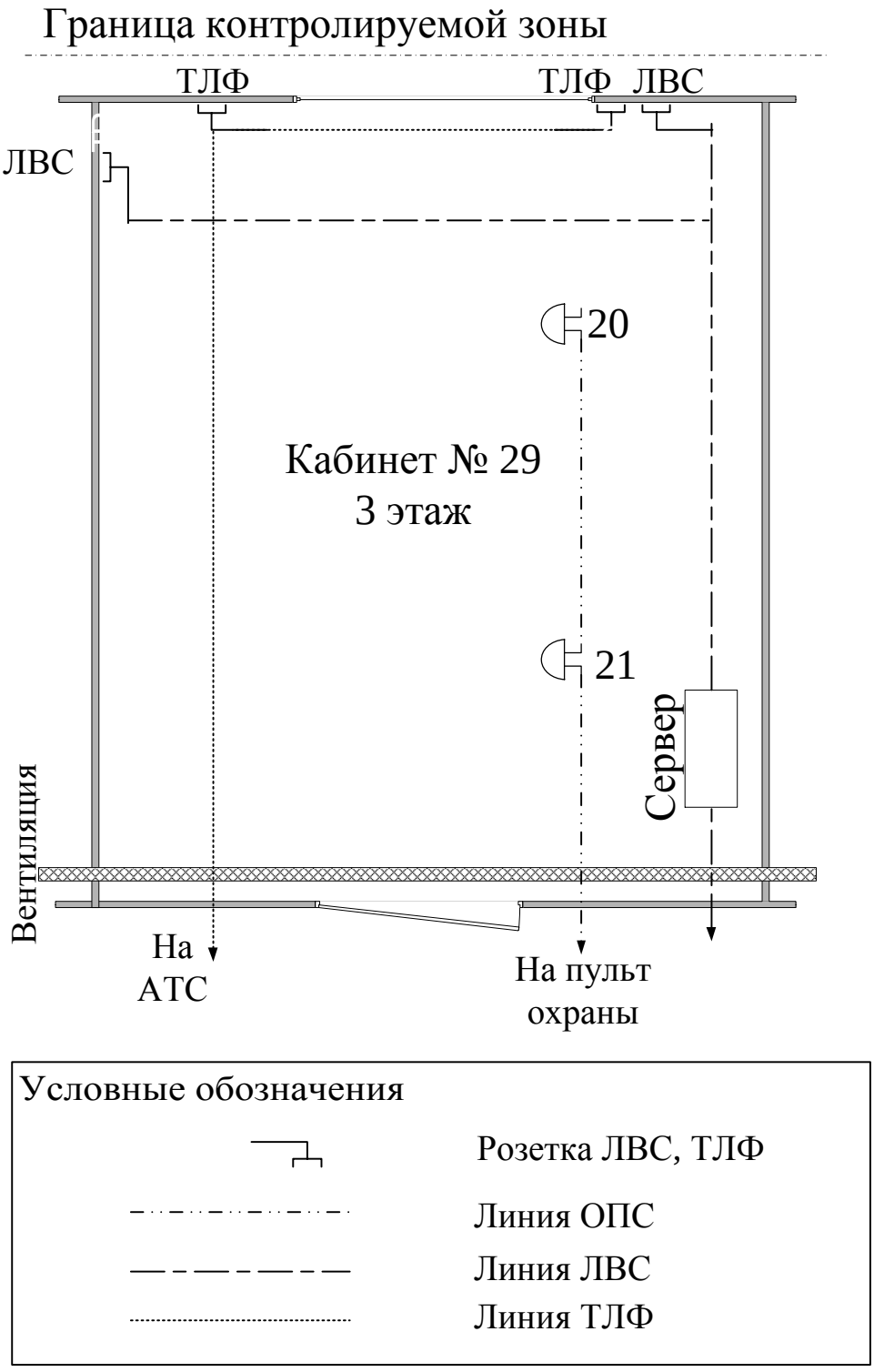

Рисунок 2.4 – Размещение ВТСС, расположение линий

*Примечание: Обозначения 20-21 приведены в Таблице 2.2 основной части технического паспорта

2.6 Размещение системы электропитания, заземления и инженерных коммуникаций приведено на рисунке 2.5.

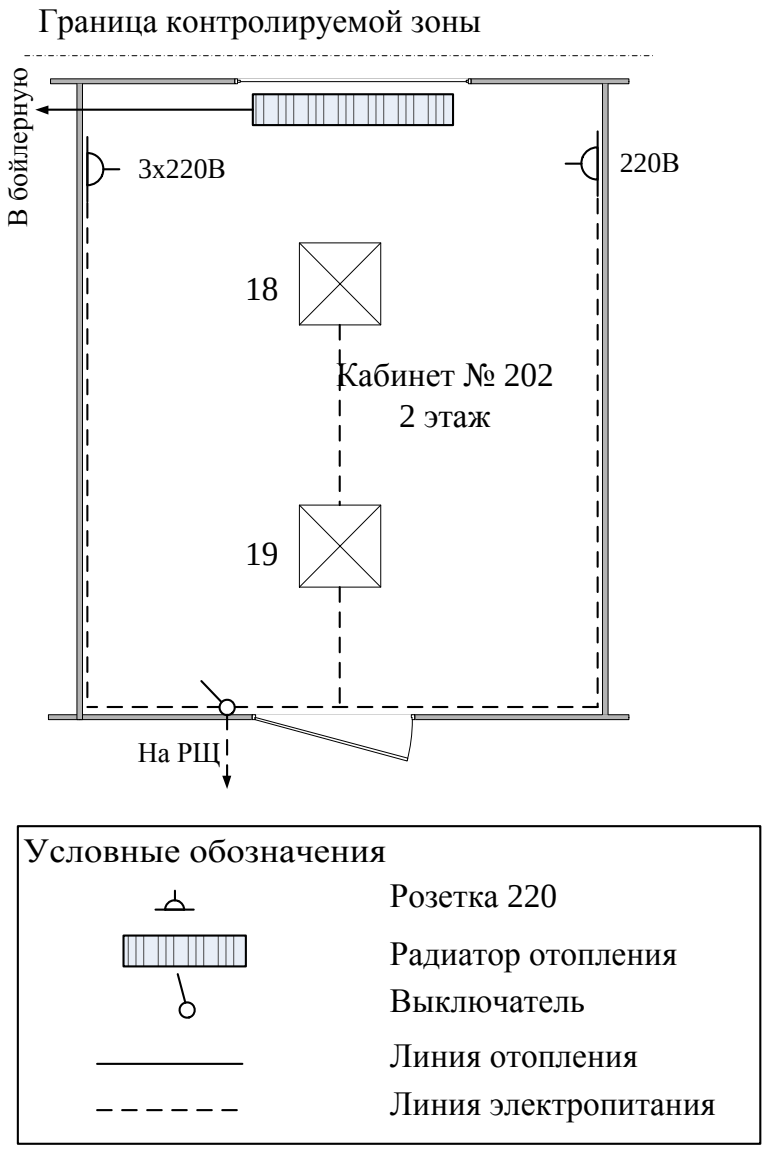

Рисунок 2.5 – Размещение системы электропитания, заземления и инженерных коммуникаций

Наименование линии	**Выходит за пределы КЗ (выходит/не выходит)**
220	да
Заземление	да
Телефонная линия	нет
Охранная сигнализация	нет
Пожарная сигнализация	нет
ЛВС	нет
Отопление	нет

Электропитание выполнено по системе с изолированной нейтралью.

Линии электропитания и заземления выходят из кабинета за пределы контролируемой зоны.

2.7 Перечень средств защиты информации, установленных на объекте информатизации «Аэропорт» приведен в Таблице 2.3.

Таблица 2.3 - **Перечень средств защиты, установленных на ОИ «Аэропорт»**

№ п/п	Наименование и тип средства защиты информации	Заводской номер	СЗЗ	Сведения о сертификате	Место установки
1.	СЗИ от НСД «Secret Net 7»	№ HF23E4BH	СЗЗ З 507635	Сертификат ФСТЭК № 2707, действителен до 07.09.2018 г	АРМ 1
		№ UL173W87	СЗЗ Е 813059		АРМ 2
		№ UK27FWA7	СЗЗ Е 813058		Сервер
2.	Средство антивирусной защиты «Kaspersky Endpoint Security 10 для Windows»	№ СМП8069-0679	СЗЗ З 273005	Сертификат ФСТЭК № 3025, действителен до 25.11.2019 г.	АРМ 1, АРМ 2, Сервер
3.	МЭ и СКЗИ «Континент» 3.7	0001894	В746103	Сертификат ФСТЭК № 3008, действителен до 01.11.2019 г. Сертификат ФСБ № СФ/124-2918 действителен до 07.07.2019 г.	Кабинет № 202

2.8 Перечень программных средств, установленных на объекте вычислительной техники «Аэропорт» приведен в Таблице 2.4**:**

Таблица 2.4 – **Перечень ПО установленного на ОИ «Аэропорт»**

№	Наименование ПО	Версия
	АРМ 1	
1	Microsoft Windows 7 Professional	6.1.7601.18869
2	Microsoft Office стандартный 2010	14.0.6029.1000
3	ПЕРСОНА МИС	25.22
4	2ГИС	3.16.3.0
5	Adobe Reader XI MUI	11.0.00
6	eToken PKI Client 5.1 SP1	5.1.66.0
7	Kaspersky Endpoint Security 10 для Windows [Русский]	10.2.4.674
8	Mozilla Firefox 43.0.4 (x86 ru)	43.0.4
9	Secret Net 7	7.0.460.0
10	WinRAR	5.00.4
11	Acronis Backup & Recovery 11.5 Agent Core	11.5.32308
12	АРМ 2	
13	Microsoft Windows 7 Professional	6.1.7601.18869
14	ПЕРСОНА МИС	25.22
15	Adobe Flash Player 24 NPAPI	24.0.0.2
16	Adobe Reader X	10.1.6
17	eToken PKI Client 5.1 SP1	5.1.66.0
18	Google Chrome	1.0.0
19	Kaspersky Endpoint Security 10 для Windows [Русский]	10.2.4.674
20	Microsoft Office стандартный 2010	14.0.6029.1000
21	Secret Net 7	7.6.604.0

22	WinRAR	4.00.0
23	Сервер	
24	Microsoft Windows Server 2003 R2 Standard Edition	5.2.3790
25	ПЕРСОНА МИС	25.22
26	WinRAR	5.20.0
27	Google Chrome	1.0.0
28	Microsoft SQL Server	9.00.1399.06
29	Microsoft Visual C++ 2012	11.0.51106.1
30	Secret Net 7	7.0.460.16
31	Kaspersky Endpoint Security 10 для Windows [Русский]	10.2.4.674

3 СВЕДЕНИЯ О СООТВЕТСТВИИ ОТСС ОБЪЕКТА ВТ ТРЕБОВАНИЯМ ПО БЕЗОПАСНОСТИ ИНФОРМАЦИИ

3.7 Протоколы испытаний и даты их регистрации

3.8 Сведения об аттестации объекта информатизации на соответствие требованиям по безопасности информации:

Заключение по результатам аттестационных испытаний объекта информатизации

Аттестат соответствия №

4 УЧЕТ ПРОВЕДЕНИЯ РЕГЛАМЕНТНЫХ ПРОВЕРОК

Таблица 4.1 - **Учет проведения регламентных проверок**

№ п/п	Наименование организации, проводившей проверку	Дата проведения проверки	Номер протокола	Примечание

5 ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Таблица 5.1 - **Лист регистрации изменения состава и размещения ОТСС, ВТСС и средств защиты объекта информатизации**

№ п/п Дата введения изменений	Наименование документа, фиксирующего изменения	№ замененных (исправленных) листов формуляра	Подпись лица, внесшего изменения

ПРИЛОЖЕНИЕ Б.
Меры

СОГЛАСОВАНО

Руководитель органа по аттестации
объектов информатизации
ЗАО «Гранит Информ»

_____ Н.В. Узбеков
«_____»_____ 2017 г.

УТВЕРЖДАЮ

Начальник Челябинского центра ОВД филиала «Аэронавигация Урала» ФГУП «Госкорпорация по ОрВД»

_____ В.П. Ковалев
«_____»_____ 2017 г.

Челябинский центр ОВД филиала «Аэронавигация Урала»
ФГУП «Госкорпорация по ОрВД»
г. Челябинск, Аэропорт

МЕРЫ
по обеспечению безопасности конфиденциальной информации
при ее обработке в государственной информационной системе
«Аэропорт»

2017 г.

УСЛОВНЫЕ СОКРАЩЕНИЯ:

ГИС – государственная информационная система;
ИС – информационная система;
АС – автоматизированная система;

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Данные требования по обеспечению защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну при ее обработке в государственной информационной системе «Аэропорт» Челябинского центра ОВД «Аэронавигация Урала» ФГУП «Госкорпорация по ОрВД» (далее ГИС) разработаны на основании Приказа ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, и «Частной модели угроз безопасности информации ограниченного доступа при ее обработке в государственной информационной системе «Аэропорт».

1.2 Требования определяют совокупность организационных и технических мероприятий, необходимых для обеспечения заданного уровня безопасности информации ограниченного доступа при ее обработке в ГИС и обеспечения требуемого класса защищенности информационной системы. Требования распространяются только на данную ГИС.

2 ОРГАНИЗАЦИОННЫЕ МЕРОПРИЯТИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА

- должны быть предусмотрены меры физической охраны помещений ГИС для предотвращения бесконтрольного доступа в помещения посторонних лиц;
- доступ в помещения ГИС посторонним лицам должен быть разрешён только в присутствии сотрудников, допущенных к работе с данными ГИС;
- доступ к техническим средствам ГИС должен быть разрешён только тем сотрудникам, которым он нужен для выполнения служебных обязанностей;
- закупка технических средств должна осуществляться только у производителей или их официальных представителей;
- пользователи ГИС должны обладать минимально необходимыми правами доступа в системе, обязанности по соответствующей настройке системы разграничения доступа возлагаются на администратора ГИС;
- доступ к информации ограниченного доступа должен предоставляться сотрудникам в соответствии с утверждённым списком;
- доступ к информации ограниченного доступа и иным защищаемым ресурсам ИС должен предоставляться в соответствии с утверждённой матрицей доступа;
- ГИС должна быть физически или логически отделена от локальной сети организации, требования по соответствующей настройке рабочих станций и коммутационного оборудования возлагаются на администратора ГИС;
- ГИС должна быть физически отделена от сетей связи общего пользования межсетевым экраном.

3 МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА ПРИ ЕЕ ОБРАБОТКЕ В ГОСУДАРСТВЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ

В комплекс мер по защите информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну при их обработке в ГИС от несанкционированного доступа (далее НСД) и неправомерных действий входят следующие направления:

3.1 Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ):

- Идентификация и аутентификация пользователей, являющихся работниками оператора;
- Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов;

- Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации;
- Защита обратной связи при вводе аутентификационной информации;
- Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей).

3.2 Управление доступом субъектов доступа к объектам доступа (УПД):

- Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей;
- Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа;
- Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами;
- Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы;
- Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы;
- Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе);
- Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу;
- Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации;
- Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети;
- Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы).

3.3 Ограничение программной среды (ОПС):

- Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов.

3.4 Защита машинных носителей информации (ЗНИ):

- Учет машинных носителей информации
- Управление доступом к машинным носителям информации;
- Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания).

3.5 Регистрация событий безопасности (РСБ):

- Определение событий безопасности, подлежащих регистрации, и сроков их хранения;
- Определение состава и содержания информации о событиях безопасности, подлежащих регистрации;
- Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения;
- Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти;
- Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них;
- Генерирование временных меток и (или) синхронизация системного времени в информационной системе;
- Защита информации о событиях безопасности.

3.6 Антивирусная защита (АВЗ):

- Реализация антивирусной защиты;
- Обновление базы данных признаков вредоносных компьютерных программ (вирусов).

3.7 Контроль (анализ) защищенности информации (АНЗ):

- Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей;
- Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации;
- Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации;
- Контроль состава технических средств, программного обеспечения и средств защиты информации;
- Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе.

3.8 Обеспечение целостности информационной системы и информации (ОЦЛ):

- Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций.

3.9 Защита среды виртуализации (ЗСВ):

- В системе не предполагается использование технологий виртуализации. В случае их использования необходимо обеспечить идентификацию и аутентификацию субъектов доступа и объектов доступа и управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре.

3.10 Защита технических средств (ЗТС):

- Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования;
- Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены;
- Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр.

3.11 Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС):

- Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи;
- Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств;
- Защита беспроводных соединений, применяемых в информационной системе;
- Защита мобильных технических средств, применяемых в информационной системе

3.12 Выявление инцидентов и реагирование на них (ИНЦ):

- Определение лиц, ответственных за выявление инцидентов и реагирование на них;
- Обнаружение, идентификация и регистрация инцидентов;

- Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами;
- Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий и принятие мер по предотвращению из повторного появления.

3.13 Обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы осуществляется оператором в соответствии с эксплуатационной документацией на систему защиты информации и организационно-распорядительными документами по защите информации и в том числе включает:

- управление (администрирование) системой защиты информации информационной системы;
- выявление инцидентов и реагирование на них;
- управление конфигурацией аттестованной информационной системы и ее системы защиты информации;
- контроль (мониторинг) за обеспечением уровня защищенности информации, содержащейся в информационной системе.

3.14 В ходе управления (администрирования) системой защиты информации информационной системы осуществляются:

- заведение и удаление учетных записей пользователей, управление полномочиями пользователей информационной системы и поддержание правил разграничения доступа в информационной системе;
- управление средствами защиты информации в информационной системе, в том числе параметрами настройки программного обеспечения, включая программное обеспечение средств защиты информации, управление учетными записями пользователей, восстановление работоспособности средств защиты информации, генерацию, смену и восстановление паролей;
- установка обновлений программного обеспечения, включая программное обеспечение средств защиты информации, выпускаемых разработчиками (производителями) средств защиты информации или по их поручению;
- централизованное управление системой защиты информации информационной системы (при необходимости);
- регистрация и анализ событий в информационной системе, связанных с защитой информации (далее - события безопасности);
- информирование пользователей об угрозах безопасности информации, о правилах эксплуатации системы защиты информации информационной системы и отдельных средств защиты информации, а также их обучение;
- сопровождение функционирования системы защиты информации информационной системы в ходе ее эксплуатации, включая корректировку эксплуатационной документации на нее и организационно-распорядительных документов по защите информации;

3.15 В ходе выявления инцидентов и реагирования на них осуществляются:

- определение лиц, ответственных за выявление инцидентов и реагирование на них;
- обнаружение и идентификация инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и средств защиты информации, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;
- своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами;

- анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;
- планирование и принятие мер по устранению инцидентов, в том числе по восстановлению информационной системы и ее сегментов в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;
- планирование и принятие мер по предотвращению повторного возникновения инцидентов.

3.16 В ходе управления конфигурацией аттестованной информационной системы и ее системы защиты информации осуществляются:

- поддержание конфигурации информационной системы и ее системы защиты информации (структуры системы защиты информации информационной системы, состава, мест установки и параметров настройки средств защиты информации, программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на систему защиты информации (поддержание базовой конфигурации информационной системы и ее системы защиты информации);
- определение лиц, которым разрешены действия по внесению изменений в базовую конфигурацию информационной системы и ее системы защиты информации;
- управление изменениями базовой конфигурации информационной системы и ее системы защиты информации, в том числе определение типов возможных изменений базовой конфигурации информационной системы и ее системы защиты информации, санкционирование внесения изменений в базовую конфигурацию информационной системы и ее системы защиты информации, документирование действий по внесению изменений в базовую конфигурацию информационной системы и ее системы защиты информации, сохранение данных об изменениях базовой конфигурации информационной системы и ее системы защиты информации, контроль действий по внесению изменений в базовую конфигурацию информационной системы и ее системы защиты информации;
- анализ потенциального воздействия планируемых изменений в базовой конфигурации информационной системы и ее системы защиты информации на обеспечение защиты информации, возникновение дополнительных угроз безопасности информации и работоспособность информационной системы;
- определение параметров настройки программного обеспечения, включая программное обеспечение средств защиты информации, состава и конфигурации технических средств и программного обеспечения до внесения изменений в базовую конфигурацию информационной системы и ее системы защиты информации;
- внесение информации (данных) об изменениях в базовой конфигурации информационной системы и ее системы защиты информации в эксплуатационную документацию на систему защиты информации информационной системы;
- принятие решения по результатам управления конфигурацией о повторной аттестации информационной системы или проведении дополнительных аттестационных испытаний.

3.17 В ходе контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе, осуществляются:

- контроль за событиями безопасности и действиями пользователей в информационной системе;
- контроль (анализ) защищенности информации, содержащейся в информационной системе;
- анализ и оценка функционирования системы защиты информации информационной системы, включая выявление, анализ и устранение недостатков в функционировании системы защиты информации информационной системы;
-

- периодический анализ изменения угроз безопасности информации в информационной системе, возникающих в ходе ее эксплуатации, и принятие мер защиты информации в случае возникновения новых угроз безопасности информации;
- документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационной системе;
- принятие решения по результатам контроля (мониторинга) за обеспечением уровня защищенности информации о доработке (модернизации) системы защиты информации информационной системы, повторной аттестации информационной системы или проведении дополнительных аттестационных испытаний.

3.18 Обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации.

3.18.1 Обеспечение защиты информации при выводе из эксплуатации аттестованной информационной системы или после принятия решения об окончании обработки информации осуществляется оператором в соответствии с эксплуатационной документацией на систему защиты информации информационной системы и организационно-распорядительными документами по защите информации и в том числе включает:

- архивирование информации, содержащейся в информационной системе;
- уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации.

3.18.2 Архивирование информации, содержащейся в информационной системе, должно осуществляться при необходимости дальнейшего использования информации в деятельности оператора.

3.18.3 Уничтожение (стирание) данных и остаточной информации с машинных носителей информации производится при необходимости передачи машинного носителя информации другому пользователю информационной системы или в сторонние организации для ремонта, технического обслуживания или дальнейшего уничтожения.

3.18.4 При выводе из эксплуатации машинных носителей информации, на которых осуществлялись хранение и обработка информации, осуществляется физическое уничтожение этих машинных носителей информации.

3.19 Технические меры защиты информации реализуются посредством применения средств защиты информации, имеющих необходимые функции безопасности. В этом случае в информационных системах 3 класса защищенности применяются средства защиты информации 6 класса, а также средства вычислительной техники не ниже 5 класса.

ПРИЛОЖЕНИЕ В
Заключение по результатам аттестационных испытаний

АКЦИОНЕРНОЕ ОБЩЕСТВО
ГРАНИТ ИНФОРМ
454006, г. Челябинск, ул. Красноармейская, 55
тел (351) 218 28 28, эл. почта: info@g-inform.ru

УТВЕРЖДАЮ

Руководитель органа по аттестации
объектов информатизации
АО «Гранит Информ»

_____ Н.В. Узбеков

«_____»_____ 2017 г.

ЗАКЛЮЧЕНИЕ

ПО РЕЗУЛЬТАТАМ АТТЕСТАЦИОННЫХ ИСПЫТАНИЙ

Объект информатизации
государственная информационная система
«Аэропорт»
Челябинского центра ОВД филиала «Аэронавигация Урала»
ФГУП «Госкорпорация по ОрВД»
г. Челябинск, Аэропорт

2017 г.

УСЛОВНЫЕ СОКРАЩЕНИЯ

АРМ - автоматизированное рабочее место;
АС - автоматизированная система;
ГИС - государственная информационная система;
ИС – информационная система;
НГМД - накопитель на гибком магнитном диске;
НЖМД - накопитель на жестких магнитных дисках;
НСД - несанкционированный доступ;
ОИ - объект информатизации;
ОПО - общесистемное программное обеспечение;
ОС - операционная система;
ППО - прикладное программное обеспечение;
ПЭВМ - персональная электронно-вычислительная машина;
РД - руководящий документ;
СВТ - средства вычислительной техники;
СЗИ - система защиты информации;
СЗИ НСД - система защиты информации от несанкционированного доступа;
ЭВМ - электронно-вычислительная машина.

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Аттестационная комиссия, сформированная АО «Гранит Информ», действующая на основании Аттестата аккредитации № СЗИ RU.1960.В167.326 (действителен до 01.02.2018 г.) в составе экспертов по соответствующим направлениям:

Рыжов К.С. – заместитель генерального директора АО «Гранит Информ», председатель комиссии;

Евдокимов С.В. – ответственный за соответствие требованиям по организационно – техническому направлению, главный инженер АО «Гранит Информ», член комиссии;

Брюхов С.В. – ответственный за проведение аттестационных испытаний на соответствие требованиям по защите информации по каналам НСД, инженер АО «Гранит Информ», член комиссии;

провела аттестационные испытания в соответствии с «Программой и методикой проведения аттестационных испытаний государственной информационной системы…». Результаты аттестационных испытаний приведены в протоколах по направлениям:

- проверка объекта на соответствие организационно-техническим требованиям;
- защита от несанкционированного доступа;

1.2 Аттестационные испытания проведены в рамках аттестации информационных систем в соответствии с Приказом ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», «Положением по аттестации объектов информатизации на соответствие требованиям безопасности информации», а также других действующих нормативно-методических документов ФСТЭК России.

1.3 Заявитель аттестационных испытаний объекта – Челябинский центр ОВД «Аэронавигация Урала» ФГУП «Госкорпорация по ОрВД».

2 ЦЕЛЬ, ОБЪЕКТЫ И УСЛОВИЯ ИСПЫТАНИЙ

2.1 Цель испытаний: оценка соответствия принятых организационно-технических мер по обеспечению защиты информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, действующим требованиям нормативно-правовых документов по защите информации, а том числе:

– Руководящий документ ФСТЭК России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»

– Руководящий документ «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)»;

– Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

2.2 Объект аттестационных испытаний – объект информатизации государственная информационная система, размещенная по адресу: г. Челябинск, Аэропорт, второй этаж здания УралАэронавигации, кабинет № 202 (далее объект информатизации – ОИ).

2.3 Состав основных технических средств и систем (ОТСС) объекта приведен в таблице 2.1. Состав средств защиты информации объекта приведен в таблице 2.2. Полное описание объекта, состав вспомогательных технических средств и систем (ВТСС), расположение ВТСС относительно ОТСС и пр. параметры приведены в «Техническом паспорте».

Таблица 2.1 - **Состав объекта информатизации**

№ п/п	Наименование технического средства	Модель	Заводской (инвентарный) номер
АРМ 1			
1	Системный блок	InWin	инв. № 01010400779
2	НЖМД	ST500DM002-1BD142	Z3TA3B6B
3	Монитор	ViewSonic	S72103502117, инв. № 0000773
4	Клавиатура	Genius KB-200	XECC04004974
5	Мышь	Genius NetScroll 110X	X81145402338
6	Принтер	HP LaserJet 1020	CNC9402074, инв. № 000.011101040000581
7	Флешкарта	Transcend TS4GJF500 USB2 4Gb	инв. № 11013400017
АРМ 2			
8	Системный блок	InWin	инв. № 1010400728
9	НЖМД	ST500DM002-1BD142	Z3T35TM1
10	Монитор	Acer V193	ETLHW0016623416DBC8504
11	Клавиатура	Microsoft Basic Keyboard 1.0A	6968200981240
12	Компьютерные колонки	Genius SP-G16	KA10057342
13	Мышь	Oklick 105M	612852
14	Принтер	Samsung ML-3310ND	Z5TPBUGBC00618L
15	Флешкарта	Transcend TS4GJF500 USB2 4Gb	инв. № 11013400016
16	ИБП	APC Back-UPS CS500	4B1223P48041, инв. № 1101040752
Сервер			
17	Системный блок	Kraftway Express 200ED12	0010192060, инв. № 0040000334
18	НЖМД	WDC WD3200JS-00P	0M21

19	Монитор	Samsung SyncMaster 740N	344.011101040000334
20	Клавиатура	Genius KB-110X	XP128S891287
21	Мышь	Genius NetScroll 110X	X75892508894
22	Флешкарта	Transcend TS4GJF500 USB2 4Gb	инв. № 1101340000012
23	Коммутатор	D-Link DES-1005D	DL1E179000427

Таблица 2.2– **Перечень СЗИ «Аэропорт»**

№ п/п	Наименование и тип средства защиты информации	Заводской номер	СЗЗ	Сведения о сертификате	Место установки
1.	СЗИ от НСД «Secret Net 7»	№ HF23E4BH	СЗЗ З 507635	Сертификат ФСТЭК № 2707, действителен до 07.09.2018 г	АРМ 1
		№ UL173W87	СЗЗ Е 813059		АРМ 2
		№ UK27FWA7	СЗЗ Е 813058		Сервер
2.	Средство антивирусной защиты «Kaspersky Endpoint Security 10 для Windows»	№ СМП8069-0679	СЗЗ З 273005	Сертификат ФСТЭК № 3025, действителен до 25.11.2019 г.	АРМ 1, АРМ 2, Сервер
3.	Межсетевой экран «Altell NEO 100FW»	0001894	В746103	Сертификат ФСТЭК № 2634, действителен до 10.05.2018 г.	Кабинет № 202

2.4. В ходе аттестационных испытаний проводились следующие мероприятия:

– проверка объекта информатизации на соответствие организационно-техническим требованиям по защите информации;

– проверка ОИ на соответствие требованиям по защите информации от несанкционированного доступа;

– подготовка отчетной документации и оценка результатов испытаний объекта информатизации.

2.5. При проведении аттестационных испытаний применялись следующие методы проверок и испытаний:

– экспертно-документальный метод, предусматривающий проверку соответствия ГИС требованиям по безопасности информации на основании экспертной оценки полноты и достаточности представленных документов по обеспечению необходимых мер защиты информации в ГИС, а также соответствия реальных условий эксплуатации требованиям по размещению, монтажу и эксплуатации ГИС;

– проверка функций или комплекса функций защиты информации от НСД с помощью тестирующих средств, а также путем пробного запуска средств защиты информации от НСД и наблюдения за их выполнением;

2.6. В ходе проведения аттестационных испытаний использовались следующие руководящие и нормативно-технические документы:

– «Положение по аттестации объектов информатизации по требованиям безопасности информации», утвержденное председателем Гостехкомиссии России 25 ноября 1994 г.

– Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

–

– Руководящий документ Гостехкомиссии России. «Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности информации», утвержден председателем Гостехкомиссии России от 30 марта 1992 г.

– Руководящий документ Гостехкомиссии России. «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» Приказ Председателя Гостехкомиссии России от 04.06.1999 г. № 114.

2.7. При проведении аттестационных испытаний использовалась программные и технические средства, перечисленные в таблице 2.3.

Таблица 2.3 - **Используемые программные и технические средства**

Тип средства измерений	**Наименование**	**Заводской номер**	**Дата очередной поверки**
Программа поиска и гарантированного уничтожения информации на дисках	«TERRIER» **(**версия 3.0)	Голограмма № А 293818	Сертификат ФСТЭК № 1193, действ. до 16.05.2018 г.
Программа фиксации и контроля исходного состояния программного комплекса	«ФИКС» (версия 2.0.1)	Голограмма № А 267757	Сертификат ФСТЭК № 913, действ. до 01.06.2019 г.
Средство создания модели системы разграничения доступа	«Ревизор 1 XP»	Голограмма № А 296220	Сертификат ФСТЭК № 989, действ. до 08.02.2017 г.
Программа контроля полномочий доступа к информационным ресурсам	«Ревизор 2 XP»	Голограмма № А 268720	Сертификат ФСТЭК № 990, действ. до 08.02.2017 г.
Программа поиска и контроля уязвимостей в вычислительных сетях	Сетевой сканер «Ревизор сети» версия 3.0	Голограмма № З 263216	Сертификат ФСТЭК № 3413, действ. до 02.06.2018 г.

3 ПОРЯДОК ПРОВЕДЕНИЯ АТТЕСТАЦИОННЫХ ИСПЫТАНИЙ

Для проведения испытаний аттестационной комиссии предъявлены исходные данные и документация, указанные в таблице 3.1.

Таблица 3.1 - **Исходные данные на объект информатизации**

№ п.п.	Требовалось по «Программе аттестационных…»	Предоставлено Заявителем
1	Технический паспорт на объект вычислительной техники	Технический паспорт на объект информатизации «Аэропорт» Челябинского центра ОВД филиала «Аэронавигация Урала» ФГУП «Госкорпорация по ОрВД»
	Планы размещения ОТСС и ВТСС	
	Схемы прокладки линий передачи данных ОТСС и ВТСС	
	Состав и схемы размещения средств защиты информации	
	Схемы и характеристики систем электропитания и заземления ОТСС и ВТСС	
	Состав технических и программных средств, входящих в ГИС	
	Состав общесистемного и прикладного ПО	
2	Перечень защищаемой информации	Перечень информации ограниченного доступа подлежащих защите в государственной информационной системе «Аэропорт» Челябинского центра ОВД филиала «Аэронавигация Урала» ФГУП «Госкорпорация по ОрВД»
3	Организационно-распорядительная документация разрешительной системы доступа персонала к защищаемым ресурсам ГИС	Список сотрудников, доступ которых к информации ограниченного доступа необходим для выполнения служебных (трудовых) обязанностей
		Разрешительная система доступа «Аэропорт» Челябинского центра ОВД филиала «Аэронавигация Урала» ФГУП «Госкорпорация по ОрВД»
4	Акт классификации ГИС	Акт присвоения класса защищенности государственной информационной системы «Аэропорт» Челябинского центра ОВД филиала «Аэронавигация Урала» ФГУП «Госкорпорация по ОрВД»
5		Акт классификации ГИС предназначенной для обработки информации ограниченного доступа «Аэропорт» Челябинского центра ОВД филиала «Аэронавигация Урала» ФГУП «Госкорпорация по ОрВД»
6	Модель угроз безопасности информации	Частная модель угроз безопасности информации ограниченного доступа государственной информационной системы «Аэропорт» Челябинского центра ОВД филиала «Аэронавигация Урала» ФГУП «Госкорпорация по ОрВД»
7	Требования по обеспечению безопасности информации	Меры по обеспечению безопасности информации ограниченного доступа при ее обработке в информационной системе «Аэропорт» Челябинского центра ОВД филиала «Аэронавигация Урала» ФГУП «Госкорпорация по ОрВД»

8	Организационная документация	Приказ об организации работ по обеспечению безопасности информации ограниченного доступа «Аэропорт» Челябинского центра ОВД филиала «Аэронавигация Урала» ФГУП «Госкорпорация по ОрВД»
		Описание технологического процесса обработки информации в информационной системе «Аэропорт» Челябинского центра ОВД филиала «Аэронавигация Урала» ФГУП «Госкорпорация по ОрВД»
9	План контролируемой зоны	Приказ об определении границ контролируемой зоны
10	Сертификаты соответствия требованиям по безопасности информации на программные и технические средства ГИС, используемые средства защиты	Сертификат соответствия ФСТЭК на СЗИ от НСД «Secret Net 7» № 2707, действителен до 07.09.2018 г
		Сертификат соответствия ФСТЭК на антивирусное ПО «Kaspersky Endpoint Security 10 для Windows» № 3025, действителен до 25.11.2019 г.
		Сертификат соответствия ФСТЭК на межсетевой экран «Altell NEO 100FW» № 2634, действителен до 10.05.2018 г.
11	Эксплуатационная документация	Инструкция администратору государственной информационной системы «Аэропорт» Челябинского центра ОВД филиала «Аэронавигация Урала» ФГУП «Госкорпорация по ОрВД»
		Инструкция пользователям государственной информационной системы «Аэропорт» Челябинского центра ОВД филиала «Аэронавигация Урала» ФГУП «Госкорпорация по ОрВД»
		Инструкция по эксплуатации СЗИ государственной информационной системы «Аэропорт» Челябинского центра ОВД филиала «Аэронавигация Урала» ФГУП «Госкорпорация по ОрВД»
		Инструкция по организации антивирусной защиты государственной информационной системы «Аэропорт» Челябинского центра ОВД филиала «Аэронавигация Урала» ФГУП «Госкорпорация по ОрВД»

Аттестационные испытания были проведены в следующем порядке:

- проанализированы и оценены представленные исходные данные и документация по защите информации на объекте информатизации;
- осуществлена проверка соответствия представленных исходных данных реальным условиям размещения, монтажа средств вычислительной техники и эксплуатации средств защиты информации, рассмотрен технологический процесс обработки и хранения информации, проанализированы информационные потоки, определен состав и структура использованных для обработки информации технических и программных средств вычислительной техники;
- проверено состояние организации работ и выполнения организационно-технических требований по защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, наличие организационно-распорядительной, проектной и эксплуатационной документации, ее соответствие требованиям государственной и отраслевой нормативной документации по безопасности информации, подготовки кадров и распределения ответственности за выполнение требований по обеспечению безопасности информации;
- проведены комплексные испытания ГИС на соответствие требованиям безопасности информации от НСД;
- подготовлена отчетная документация и настоящее заключение по результатам аттестационных испытаний.

4 РЕЗУЛЬТАТЫ АТТЕСТАЦИОННЫХ ИСПЫТАНИЙ

В результате проверки организации работ и готовности к функционированию объекта информатизации на соответствие требованиям безопасности информации установлено:

4.1 Перечень представленных нормативных и организационно-распорядительных документов достаточен и их содержание соответствует требованиям стандартов и других нормативных документов по безопасности информации ФСТЭК России и иных органов государственного управления в пределах их компетенции.

4.2 Присвоение класса защищенности информации, обрабатываемой в информационной системе проведено без нарушений требований руководящих документов и в соответствии с постановлением приказом ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». Класс защищенности государственной информационной системы – «К3».

4.3 В организации произведен анализ угроз безопасности обрабатываемой информации ограниченного доступа, модель угроз составлена без нарушений требований руководящих документов.

4.4 На объект информатизации разработан технический паспорт, соответствующий требованиям приложения В СТР-К. Состав ОТСС и ВТСС, установленных на объекте, соответствует указанному в техническом паспорте.

4.5 В организации произведен анализ угроз безопасности обрабатываемой информации ограниченного доступа, модель угроз составлена без нарушений требований руководящих документов.

4.6 В организации приняты меры по ограничению доступа посторонних лиц к техническим средствам обработки защищаемой информации. Визуальный просмотр обрабатываемой на объекте информации посторонними лицами невозможен. Окно помещения, в котором расположен объект информатизации, оборудовано жалюзи. Помещения, в которых установлены ОТСС и хранятся машинные носители информации, оборудованы надежными замками, используются технические средства охраны и сигнализации. Допуск посторонних лиц в помещение ограничен и без контроля невозможен.

4.7 Допуск сотрудников к обработке конфиденциальной информации обеспечивается в рамках действующей в организации разрешительной системы и в соответствии с возложенными на персонал функциями.

4.8 На объекте имеются инструкции, на основании которых осуществляется работа пользователей, администраторов и обслуживающего персонала. Имеется эксплуатационная документация на используемые средства защиты информации.

4.9 Используемые средства защиты информации позволяют выполнить требования по защите информации ограниченного доступа.

4.10 Требования руководящих документов по защите информации от несанкционированного доступа к классу защищенности ГИС «К3» в части подсистем управления доступом, регистрации событий, обеспечения целостности и антивирусной защите выполнены.

4.11 Сертификаты соответствия на используемые средства защиты информации подтверждают возможность использования СЗИ в ГИС класса защищенности «К3».

5 ПРОТОКОЛ АТТЕСТАЦИОННЫХ ИСПЫТАНИЙ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, ПО НАПРАВЛЕНИЮ «ПРОВЕРКА ОБЪЕКТА НА СООТВЕТСТВИЕ ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИМ ТРЕБОВАНИЯМ»

5.1 Общие положения

Аттестационные испытания ГИС проводились в соответствии с разделом 2 «Программы и методики проведения аттестационных испытаний…» в следующем порядке: Состав основных технических средств и систем (ОТСС), системного и прикладного программного обеспечения, а также средств и систем защиты информации объекта информатизации приведен в Таблице 2.1, а также техническом паспорте на ОИ.

5.2 Результаты испытаний. Проверка достаточности представленных документов и соответствия их содержания требованиям по безопасности информации

Аттестационной комиссии были представлены исходные данные и документация на объект информатизации, приведенные в Таблице 3.1.

Заключение: *В предоставленных документах (см. Таблицу 3.1) содержатся все необходимые исходные данные об объекте информатизации. Дополнительных документов не требуется.*

5.3 Исследование технологического процесса обработки и хранения информации, анализ информационных потоков, определение состава использованных для обработки информации технических средств

5.3.1 При проведении исследования технологического процесса обработки информации на объекте информатизации, было определено, что:

объектами доступа ГИС являются:

а) ПЭВМ в целом;
б) машинные носители информации (в т.ч. флешкарты);
в) коммуникационные порты системного блока (LPT-порт, COM-порт, USB-порт);
г) файлы, содержащие защищаемые сведения;
д) программное обеспечение (общесистемное и прикладное);
е) основные и вспомогательные технические средства;
ж) средства и системы защиты информации.

субъектами доступа в ГИС являются:

а) прикладное программное обеспечение, применяемое для создания и/или редактирования файлов;

б) администратор информационной безопасности, осуществляющий администрирование программно-аппаратного комплекса СЗИ от НСД, а также установку и настройку прикладного и системного программного обеспечения;

в) пользователь, работающий на ПЭВМ;

г) обслуживающий персонал, осуществляющий техническое обслуживание средств вычислительной техники;

5.3.2 Была проанализирована обобщенная технологическая схема ГИС с существующими и возможными информационными потоками, возможностями доступа к обрабатываемой и передаваемой информации.

5.3.3 Было проверено соответствие описания технологического процесса обработки и хранения защищаемой информации с реальной технологией обработки данных на объекте. Противоречий не обнаружено.

Заключение: *Описание технологического процесса обработки и хранения конфиденциальной информации соответствует реальной практике, принятой на рассматриваемом объекте информатизации.*

5.3.4 Были проверены предоставленные исходные данные на рассматриваемую автоматизированную систему, комплектность и характеристики применяемых средств и систем защиты информации. Проанализированы вероятные опасные факторы и угрозы, которые могут воздействовать на автоматизированную систему, рассмотрены потенциально возможные критические места автоматизированной системы, снижающие уровень защиты.

Заключение: *Анализ исходных данных по автоматизированной системе не выявил опасных факторов, угроз и критических мест в автоматизированной системе, снижающих уровень защищенности информации и характеристики средств защиты информации.*

5.4 Проверка правильности присвоения уровня защищенности объекта информатизации и классификации ГИС

В ГИС обрабатывается информация ограниченного доступа, указанная в «Перечне информации ограниченного доступа подлежащих защите в государственной информационной системе». Масштаб системы определен как объектовый, определенный экспертным методом уровень значимости информации «УЗ 3». Для ГИС установлен класс защищенности государственных информационных систем «К3».

Заключение: *Классификация проведена без нарушений требований руководящих документов ФСТЭК (Гостехкомиссии) России.*

5.5 Проверка уровня подготовки кадров и распределения ответственности между персоналом по следующим направлениям:

– на объекте информатизации принята и подтверждена соответствующими организационно-распорядительными документами разрешительная система доступа персонала к защищаемым ресурсам;

– пользователи, администраторы и обслуживающий персонал подтвердили знание эксплуатационной документации (в пределах выполнения своих производственных задач), уровень овладения ими технологии безопасной обработки информации соответствует требованиям, изложенным в эксплуатационной документации;

Заключение: *Уровень подготовки кадров и распределение ответственности персонала, разрешительная система доступа персонала к защищаемым ресурсам объекта информатизации, определяющая полномочия по доступу к защищаемой информации, а также процедура оформления их полномочий, соответствуют предъявляемым к ним требованиям.*

5.6 Проверка наличия сертификатов соответствия на технические средства и средства защиты информации

На используемые средства защиты информации были представлены сертификаты, указанные в таблице 3.1.

Сертификаты подтверждают возможность использования средств защиты в ГИС данного класса.

Заключение: *На используемые средства защиты информации предоставлены все необходимые сертификаты. Сертификаты соответствуют классу защищенности ГИС.*

5.7 Проверка выполнения требований к помещениям, в которых производится обработка информации

Помещения оборудованы средствами пожарной и охранной сигнализации, доступ в помещения возможен только под присмотром сотрудников организации. Технические средства обработки защищаемой информации отдалены от границы контролируемой зоны. Просмотр информации с экранов мониторов, распечаток принтеров и с других устройств ввода-вывода информации из-за пределов контролируемой зоны исключён.

Заключение: *Требования руководящих документов по условиям размещения технических средств в помещениях выполняются.*

5.8 Выводы аттестационной комиссии

По результатам аттестационных испытаний комиссия считает, что:

5.8.1 Перечень представленных нормативных и организационно-распорядительных документов достаточен и их содержание соответствует требованиям стандартов и других нормативных документов по безопасности информации ФСТЭК России, ФСБ и иных органов государственного управления в пределах их компетенции.

5.8.2 Реализация требований инструкций и применение сертифицированных СЗИ от НСД обеспечивает выполнение установленных требований по защите информации при использовании технических и программных средств вычислительной техники.

5.8.3 Состав и структура программно-технических средств автоматизированной системы соответствует представленной документации.

5.8.4 Классификация автоматизированной системы проведена без нарушений требований руководящих документов ФСТЭК (Гостехкомиссии) России.

5.8.5 Помещение, в котором расположены ОТСС, отвечает требованиям руководящих документов, предъявляемым к рабочим помещениям, в которых устанавливаются СВТ для обработки информации с ограниченным доступом.

5.8.6 Допуск персонала к работе обеспечивается в рамках действующей в организации разрешительной системой и в соответствии с возложенными на персонал функциями.

5.8.7 Уровень подготовки персонала позволяет реализовать установленные для данного объекта информатизации требования по безопасности информации.

6 ПРОТОКОЛ АТТЕСТАЦИОННЫХ ИСПЫТАНИЙ ОБЪЕКТА ИНФОРМАТИЗАЦИИ НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ ПО ЗАЩИТЕ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К АВТОМАТИЗИРОВАННОЙ СИСТЕМЕ

6.1 Общие положения

ГИС построена на базе основных технических средств и систем, системного и прикладного программного обеспечения, а также средств и систем защиты информации, состав которых приведен в Таблице 2.1, а также техническом паспорте на ОИ.

6.2 Результаты проведения проверки качества и эффективности функционирования системы защиты информации от несанкционированного доступа

При проведении проверки качества и эффективности функционирования системы защиты информации от несанкционированного доступа проверяющая сторона руководствовалась следующими руководящими и нормативно-методическими документами:

- Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»;
- Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности СВТ»;
- Руководящий документ ФСТЭК России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»;
- Руководящий документ «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)»;
- Приказ ФСТЭК России от 11 февраля 2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

6.3 Анализ и оценка технологического процесса обработки информации

Проверка состояла:

- в анализе состояния реального технологического процесса обработки информации в ГИС;
- в выработке заключения о ее соответствии конструкторской (проектной), эксплуатационной и организационно-распорядительной документации на ГИС, предоставленной проверяющей стороной.

В рамках данного пункта проверки были проведены следующие мероприятия:

- анализ соответствия состава объектов и субъектов доступа, средств передачи и обработки информации исходным данным по функционированию ГИС, разрешительной системе доступа персонала к защищаемым ресурсам и соответствия реального технологического процесса обработки информации на средствах ГИС представленному описанию технологического процесса;
- определение опасных факторов и угроз, критических мест ГИС, снижающих уровень защиты; проверка наличия документов по разрешительной системе доступа персонала к защищаемой информации, хранящейся и (или) обрабатываемой в ГИС;
- проверка соответствия технологических инструкций пользователя и администратора защиты информации установленным требованиям.

В ходе проверки проверяемой стороной были представлены документы (см. Таблицу 3.1)

6.3.1 Анализ соответствия состава объектов и субъектов доступа, средств передачи и обработки информации исходным данным по технологии функционирования автоматизированной системы, разрешительной системе доступа персонала к защищаемым ресурсам

В процессе анализа были выполнены следующие операции:

- определен состав и режимы функционирования средств передачи и обработки информации, среды передачи информации;
- определены объекты и субъекты доступа, перечни штатных средств доступа к информации, средства защиты информации;
- проверено функционирование системы доступа персонала к защищаемым ресурсам.

6.3.1.1 Состав и функционирование средств передачи и обработки информации, среды передачи и обработки информации

На момент проведения проверки качества и эффективности функционирования системы защиты информации от несанкционированного доступа объект информатизации «Аэропорт» представляет из себя ЛВС из трех АРМ, расположенную в кабинете № 202 под управлением операционной системы «Microsoft Windows 7 Professional» (для «АРМ 1» и «АРМ 2») и «Microsoft Windows Server 2003 R2 Standard Edition» (для «Сервер»).

Внешними устройствами ГИС «Аэропорт» являются принтеры HP LaserJet 1020 и Samsung ML-3310ND, подключенные по интерфейсу USB, флешкарты (3 шт.). ЛВС Челябинского центра ОВД «Аэронавигация Урала» ФГУП «Госкорпорация по ОрВД» соединена с сетями общего пользования через сертифицированный программно-аппаратный межсетевой экран «Altell NEO 100FW», выполняющий функции маршрутизатора.

ГИС «Аэропорт» является многопользовательской системой без разграничения прав доступа пользователей.

Защищаемая информация хранится на жёстком диске АРМ «Сервер». Предоставляется сетевой доступ к данным для «АРМ 1» и «АРМ 2». Технологическим процессом предусмотрен вывод документов на «твердую» копию.

К работе с информацией ограниченного доступа допускаются лишь сотрудники, указанные в утверждённом списке.

Носители информации (флешкарты) учитываются, выдаются, уничтожаются согласно установленному порядку, что отражается в специальных журналах.

6.3.1.2 Перечень объектов и субъектов доступа

Анализ технологического процесса показал, что объектами доступа являются:

- ОТСС, предназначенные для обработки и передачи информации ограниченного доступа приведенные в техническом паспорте;
- программные средства информационной системы, предназначенные для обработки и передачи информации ограниченного доступа;
- учтенные машинные носители информации (далее - МНИ): флешкарты;
- все виды памяти ПЭВМ ГИС, в т.ч. оперативная память ПЭВМ, в которых может находиться защищаемая информация;
- база информации ограниченного доступа специализированного программного обеспечения.

Субъектами доступа в ГИС являются пользователи и процессы, выполняемые от их имени, которые имеют возможность доступа к объектам в ГИС штатными средствами. Субъектам доступа присваиваются официальные полномочия на уровне подсистемы защиты информации.

В процессе анализа технологического процесса обработки информации в ГИС установлено, что все субъекты доступа идентифицируются по имени учетной записи и аутентифицируются по паролям средствами СЗИ от НСД «Secret Net 7».

6.3.1.3 Перечень штатных средств доступа к информации в автоматизированной системе

Проверялось наличие штатных средств доступа к информации в ГИС.

Доступ к информации обеспечивается системным программным обеспечением ОС, а также с помощью прикладного программного обеспечения, указанного в «Техническом паспорте», предоставляющего субъектам документированные возможности доступа к объектам.

Произведен анализ состава программного обеспечения на наличие потенциально опасных или запрещенных программных модулей.

Произведен расчет контрольных сумм исполняемых модулей (компонентов) системы защиты информации от несанкционированного доступа средствами программы фиксации и контроля исходного состояния программного комплекса «ФИКС» версии 2.0.1 (Сертификат ФСТЭК России № 913 от 28 мая 2004 года, действителен до 1 июня 2019 года. Знак соответствия: № А 267757. Регистрационный номер: ЦС50-467А267757).

6.3.1.4 Перечень средств защиты информации

Проверялся перечень имеющихся средств защиты информации в ГИС.

На АРМ ОИ установлены СЗИ от НСД «Secret Net 7», средство антивирусной защиты «Kaspersky Endpoint Security 10 для Windows», межсетевой экран «Altell NEO 100FW».

Согласно представленным документам, при обработке защищаемой информации дополнительно проводятся организационно-технические мероприятия, обеспечивающие требуемый режим конфиденциальности, а также целостность и сохранность информации ограниченного доступа.

6.3.1.5 Проверка разрешительной системы доступа персонала к защищаемым ресурсам

Проверка заключалась в анализе организационно-распорядительной документации, устанавливающей разрешительную систему доступа персонала к защищаемым ресурсам ГИС. Анализ показал, что действующими факторами разрешительной системы являются:

- определение и документальное закрепление перечня сотрудников, допущенных к обработке конфиденциальной информации на данной ГИС.
- определение и документальной закрепление разрешительной системы доступа в матрице доступа.
- размещение АРМ в условиях ограниченного и контролируемого доступа;
- действия персонала (администратора защиты), имеющего доступ к автоматизированному рабочему месту, регламентированы специальными инструкциями;
- сопровождение и контроль функционирования ГИС осуществляется только администратором защиты ГИС.

6.3.2 Определение опасных факторов и угроз, критических мест автоматизированной системы, снижающих уровень защиты

В рамках данной проверки были выполнены следующие операции:

- проверен порядок организации охраны помещений, где установлены рабочие места ГИС;
- проверен порядок хранения в архивах копий программного обеспечения и конфигурационных данных;
- проверена настройка программных средств, посредством которых осуществляется доступ к объектам.

Анализ структуры ГИС и технологического процесса обработки информации показал, что в качестве основных факторов риска для ГИС могут рассматриваться:

- Компьютерные вирусы;
- Несанкционированный доступ через сети международного обмена;
- Кража технических средств, носителей информации (в т.ч. сервера БД);
- Порча или уничтожение технических средств, носителей информации;
- Внедрение по сети вредоносных программ.

Основными механизмами уменьшения факторов риска применительно к уязвимым местам ГИС, реализованными в ГИС на момент проведения проверки качества и эффективности функционирования системы защиты информации от НСД, являются:

- организация контроля за несанкционированным доступом в помещение с оборудованием ГИС;
- реализация механизмов идентификации и аутентификации при доступе к ресурсам АРМ в составе ГИС;
- использование сертифицированных средств защиты информации;
- детально описанная разрешительная система доступа к программным и аппаратным средствам ГИС для всех пользователей системы;
- использование только лицензионного программного обеспечения;
- регулярное резервное копирование защищаемых информационных ресурсов ГИС;
- наличие необходимой организационно-распорядительной документации;
- наличие администратора защиты ГИС.

Вывод: Используемые средства защиты информации и организационно-технические меры позволяют избежать проявления выявленных угроз безопасности информации.

6.3.3 Проверка соответствия технологических инструкций пользователя и администратора защиты информации установленным требованиям

Была проведена проверка оформленных разрешений на допуск персонала к различной защищаемой информации и соответствия технологических инструкций пользователям и администратору защиты установленным требованиям.

В рамках данной проверки были выполнены следующие операции:

- проверено наличие утвержденных разрешений на доступ персонала к защищаемой информации;
- проверено наличие и содержание технологической инструкции для пользователей ГИС;
- проверено наличие и содержание технологических инструкций для администратора защиты ГИС.

Установлено, что разрешения на доступ персонала к информации в ГИС, технологические инструкции пользователям и администратору защиты соответствуют требованиям нормативных документов по безопасности информации.

Вывод по разделу 6.3: Состав объектов и субъектов доступа, средств передачи и обработки информации в ГИС соответствует представленной документации, исходным данным по технологии функционирования ГИС, разрешительной системе доступа персонала к защищаемым ресурсам. В ГИС выполняются требования РД по документальному закреплению разрешительной системы доступа. Защитные механизмы уменьшают выявленные факторы и угрозы безопасности информации. В ГИС определены технологические инструкции пользователям и администратору.

6.4 Выбор инструментальных средств и методики испытаний.

По результатам анализа технологического процесса в соответствии с «Программой и методикой проведения испытаний…» решено проводить испытания подсистем управления доступом, регистрации и учёта, контроля целостности и антивирусной защиты на соответствие требованиям руководящих документов по защите информации. При проведении испытаний решено пользоваться специальными средствами проверки, определёнными в таблице 1.2 «Программы и методики…», а также проверкой реализованных функций средств защиты, просмотром журналов безопасности и другими методами, определёнными методикой испытаний.

6.4.1 Проверка подсистемы управления доступом

6.4.1.1 Описание реализованных правил разграничения доступа

Оценка реализованных правил разграничения доступа в ГИС проводилась по реальным возможностям защиты информации используемых СЗИ и при помощи программы контроля полномочий доступа к информационным ресурсам «РЕВИЗОР-2 XP» (Сертификат ФСТЭК России № 990 от 08 февраля 2005 года, действителен до 08 февраля 2017 года. Регистрационный номер программы: ЦС-50-0427А268720).

Механизмами разграничения доступа СЗИ являются:

- механизм контроля входа в систему;
- механизм избирательного разграничения доступа к локальным ресурсам;
- механизм разграничения доступа к устройствам компьютера.

Дополнительно к реализованным механизмам средствами СЗИ может быть обеспечено:

- механизм разграничения доступа к устройствам компьютера.

Вывод: По реализованным правилам разграничения доступа ГИС удовлетворяет требованиям к заявленному классу защищенности «К3».

6.4.2 Идентификация и аутентификация субъектов доступа и объектов доступа

Проверялась правильность предоставления доступа в соответствии с установленными правами субъектов по отношению к конкретным объектам в соответствии с матрицей доступа.

Права администратора безопасности и пользователей по доступу к информационным ресурсам ГИС отличаются. Разграничение доступа производятся на основании настроек операционной системы, которые производятся для пары «объект-субъект», где в качестве объекта выступает либо том, либо директория, либо конечный файл, а в качестве субъекта - учетные записи пользователей, а также пользовательские группы.

Проверка проводилась с использованием программы контроля полномочий доступа к информационным ресурсам «РЕВИЗОР-2 XP» (Сертификат ФСТЭК России № 990 от 08 февраля 2005 года, действителен до 08 февраля 2017 года. Регистрационный номер программы: ЦС-50-0427А268720). Данные для контроля формировались средством создания модели системы доступа «Ревизор-1 XP» (Сертификат ФСТЭК России № 989 от 08 февраля 2005 года, действителен до 08 февраля 2017 года. Регистрационный номер: ЦС50-0427А296220).

При попытке доступа пользователя к запрещенным настройкам, система прекращает выполнение запроса и выдает предупреждающее сообщение.

Вывод: Контроль доступа к защищаемым ресурсам производится в соответствии с матрицей доступа средствами операционной системы и СЗИ, что соответствует требованиям РД ГИС класса защищенности «К3».

6.4.3 Управление доступом субъектов доступа к объектам доступа

Согласно матрице доступа пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы, назначены минимально необходимые права и

привилегии. Ограничение неуспешных попыток входа в информационную систему выполняется средствами операционной системы и СЗИ от НСД«Secret Net 7».

Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу выполняется средствами операционной системы и СЗИ. Время блокировки установлено в 15 минут. Действия пользователя до прохождения системы идентификации и аутентификации запрещены средствами ОС и СЗИ от НСД «Secret Net 7».

Удаленный доступ субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети не предоставляется. Беспроводной доступ в системе не предоставляется. Использование мобильных технических средств не допускается. Сторонние организации к взаимодействию с ГИС не допускаются.

Вывод: Управление доступом субъектов доступа к объектам доступа производится в соответствии с матрицей доступа средствами операционной системы и СЗИ, что соответствует требованиям РД к ГИС класса защищенности «К3».

6.4.4 Проверка учёта всех защищаемых носителей информации с помощью их маркировки и занесением учётных данных в журнал учёта с отметкой об их выдаче (приёме).

Проверка показала, что используемые в ГИС съемные носители информации учитывается в специальном «Журнале учета машинных носителей». Их выдача/прием соответствующим образом регистрируется.

Вывод: Требования РД по учету защищаемых носителей информации АС класса «К3» выполнены.

6.4.5 Проверка подсистемы обеспечения целостности.

В соответствии с требованиями РД данная проверка включала в себя возможность восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций.

Вывод: В ГИС обеспечивается целостность программной среды в соответствии с требованиями РД к ГИС класса защищенности «К3».

6.4.6 Проверка физической охраны средств вычислительной техники.

В здании, в котором расположены технические средства ГИС, определён пропускной режим. Доступ посторонних лиц возможен только при предъявлении документа, удостоверяющего личность. Охрана здания, в котором размещается ГИС, осуществляется постоянно с помощью технических средств охраны и организационных мер, что исключает неконтролируемое пребывание посторонних лиц.

Вывод: В ГИС осуществляется физическая охрана средств вычислительной техники, что соответствует требованиям РД к ГИС класса защищенности «К3».

6.4.7 Проверка наличия средств восстановления системы защиты информации.

Осуществляется контроль установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации и программное обеспечение базовой системы ввода-вывода.

Вывод: В ГИС средства восстановления СЗИ соответствуют требованиям РД к ГИС класса защищенности «К3».

6.4.8 Проверка наличия сертифицированных средств защиты

Проверялось наличие на ОИ сертифицированных средств защиты информации.

Перечень СЗИ указан в пункте 2.1.1.4

Используемые СЗИ имеют сертификаты ФСТЭК России, сведения о которых приведены в таблице 3.1.

В соответствии с сертификатами и руководящими документами ФСТЭК (Гостехкомиссии) России данные СЗИ могут использоваться в ГИС класса защищенности «К3».

Вывод: По количественному составу и параметрам настройки сертифицированных средств защиты информации ГИС соответствуют требованиям РД к ГИС класса защищенности «К3».

6.4.9 Проверка подсистемы антивирусной защиты.

В качестве антивирусной защиты на АРМ ГИС установлена лицензионная копия сертифицированного антивирусного программного обеспечения «Kaspersky Endpoint Security 10 для Windows».

Условия, порядок и правила использования антивирусного программного обеспечения определены в «Инструкции по организации антивирусной защиты». Ответственность за организацию и проведения антивирусного контроля возложена на администратора информационной системы.

Вывод: Условия эксплуатации и обновления антивирусного программного обеспечения соответствуют требованиям РД к ГИС класса защищенности «К3».

6.4.10 Проверка защиты информации при межсетевом взаимодействии.

В соответствие с «Руководящим документом. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации» безопасное межсетевое взаимодействие для ГИС класса защищенности «К3» при их подключении к сетям международного информационного обмена достигается путем применения средств межсетевого экранирования, которые соответствуют следующим требованиям:

- фильтрация на сетевом уровне для каждого сетевого пакета независимо;
- идентификация и аутентификация администратора межсетевого экрана при его удаленных запросах методами, устойчивыми к пассивному и активному перехвату информации;
- регистрация входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова;
- контроль целостности своей программной и информационной части;
- восстановление свойств межсетевого экрана после сбоев и отказов оборудования;
- регламентное тестирование реализации правил фильтрации, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления.

Установленный в системе межсетевой экран «Altell NEO 100FW» имеет сертификат соответствия ФСТЭК и отвечает всем предъявляемым требованиям к средствам межсетевого экранирования.

6.4.11 Ограничение программной среды

Регистрация запуска/завершения программ и процессов (заданий, задач) осуществляется при помощи средств операционной системы и СЗИ. Установка компонентов ПО осуществляется только администраторами системы согласно матрице доступа, ограничение возможности установки выполнено локальными политиками ОС и СЗИ «Secret Net 7».

Проверка осуществлялась путем запуска/завершения любой доступной программы, и просмотра журнала безопасности на наличие соответствующего события. Проверялось наличие параметров регистрации, требуемых РД. В параметрах регистрации указывается путь к выполняемому файлу, используемые библиотеки, дата и время запуска, идентификатор пользователя, результат запуска.

Средства операционной системы и СЗИ в полной мере реализуют требуемые РД параметры регистрации указанных событий.

Вывод: Настройка ограничения программной среды соответствуют требованиям РД к ГИС класса защищенности «К3».

6.4.12 Защита машинных носителей информации, на которых хранится информация ограниченного доступа

Использование не учтенных съемных носителей информации контролируется СЗИ. Машинные носители учитываются в журнале. Охрана здания, в котором размещается ГИС, осуществляется постоянно с помощью технических средств охраны и организационных мер, что исключает неконтролируемое пребывание посторонних лиц в помещения, в которых обрабатывается и хранится информация конфиденциального характера. Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации определено внутренними локальными документами.

Вывод: В ГИС установлено СЗИ предотвращающее использование неучтенных съемных носителей информации, а так же предотвращен неконтролируемый доступ в помещения, в которых находятся машинные носители информации. Защита машинных носителей, на которых хранится и обрабатывается информация ограниченного доступа соответствует требованиям РД к ГИС класса защищенности «К3».

6.4.13 Регистрация событий безопасности

Регистрации запуска/завершения программ и процессов (заданий, задач) осуществляется при помощи средств операционной системы и СЗИ «Secret Net 7».

Проверка осуществлялась путем запуска/завершения любой доступной программы, и просмотра журнала безопасности на наличие соответствующего события. Проверялось наличие параметров регистрации, требуемых РД. В параметрах регистрации указывается путь к выполняемому файлу, используемые библиотеки, дата и время запуска, идентификатор пользователя, результат запуска.

Средства операционной системы и СЗИ в полной мере реализуют требуемые РД параметры регистрации указанных событий.

Проверка осуществлялась путем запуска на АРМ прикладных программ для получения доступа к защищаемым ресурсам. Доступ к ресурсу устанавливается в соответствии с разрешениями и текущим уровнем доступа исполняемого процесса.

Средства операционной системы и СЗИ осуществляют регистрацию попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам в объеме, требуемом РД.

Осуществлялась проверка наличия регистрации событий в журнале СЗИ.

Вывод: Параметры регистрации запуска/завершения программ и процессов удовлетворяют требованиям РД к ГИС класса защищенности «К3». Средствами операционной системы и СЗИ осуществляется полная регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам и данным, что удовлетворяет требованиям РД к ГИС класса защищенности «К3». Осуществляется регистрация событий безопасности в журнале СЗИ.

6.4.14 Контроль защищенности информации

Выявление уязвимостей информационной системы и их оперативное устранение ведется администратором информационной безопасности. Администратор информационной безопасности осуществляет проверку установки обновлений ПО и программных средств СЗИ, осуществляет контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и СЗИ, контроль состава технических средств, ПО и СЗИ, контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализация правил разграничения доступа, полномочий пользователя в информационной системе.

Была проверена парольная политика системы, а так же наличие обновлений безопасности операционной системы.

В ходе проверки были устранены выявленные уязвимости, осуществлен контроль установки обновлений, правильность настройки программ, состав технических средств, ПО и СЗИ, а так же проверена правильность используемых паролей

Вывод: Контроль защищенности системы соответствуют требованиям РД к ГИС класса защищенности «К3».

6.4.15 Защита среды виртуализации

Технологии виртуализации не используются. Требования РД по идентификации и аутентификации субъектов доступа и объектов доступа в виртуальной инфраструктуре выполняются.

Вывод: Защита среды виртуализации соответствует требованиям РД к ГИС класса защищенности «К3».

6.4.16 Защита технических средств

Контролируемая зона утверждена Приказом «Об определении контролируемой территории». В здании, в котором расположены технические средства ГИС, определён пропускной режим. Доступ посторонних лиц возможен только при предъявлении документа, удостоверяющего личность. Охрана здания, в котором размещается ГИС, осуществляется постоянно с помощью технических средств охраны и организационных мер, что исключает неконтролируемое пребывание посторонних лиц. Устройства вывода информации, расположены так, что исключается их несанкционированный просмотр. Окно занавешено жалюзи.

Вывод: В ГИС осуществляется физическая охрана средств вычислительной техники, что соответствует требованиям РД к ГИС класса защищенности «К3».

6.4.17 Защита информационной системы, ее средств, систем связи и передачи данных

Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи обеспечивается МЭ «Altell NEO 100FW».

Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств ведется средствами СЗИ «Secret Net 7»

В информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы разделены.

Передача информации по каналам, выходящим за пределы контролируемой зоны, не ведется.

Вывод: В ГИС используются СЗИ, которые соответствует требованиям РД к ГИС класса защищенности «К3».

6.4.18 Выявление инцидентов, которые могут привести к сбоям или нарушению функционирования информационной системы и к возникновению угроз безопасности персональных данных, и реагирование на них

Приняты организационно-распорядительные документы, определяющие лиц, ответственных за выявление инцидентов и реагирование на них. Ведется проверка обнаружения, идентификации и регистрации инцидентов. Осуществляется своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами. Ведется анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий. Принимаются меры по устранению инцидентов и предотвращению их повторного возникновения, в частности обновление баз антивирусного ПО.

Вывод: В ходе проверки были определены ответственные, была проверена регистрация инцидентов и меры по устранению возникших инцидентов. Принятые меры требованиям РД к ГИС класса защищенности «К3».

6.4.19 Управление конфигурацией информационной системы и системы защиты информации

Вносить изменения в конфигурацию информационной системы и СЗИ может только администратор. Список работников, имеющих соответствующие права, утвержден в Разрешительной системе доступа. Изменения конфигурации информационной системы и СЗИ выполняются только администратором безопасности и согласуются с ответственным по обеспечению безопасности информации ограниченного доступа.

Была произведена проверка документов, регистрирующих изменение в конфигурации информационной системы и системы защиты информации.

Вывод: Меры управления конфигурацией информационной системы и системы защиты информации соответствуют требованиям РД к ГИС класса защищенности «К3».

6.4.20 Выводы по результатам проверки качества и эффективности функционирования системы защиты информации от несанкционированного доступа.

Результаты проведенных проверок показали, что автоматизированная система объекта информатизации «Аэропорт», по совокупности используемых настроек СЗИ и принятых организационных мер **соответствует** требованиям приказа ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», предъявляемым **к ГИС класса защищенности «К3».**

ОТЧЁТ
о фиксации исходного состояния
«Аэропорт»

СЗИ от НСД «Secret Net 7» (для «АРМ 1»)
(Уровень-1, программно)

№ пп	Имя файла	Дата создания	Длина, байт	Длина, строк	КС
Каталог C:\Program Files\Secret Net\Client					
1	BCGCBPRO100u90.dll	23.03.16 23-11	5546264	7534	9e42099eef0355133eead8501d759e2572
2	BCGCBProResRUS.dll	23.03.16 23-11	272664	766	8e8a6892a0f619531e9fbf53ff16173bf7
3	dpp.dll	23.03.16 23-12	170776	152	f315cf2e35da3681182f992011dc350373
4	lc.dll	23.03.16 23-14	695576	776	9cb77c91a9aa09f37fbefdbe1e7921d959
5	OMSLogManager.exe	23.03.16 23-07	2546456	6304	e1270a7308a981d1c358478ca893b63664
6	OmsServices.dll	23.03.16 23-16	739608	3229	a60fdbc09982019a31815993e8c93ef145
7	OneLookFeatRes.dll	23.03.16 23-16	53528	186	9d7ed007a6f139bb99d17d966b378afa92
8	Setup Security.inf	23.03.16 17-33	5519	220	9af60725747cca9a05bc057d871924f6ee
9	SnAsAdm.exe	23.03.16 23-08	15128	60	3584ec10794b77d923ec737256aa38787b
10	sncontrol.dll	23.03.16 23-17	123160	182	44cb76f3de24a998f9466584390f7b4c98
11	SnCpCom.dll	23.03.16 23-17	1526040	2072	2ae927801959ccce26ffc0228ed415b5b0
12	SnCtxVChannel Client.dll	23.03.16 23-18	74008	165	db1764a23b106b8060c48d06a73e969b91
13	sndc.dll	23.03.16 23-18	348440	542	cf00866406b1d2bb7c80d4bbcb2f033645
14	SnDCDesc.dll	23.03.16 23-18	81176	134	afc5d4b36996eb00a6f7735fbd8eb452e3
15	SnDrvSupport.dll	23.03.16 23-18	196376	252	d22e53975385de065efe50ef977ea20aed
16	SnEsmart.dll	23.03.16 23-18	112920	179	ab25d90d21e525aec84a0593cfc92758c8
17	SnEtalonsDB.Dll	23.03.16 23-19	161048	182	9ba2630525a168d9d8d96fc9e093bd5115
18	SnEtokenEx.dll	23.03.16 23-19	131352	186	0519d3e9c99ec714b42a1299a31344e720
19	SnEtokenSC.dll	23.03.16 23-19	130840	202	85da4a9ee25520eb72d4c0311f79b7dcd9
20	SnFileExt.dll	23.03.16 23-19	527128	1538	8ada2bdf4e5614e859226e6c21d8eb51b3
21	SnFloppy.dll	23.03.16 23-19	108312	219	d90a5fbc63c7c109a3f45eb6d1eda14968
22	SnGpeUpd.dll	23.03.16 23-20	294168	287	6ebccad4d359ca390a48e448a9512840e5
23	SnHWc.dll	23.03.16 23-20	443160	475	b55949d827af99c83ab4206706d190c47d
24	SnHwSrv.exe	23.03.16 23-08	331032	488	a2aebf222c8cf63ee38c4abb111fe926ee
25	SnICheckAdm.exe	23.03.16 23-09	2068760	3387	9ee04a6fba506393cfade8d3052eb00afe
26	SnIcheckCmdTool.exe	23.03.16 23-09	60184	139	51b4ba401d8d1efdc12bf734cc69c7c3b8
27	SNICheckLDB.dll	23.03.16 23-20	304408	319	5f98609b7fdf9d6dcc378a564c82c4efb0
28	SnicheckSrv.Exe	23.03.16 23-09	1167640	1383	b57ee4449ccda75b9ed2c28ecdb2c411a4
29	SnIcon.exe	23.03.16 23-09	608536	521	7829376bf0a283a9ff2482245512f81521
30	SniKey.dll	23.03.16 23-21	56088	105	6abe9fe6bcd82ccef653d243320e4c21d0
31	SnJacarta.dll	23.03.16 23-21	131864	191	b53e6d645f70c1b9f721bc2c99a4677475
32	snldb.dll	23.03.16 23-21	185624	250	9197553f99db19eb7cf71c214f113fe124
33	SnMCTune.exe	23.03.16 23-10	826136	1652	515e4f9fde086001281545324be5ca5f78
34	SnOptions.dll	23.03.16 23-22	6183192	9508	581fe20ffa63721af099f7b3720733d100
35	SnOptionsCtrls.dll	23.03.16 23-22	701720	2081	b1fa9cc039a60ca530a012126f1dac18cb
36	SnPC.dll	23.03.16 23-22	1354008	1988	607872fd9a2171275c0480c5735d9215f1
37	SnPrint.exe	23.03.16 23-10	121624	174	264c4762c5b69e514fb4d8abc85dee9ef2
38	SnPrintConfig.dll	23.03.16 23-22	241432	691	b9bdb5f1ba00e1000689c65e30b8d6e27e

39	SnPrintlib.dll	23.03.16 23-22	926488	3911	e1403757d2c018099e02b1cb759a53400
40	SnPrintLIbNG.dll	23.03.16 23-23	763672	5747	1607e1c1b34922258f07c56c3812cd70b2
41	SnReportBuilder.dll	23.03.16 23-23	77080	155	a9b6af67e7764f025227b7d676f6786187
42	SnReportForms.dll	23.03.16 23-23	400152	661	eaa495214faad05ad66afe6f38bdbea900
43	SnRuToken.dll	23.03.16 23-23	132376	198	f7867a9b836f24f28443dba597efc6a662
44	SnSable.dll	23.03.16 23-24	106264	237	9ed8d32dde28546e090a5aa668249f4d6c
45	SnServerObjects.dll	23.03.16 23-24	1005848	6890	1dc1aeefa113f7d8d930d5274cc47d378d
46	SnSrv.exe	23.03.16 23-10	213272	275	98f049b59096cc4ea2fc4cda3ed4e1a708
47	snsrvalarm.dll	23.03.16 23-25	351512	318	3c7cdc7a8acf9ef47544c3f270caa5281e
48	SnSrvGpe.dll	23.03.16 23-25	503064	529	0d29e4b8b4d90b0e59d1ade22899f0630f
49	SnSrvKrn.dll	23.03.16 23-25	178968	205	aa22ecfd30334da4d956c32f9b48a8d73f
50	SnSrvLib.dll	23.03.16 23-25	1067288	1655	9a9777d79398b06dcf9f5a8bcbd2be66e9
51	SnSrvLog.dll	23.03.16 23-25	188184	216	0bf977e18ecebf030b4e0b6a51ede63eae
52	SnTmCard.dll	23.03.16 23-25	109336	226	e773c76f788130dbca5d0e35aba02f09a3
53	SnTmlEdit.exe	23.03.16 23-10	1235224	2107	08c35cd3ca9737295887de31cb2dcaa7ae
54	SnUsers.dll	23.03.16 23-26	2026264	3326	54116e96ab6ce5d460fc72f996cceb6b46
55	SnVChannelClient.dll	23.03.16 23-26	82200	124	ff2874a0181a0b7cfab7da543c12aa0c95
56	TblRescue.exe	23.03.16 23-11	2501400	3761	ec57a12e897a2f35fcc5191f22bdafa84d
57	uc.dll	23.03.16 23-26	1111320	2250	9f434dcdd37d90f95cd267744f0983d04d
58	xerces-c_2_5_0.dll	23.03.16 23-26	1896728	7670	6e7f7202d35c5595d49c1c63245929b1ae
59	XmlDocument.dll	23.03.16 23-26	280856	689	9b044b0597895a58dbb780a55cbbdfa092
итого: файлов - 59			**43803391**	**89869**	**45d6ccd0c43da0104cf09bfe2f941adfe7**
Каталог C:\Program Files\Secret Net\Client\Grouppolicy					
60	Setup Security.inf	23.03.16 17-33	5519	220	9af60725747cca9a05bc057d871924f6ee
итого: файлов - 1			**5519**	**220**	**9af60725747cca9a05bc057d871924f6ee**
Каталог C:\Program Files\Secret Net\Client\virtualprinter					
61	SnXpsfsf.dll	23.03.16 23-05	242968	378	65e2c420cd1513e518cc574d1ca6c572da
62	SnXpsVP.dll	23.03.16 23-05	2098968	2514	93a786f685a68a3c2f7126e73239e4d158
63	SnXpsVP.inf	23.03.16 23-05	3090	75	fc74e24d5a2e738868aa99d1ab2f4f92d5
итого: файлов - 3			**2345026**	**2967**	**f4fd2c63ace910a9afe71605f90ef8d507**
Каталог C:\Program Files\Secret Net\TmCardDrv					
64	SnTmCardDrv.inf	23.03.16 23-04	3395	126	6032837802e3b4fd0ee37bd4416b400e30
65	SnTmCardDrv.sys	23.03.16 23-04	23792	99	ac9f1c299e5ac8e94793449ea812bd47fa
66	WdfCoInstaller 01009.dll	14.07.09 13-27	1461992	5663	cdd332effaf81000cb34c9a637335fc7d1
67	WUDFUpdate_ 01009.dll	14.07.09 13-21	1837296	7055	73066616c3ba48de31163293a81bac7e7c
итого: файлов - 4			**3326475**	**12943**	**4caa37a65defd4c451c0baabc8cb089a77**
ВСЕГО: файлов - 67			**49480411**	**105999**	**1f7336fe41914e175153702b77863e4453**

Конец

Антивирусное СЗИ «Kaspersky Endpoint Security 10 для Windows» (для «АРМ 1»)
(Уровень-2, программно)

№ пп	Имя файла	Дата создания	Длина, байт	Длина, строк	КС
Каталог C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security 10 for Windows					
1	ACAssembler.dll	17.04.12 10-13	201104	284	ab217200
2	am_facade.dll	17.04.12 10-13	283024	3274	1873771b
3	anti_phishing_http_filter.dll	17.04.12 10-13	405904	626	ce6546c3
4	avp.exe	07.02.13 20-55	515888	963	75280015
5	AVPCon.dll	28.01.13 21-53	783216	1013	bcd35c23
6	avzkrnl.dll	17.04.12 10-13	2121104	4129	1ae9cef9
7	categorizer_facade.dll	17.04.12 10-13	422288	630	74a648ff
8	cbi.dll	17.04.12 10-32	20968	66	45a18e63
9	cf_response_provider.dll	17.04.12 10-13	242064	262	0e60bd36
10	ckahcomm.dll	17.04.12 10-13	57744	75	d9f79bd0
11	ckahrule.dll	17.04.12 10-13	135568	122	1fa1c650
12	ckahstat.dll	17.04.12 10-13	78224	202	4d0fe71c
13	ckahum.dll	17.04.12 10-13	385424	721	2462281f
14	clldr.dll	17.04.12 10-13	19856	66	ba6bbedf
15	CryptoStaticProvider.dll	17.04.12 10-13	90512	127	9f9caba5
16	dbghelp.dll	17.04.12 08-29	1213200	3341	52e3c283
17	device_control.dll	17.04.12 10-13	262544	301	bb3efb44
18	diffs.dll	17.04.12 10-13	135568	307	376f88e1
19	dtp_lib.dll	17.04.12 10-13	66448	515	e875025f
20	DumpWriter.dll	17.04.12 10-13	123280	275	92137fbb
21	ekasyswatch.dll	17.04.12 10-13	94608	160	127cf03a
22	eka_meta.dll	17.04.12 10-13	1098128	1712	717af67c
23	enterprise_application_control.dll	17.04.12 10-13	1225104	2313	4d2b7195
24	esmgr.dll	17.04.12 10-13	319888	418	310621db
25	excludemanager.dll	17.04.12 10-13	131472	211	4bb4cb3f
26	FileCategorizer.dll	17.04.12 10-13	430480	546	4fa2f9d4
27	format_recognizer.dll	17.04.12 10-13	418192	743	d02f3b85
28	fssync.dll	17.04.12 10-13	98704	213	4d0bd4b9
29	fssync_s.dll	17.04.12 10-16	147856	340	5fc68fa4
30	FTPprtc.dll	17.04.12 10-13	209296	404	7e9fe278
31	GetSI.dll	17.04.12 10-13	250256	284	0ab3a34d
32	http_protocoller_pipeline.dll	17.04.12 10-13	438672	451	fa304b17
33	ichecker.dll	17.04.12 10-13	143760	198	311b45c5
34	ICQprtc.dll	17.04.12 10-13	278928	703	c2ca4bd2
35	icudt40.dll	17.04.12 10-13	2974096	8882	82c7ac52
36	icuuc40.dll	17.04.12 10-13	967056	8177	12373c50
37	IRCprtc.dll	17.04.12 10-13	143760	197	41a99592
38	JBRprtc.dll	17.04.12 10-13	197008	375	53c4ccae
39	kldw.exe	17.04.12 10-17	38080	99	04f9de58
40	klifpp.dll	17.04.12 10-13	561552	1010	115a1d37
41	kltbar.dll	28.01.13 21-53	242544	245	918b7d8a
42	ksnhelper.dll	17.04.12 10-14	176528	175	541e51e8

43	ksn_client.dll	17.04.12 10-14	418192	498	464b6a48
44	ksn_facade.dll	17.04.12 10-14	127376	209	61d292c9
45	libola.dll	17.04.12 10-14	86416	104	4124c5d8
46	Load46St.dll	17.04.12 08-29	247312	374	d83de5c1
47	localization_manager.dll	17.04.12 10-14	594320	461	666979ff
48	MAPIEDK.dll	17.04.12 10-14	123280	237	ae1ec078
49	mcou.dll	17.04.12 10-14	340368	640	bda36c76
50	memmon.dll	17.04.12 10-14	74128	114	86874f57
51	MMPprtc.dll	17.04.12 10-14	197008	396	f0f702d4
52	MSNprtc.dll	17.04.12 10-14	246160	535	a2b0a4d0
53	msvcm80.dll	17.04.12 08-29	479232	2465	8386765c
54	msvcp80.dll	17.04.12 08-29	548864	596	728f22bf
55	msvcr80.dll	17.04.12 08-29	626688	1309	28289ab9
56	network_services.dll	17.04.12 10-14	311696	518	32d33b3e
57	packed_io.dll	17.04.12 10-14	57744	95	971b1453
58	patchmanager.exe	29.07.13 09-16	373520	806	7b4346e0
59	prloader.dll	22.06.12 12-59	262584	362	33a355ff
60	ProcessMonitor.dll	17.04.12 10-14	303504	316	2e03976f
61	prremote.dll	17.04.12 10-14	147856	207	f65a147f
62	sax_xml_parser.dll	17.04.12 10-14	143760	445	ca22faf5
63	service.dll	17.04.12 10-14	332176	499	32d9057e
64	shellex.dll	28.01.13 21-53	148336	169	5b2198ab
65	storage.dll	17.04.12 10-14	541072	688	916cfe19
66	swpragueplugin.dll	17.04.12 10-14	78224	137	e70aff97
67	test_access.dll	17.04.12 10-14	258448	284	153500eb
68	ThreatsManager.dll	17.04.12 10-14	160144	206	196b4a16
69	threats_disinfection.dll	17.04.12 10-14	496016	661	6889a8cf
70	transport_provider.dll	17.04.12 10-14	197008	199	9edb2610
71	updater.dll	17.04.12 10-14	1208720	1767	80fa1b91
72	ushata.dll	17.04.12 10-14	78224	215	3a19a118
73	vul_rt_scan.dll	17.04.12 10-14	139664	196	92e37647
74	vul_scan.dll	17.04.12 10-14	233872	398	e3e900fa
75	vul_strg.dll	17.04.12 10-14	672144	1444	ae7491c5
76	web_control.dll	17.04.12 10-14	323984	354	c9edef00
77	wmi32.exe	17.04.12 10-17	19000	72	c09c0b40
78	wmias.exe	17.04.12 10-32	26088	85	4fe50609
79	wmiav.exe	17.04.12 10-32	26088	85	eeef89f1
80	wmifw.exe	17.04.12 10-32	26088	85	ce236695
81	Yhoprtc.dll	17.04.12 10-14	156048	212	41bde8bc
итого: файлов - 81			**28981248**	**63598**	**e7854b8d**
Каталог C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security 10 for Windows\kl1_x64					
82	kl1.inf	18.08.11 17-11	1199	70	59336a69
83	kl1.sys	18.08.11 17-11	464176	510	d35a2da2
итого: файлов - 2			**465375**	**580**	**2c8e970b**
Каталог C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security 10 for Windows\kl2_x64					

84	kl2.inf	18.08.11 17-11	1229	71	99f8e278
85	kl2.sys	18.08.11 17-12	13616	52	9af8085f
итого: файлов - 2			**14845**	**123**	**33f1ebd7**
Каталог C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security 10 for Windows\klflt-dev_x64_600					
86	klfltdev.inf	03.04.12 16-44	11224	243	d05b5862
87	klfltdev.sys	03.04.12 16-44	58672	214	e0b20185
итого: файлов - 2			**69896**	**457**	**b00e5ae7**
Каталог C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security 10 for Windows\klif_x64_nt600					
88	klif.inf	14.05.12 20-05	3464	131	bda41073
89	klif.sys	14.05.12 20-05	636720	2371	0f5e91f0
итого: файлов - 2			**640184**	**2502**	**cc02a263**
Каталог C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security 10 for Windows\KLIFX64					
90	drvins64.exe	17.04.12 10-16	19856	68	4f96647b
итого: файлов - 1			**19856**	**68**	**4f96647b**
Каталог C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security 10 for Windows\KLIMX64					
91	klim6.inf	01.09.11 15-28	2767	100	83d32139
92	klim6.sys	01.09.11 15-28	32048	132	1fb35b19
93	netcfg.exe	17.04.12 10-16	21392	76	858c6cdf
итого: файлов - 3			**56207**	**308**	**2713ea31**
Каталог C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security 10 for Windows\x64					
94	dbghelp.dll	17.04.12 08-29	1443328	5807	d2b4a49e
95	DumpWriter.dll	17.04.12 10-16	147344	515	5d250363
96	eka_meta.dll	17.04.12 10-16	2050448	9003	98f7beaf
97	fssync.dll	17.04.12 10-16	123792	334	ec295d57
98	fssync_s.dll	17.04.12 10-17	123792	336	62ccb5cf
99	kldw.exe	17.04.12 10-17	45320	141	90023bf5
100	kltbar.dll	28.01.13 21-54	317296	601	ccd852cf
101	mapiedk.dll	17.04.12 10-16	131472	514	6ac6b6b8
102	mcou.dll	17.04.12 10-16	457104	1523	442ce643
103	msvcm80.dll	17.04.12 08-29	516096	3287	42f60245
104	msvcp80.dll	17.04.12 08-29	1061376	5354	5ba5e2a5
105	msvcr80.dll	17.04.12 08-29	796672	5911	9e4f4ec0
106	prLoader.dll	17.04.12 10-16	386960	1228	f8bcdc27
107	prremote.dll	17.04.12 10-16	189840	500	1c814e40
108	service.dll	17.04.12 10-16	545680	1308	1afe1abb
109	ShellEx.dll	28.01.13 21-54	191856	426	5447212e
110	wmi64.exe	17.04.12 10-17	21104	81	e9c9763d
итого: файлов - 17			**8549480**	**36869**	**c5ceb6d3**
Каталог C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security 10 for Windows\x86					
111	expsrv.dll	17.04.12 08-29	380957	1454	be24d021
112	mfc42.dll	17.04.12 08-29	1019959	1470	574bbba1
113	msvbvm50.dll	17.04.12 08-29	1355776	4267	b2e3e0be
114	msvbvm60.dll	17.04.12 08-29	1392671	3480	007fa56b

115	msvcp60.dll	17.04.12 08-29	401462	165	86843a57
116	msvcr80.dll	17.04.12 08-29	626688	1309	28289ab9
итого: файлов - 6			**5177513**	**12145**	**757fe6fe**
ВСЕГО: файлов - 116			**43974604**	**116650**	**720eb73b**
Конец					

СЗИ от НСД «Secret Net 7» (для «АРМ 2»)

(Уровень-1, программно)

№ пп	Имя файла	Дата создания	Длина, байт	Длина, строк	КС
Каталог C:\Program Files\Secret Net\Client					
1	BCGCBPRO100u90.dll	23.03.16 23-11	5546264	7534	9e42099eef0355133eead8501d759e2572
2	BCGCBProResRUS.dll	23.03.16 23-11	272664	766	8e8a6892a0f619531e9fbf53ff16173bf7
3	dpp.dll	23.03.16 23-12	170776	152	f315cf2e35da3681182f992011dc350373
4	lc.dll	23.03.16 23-14	695576	776	9cb77c91a9aa09f37fbefdbe1e7921d959
5	OMSLogManager.exe	23.03.16 23-07	2546456	6304	e1270a7308a981d1c358478ca893b63664
6	OmsServices.dll	23.03.16 23-16	739608	3229	a60fdbc09982019a31815993e8c93ef145
7	OneLookFeatRes.dll	23.03.16 23-16	53528	186	9d7ed007a6f139bb99d17d966b378afa92
8	Setup Security.inf	23.03.16 17-33	5519	220	9af60725747cca9a05bc057d871924f6ee
9	SnAsAdm.exe	23.03.16 23-08	15128	60	3584ec10794b77d923ec737256aa38787b
10	sncontrol.dll	23.03.16 23-17	123160	182	44cb76f3de24a998f9466584390f7b4c98
11	SnCpCom.dll	23.03.16 23-17	1526040	2072	2ae927801959ccce26ffc0228ed415b5b0
12	SnCtxVChannelClient.dll	23.03.16 23-18	74008	165	db1764a23b106b8060c48d06a73e969b91
13	sndc.dll	23.03.16 23-18	348440	542	cf00866406b1d2bb7c80d4bbcb2f033645
14	SnDCDesc.dll	23.03.16 23-18	81176	134	afc5d4b36996eb00a6f7735fbd8eb452e3
15	SnDrvSupport.dll	23.03.16 23-18	196376	252	d22e53975385de065efe50ef977ea20aed
16	SnEsmart.dll	23.03.16 23-18	112920	179	ab25d90d21e525aec84a0593cfc92758c8
17	SnEtalonsDB.Dll	23.03.16 23-19	161048	182	9ba2630525a168d9d8d96fc9e093bd5115
18	SnEtokenEx.dll	23.03.16 23-19	131352	186	0519d3e9c99ec714b42a1299a31344e720
19	SnEtokenSC.dll	23.03.16 23-19	130840	202	85da4a9ee25520eb72d4c0311f79b7dcd9
20	SnFileExt.dll	23.03.16 23-19	527128	1538	8ada2bdf4e5614e859226e6c21d8eb51b3
21	SnFloppy.dll	23.03.16 23-19	108312	219	d90a5fbc63c7c109a3f45eb6d1eda14968
22	SnGpeUpd.dll	23.03.16 23-20	294168	287	6ebccad4d359ca390a48e448a9512840e5
23	SnHWc.dll	23.03.16 23-20	443160	475	b55949d827af99c83ab4206706d190c47d
24	SnHwSrv.exe	23.03.16 23-08	331032	488	a2aebf222c8cf63ee38c4abb111fe926ee
25	SnICheckAdm.exe	23.03.16 23-09	2068760	3387	9ee04a6fba506393cfade8d3052eb00afe
26	SnIcheckCmdTool.exe	23.03.16 23-09	60184	139	51b4ba401d8d1efdc12bf734cc69c7c3b8
27	SNICheckLDB.dll	23.03.16 23-20	304408	319	5f98609b7fdf9d6dcc378a564c82c4efb0
28	SnicheckSrv.Exe	23.03.16 23-09	1167640	1383	b57ee4449ccda75b9ed2c28ecdb2c411a4
29	SnIcon.exe	23.03.16 23-09	608536	521	7829376bf0a283a9ff2482245512f81521
30	SniKey.dll	23.03.16 23-21	56088	105	6abe9fe6bcd82ccef653d243320e4c21d0
31	SnJacarta.dll	23.03.16 23-21	131864	191	b53e6d645f70c1b9f721bc2c99a4677475
32	snldb.dll	23.03.16 23-21	185624	250	9197553f99db19eb7cf71c214f113fe124
33	SnMCTune.exe	23.03.16 23-10	826136	1652	515e4f9fde086001281545324be5ca5f78
34	SnOptions.dll	23.03.16 23-22	6183192	9508	581fe20ffa63721af099f7b3720733d100
35	SnOptionsCtrls.dll	23.03.16 23-22	701720	2081	b1fa9cc039a60ca530a012126f1dac18cb
36	SnPC.dll	23.03.16 23-22	1354008	1988	607872fd9a2171275c0480c5735d9215f1

37	SnPrint.exe	23.03.16 23-10	121624	174	264c4762c5b69e514fb4d8abc85dee9ef2
38	SnPrintConfig.dll	23.03.16 23-22	241432	691	b9bdb5f1ba00e1000689c65e30b8d6e27e
39	SnPrintlib.dll	23.03.16 23-22	926488	3911	e1403757d2c018099e02b1cb759a534002
40	SnPrintLIbNG.dll	23.03.16 23-23	763672	5747	1607e1c1b34922258f07c56c3812cd70b2
41	SnReportBuilder.dll	23.03.16 23-23	77080	155	a9b6af67e7764f025227b7d676f6786187
42	SnReportForms.dll	23.03.16 23-23	400152	661	eaa495214faad05ad66afe6f38bdbea900
43	SnRuToken.dll	23.03.16 23-23	132376	198	f7867a9b836f24f28443dba597efc6a662
44	SnSable.dll	23.03.16 23-24	106264	237	9ed8d32dde28546e090a5aa668249f4d6c
45	SnServerObjects.dll	23.03.16 23-24	1005848	6890	1dc1aeefa113f7d8d930d5274cc47d378d
46	SnSrv.exe	23.03.16 23-10	213272	275	98f049b59096cc4ea2fc4cda3ed4e1a708
47	snsrvalarm.dll	23.03.16 23-25	351512	318	3c7cdc7a8acf9ef47544c3f270caa5281e
48	SnSrvGpe.dll	23.03.16 23-25	503064	529	0d29e4b8b4d90b0e59d1ade22899f0630f
49	SnSrvKrn.dll	23.03.16 23-25	178968	205	aa22ecfd30334da4d956c32f9b48a8d73f
50	SnSrvLib.dll	23.03.16 23-25	1067288	1655	9a9777d79398b06dcf9f5a8bcbd2be66e9
51	SnSrvLog.dll	23.03.16 23-25	188184	216	0bf977e18ecebf030b4e0b6a51ede63eae
52	SnTmCard.dll	23.03.16 23-25	109336	226	e773c76f788130dbca5d0e35aba02f09a3
53	SnTmlEdit.exe	23.03.16 23-10	1235224	2107	08c35cd3ca9737295887de31cb2dcaa7ae
54	SnUsers.dll	23.03.16 23-26	2026264	3326	54116e96ab6ce5d460fc72f996cceb6b46
55	SnVChannelClient.dll	23.03.16 23-26	82200	124	ff2874a0181a0b7cfab7da543c12aa0c95
56	TblRescue.exe	23.03.16 23-11	2501400	3761	ec57a12e897a2f35fcc5191f22bdafa84d
57	uc.dll	23.03.16 23-26	1111320	2250	9f434dcdd37d90f95cd267744f0983d04d
58	xerces-c_2_5_0.dll	23.03.16 23-26	1896728	7670	6e7f7202d35c5595d49c1c63245929b1ae
59	XmlDocument.dll	23.03.16 23-26	280856	689	9b044b0597895a58dbb780a55cbbdfa092
итого: файлов - 59			**43803391**	**89869**	**45d6ccd0c43da0104cf09bfe2f941adfe7**
Каталог C:\Program Files\Secret Net\Client\Grouppolicy					
60	Setup Security.inf	23.03.16 17-33	5519	220	9af60725747cca9a05bc057d871924f6ee
итого: файлов - 1			**5519**	**220**	**9af60725747cca9a05bc057d871924f6ee**
Каталог C:\Program Files\Secret Net\Client\virtualprinter					
61	SnXpsfsf.dll	23.03.16 23-05	242968	378	65e2c420cd1513e518cc574d1ca6c572da
62	SnXpsVP.dll	23.03.16 23-05	2098968	2514	93a786f685a68a3c2f7126e73239e4d158
63	SnXpsVP.inf	23.03.16 23-05	3090	75	fc74e24d5a2e738868aa99d1ab2f4f92d5
итого: файлов - 3			**2345026**	**2967**	**f4fd2c63ace910a9afe71605f90ef8d507**
Каталог C:\Program Files\Secret Net\TmCardDrv					
64	SnTmCardDrv.inf	23.03.16 23-04	3395	126	6032837802e3b4fd0ee37bd4416b400e30
65	SnTmCardDrv.sys	23.03.16 23-04	23792	99	ac9f1c299e5ac8e94793449ea812bd47fa
66	WdfCoInstaller01009.dll	14.07.09 13-27	1461992	5663	cdd332effaf81000cb34c9a637335fc7d1
67	WUDFUpdate_01009.dll	14.07.09 13-21	1837296	7055	73066616c3ba48de31163293a81bac7e7c
итого: файлов - 4			**3326475**	**12943**	**4caa37a65defd4c451c0baabc8cb089a77**
ВСЕГО: файлов - 67			**49480411**	**105999**	**1f7336fe41914e175153702b77863e4453**

Конец

Антивирусное СЗИ «Kaspersky Endpoint Security 10 для Windows» (для «АРМ 2»)

(Уровень-2, программно)

№ пп	Имя файла	Дата создания	Длина, байт	Длина, строк	КС
Каталог C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security 10 for Windows					
1	ACAssembler.dll	17.04.12 10-13	201104	284	ab217200
2	am_facade.dll	17.04.12 10-13	283024	3274	1873771b

3	anti_phishing_http_filter.dll	17.04.12 10-13	405904	626	ce6546c3
4	avp.exe	07.02.13 20-55	515888	963	75280015
5	AVPCon.dll	28.01.13 21-53	783216	1013	bcd35c23
6	avzkrnl.dll	17.04.12 10-13	2121104	4129	1ae9cef9
7	categorizer_facade.dll	17.04.12 10-13	422288	630	74a648ff
8	cbi.dll	17.04.12 10-32	20968	66	45a18e63
9	cf_response_provider.dll	17.04.12 10-13	242064	262	0e60bd36
10	ckahcomm.dll	17.04.12 10-13	57744	75	d9f79bd0
11	ckahrule.dll	17.04.12 10-13	135568	122	1fa1c650
12	ckahstat.dll	17.04.12 10-13	78224	202	4d0fe71c
13	ckahum.dll	17.04.12 10-13	385424	721	2462281f
14	clldr.dll	17.04.12 10-13	19856	66	ba6bbedf
15	CryptoStaticProvider.dll	17.04.12 10-13	90512	127	9f9caba5
16	dbghelp.dll	17.04.12 08-29	1213200	3341	52e3c283
17	device_control.dll	17.04.12 10-13	262544	301	bb3efb44
18	diffs.dll	17.04.12 10-13	135568	307	376f88e1
19	dtp_lib.dll	17.04.12 10-13	66448	515	e875025f
20	DumpWriter.dll	17.04.12 10-13	123280	275	92137fbb
21	ekasyswatch.dll	17.04.12 10-13	94608	160	127cf03a
22	eka_meta.dll	17.04.12 10-13	1098128	1712	717af67c
23	enterprise_application_control.dll	17.04.12 10-13	1225104	2313	4d2b7195
24	esmgr.dll	17.04.12 10-13	319888	418	310621db
25	excludemanager.dll	17.04.12 10-13	131472	211	4bb4cb3f
26	FileCategorizer.dll	17.04.12 10-13	430480	546	4fa2f9d4
27	format_recognizer.dll	17.04.12 10-13	418192	743	d02f3b85
28	fssync.dll	17.04.12 10-13	98704	213	4d0bd4b9
29	fssync_s.dll	17.04.12 10-16	147856	340	5fc68fa4
30	FTPprtc.dll	17.04.12 10-13	209296	404	7e9fe278
31	GetSI.dll	17.04.12 10-13	250256	284	0ab3a34d
32	http_protocoller_pipeline.dll	17.04.12 10-13	438672	451	fa304b17
33	ichecker.dll	17.04.12 10-13	143760	198	311b45c5
34	ICQprtc.dll	17.04.12 10-13	278928	703	c2ca4bd2
35	icudt40.dll	17.04.12 10-13	2974096	8882	82c7ac52
36	icuuc40.dll	17.04.12 10-13	967056	8177	12373c50
37	IRCprtc.dll	17.04.12 10-13	143760	197	41a99592
38	JBRprtc.dll	17.04.12 10-13	197008	375	53c4ccae
39	kldw.exe	17.04.12 10-17	38080	99	04f9de58
40	klifpp.dll	17.04.12 10-13	561552	1010	115a1d37
41	kltbar.dll	28.01.13 21-53	242544	245	918b7d8a
42	ksnhelper.dll	17.04.12 10-14	176528	175	541e51e8
43	ksn_client.dll	17.04.12 10-14	418192	498	464b6a48
44	ksn_facade.dll	17.04.12 10-14	127376	209	61d292c9
45	libola.dll	17.04.12 10-14	86416	104	4124c5d8
46	Load46St.dll	17.04.12 08-29	247312	374	d83de5c1
47	localization_manager.dll	17.04.12 10-14	594320	461	666979ff
48	MAPIEDK.dll	17.04.12 10-14	123280	237	ae1ec078
49	mcou.dll	17.04.12 10-14	340368	640	bda36c76

50	memmon.dll	17.04.12 10-14	74128	114	86874f57
51	MMPprtc.dll	17.04.12 10-14	197008	396	f0f702d4
52	MSNprtc.dll	17.04.12 10-14	246160	535	a2b0a4d0
53	msvcm80.dll	17.04.12 08-29	479232	2465	8386765c
54	msvcp80.dll	17.04.12 08-29	548864	596	728f22bf
55	msvcr80.dll	17.04.12 08-29	626688	1309	28289ab9
56	network_services.dll	17.04.12 10-14	311696	518	32d33b3e
57	packed_io.dll	17.04.12 10-14	57744	95	971b1453
58	patchmanager.exe	29.07.13 09-16	373520	806	7b4346e0
59	prloader.dll	22.06.12 12-59	262584	362	33a355ff
60	ProcessMonitor.dll	17.04.12 10-14	303504	316	2e03976f
61	prremote.dll	17.04.12 10-14	147856	207	f65a147f
62	sax_xml_parser.dll	17.04.12 10-14	143760	445	ca22faf5
63	service.dll	17.04.12 10-14	332176	499	32d9057e
64	shellex.dll	28.01.13 21-53	148336	169	5b2198ab
65	storage.dll	17.04.12 10-14	541072	688	916cfe19
66	swpragueplugin.dll	17.04.12 10-14	78224	137	e70aff97
67	test_access.dll	17.04.12 10-14	258448	284	153500eb
68	ThreatsManager.dll	17.04.12 10-14	160144	206	196b4a16
69	threats_disinfection.dll	17.04.12 10-14	496016	661	6889a8cf
70	transport_provider.dll	17.04.12 10-14	197008	199	9edb2610
71	updater.dll	17.04.12 10-14	1208720	1767	80fa1b91
72	ushata.dll	17.04.12 10-14	78224	215	3a19a118
73	vul_rt_scan.dll	17.04.12 10-14	139664	196	92e37647
74	vul_scan.dll	17.04.12 10-14	233872	398	e3e900fa
75	vul_strg.dll	17.04.12 10-14	672144	1444	ae7491c5
76	web_control.dll	17.04.12 10-14	323984	354	c9edef00
77	wmi32.exe	17.04.12 10-17	19000	72	c09c0b40
78	wmias.exe	17.04.12 10-32	26088	85	4fe50609
79	wmiav.exe	17.04.12 10-32	26088	85	eeef89f1
80	wmifw.exe	17.04.12 10-32	26088	85	ce236695
81	Yhoprtc.dll	17.04.12 10-14	156048	212	41bde8bc
итого: файлов - 81			**28981248**	**63598**	**e7854b8d**
Каталог C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security 10 for Windows\kl1_x64					
82	kl1.inf	18.08.11 17-11	1199	70	59336a69
83	kl1.sys	18.08.11 17-11	464176	510	d35a2da2
итого: файлов - 2			**465375**	**580**	**2c8e970b**
Каталог C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security 10 for Windows\kl2_x64					
84	kl2.inf	18.08.11 17-11	1229	71	99f8e278
85	kl2.sys	18.08.11 17-12	13616	52	9af8085f
итого: файлов - 2			**14845**	**123**	**33f1ebd7**
Каталог C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security 10 for Windows\klfltdev_x64_600					
86	klfltdev.inf	03.04.12 16-44	11224	243	d05b5862
87	klfltdev.sys	03.04.12 16-44	58672	214	e0b20185

итого: файлов - 2			**69896**	**457**	**b00e5ae7**
Каталог C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security 10 for Windows\klif_x64_nt600					
88	klif.inf	14.05.12 20-05	3464	131	bda41073
89	klif.sys	14.05.12 20-05	636720	2371	0f5e91f0
итого: файлов - 2			**640184**	**2502**	**cc02a263**
Каталог C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security 10 for Windows\KLIFX64					
90	drvins64.exe	17.04.12 10-16	19856	68	4f96647b
итого: файлов - 1			**19856**	**68**	**4f96647b**
Каталог C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security 10 for Windows\KLIMX64					
91	klim6.inf	01.09.11 15-28	2767	100	83d32139
92	klim6.sys	01.09.11 15-28	32048	132	1fb35b19
93	netcfg.exe	17.04.12 10-16	21392	76	858c6cdf
итого: файлов - 3			**56207**	**308**	**2713ea31**
Каталог C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security 10 for Windows\x64					
94	dbghelp.dll	17.04.12 08-29	1443328	5807	d2b4a49e
95	DumpWriter.dll	17.04.12 10-16	147344	515	5d250363
96	eka_meta.dll	17.04.12 10-16	2050448	9003	98f7beaf
97	fssync.dll	17.04.12 10-16	123792	334	ec295d57
98	fssync_s.dll	17.04.12 10-17	123792	336	62ccb5cf
99	kldw.exe	17.04.12 10-17	45320	141	90023bf5
100	kltbar.dll	28.01.13 21-54	317296	601	ccd852cf
101	mapiedk.dll	17.04.12 10-16	131472	514	6ac6b6b8
102	mcou.dll	17.04.12 10-16	457104	1523	442ce643
103	msvcm80.dll	17.04.12 08-29	516096	3287	42f60245
104	msvcp80.dll	17.04.12 08-29	1061376	5354	5ba5e2a5
105	msvcr80.dll	17.04.12 08-29	796672	5911	9e4f4ec0
106	prLoader.dll	17.04.12 10-16	386960	1228	f8bcdc27
107	prremote.dll	17.04.12 10-16	189840	500	1c814e40
108	service.dll	17.04.12 10-16	545680	1308	1afe1abb
109	ShellEx.dll	28.01.13 21-54	191856	426	5447212e
110	wmi64.exe	17.04.12 10-17	21104	81	e9c9763d
итого: файлов - 17			**8549480**	**36869**	**c5ceb6d3**
Каталог C:\Program Files (x86)\Kaspersky Lab\Kaspersky Endpoint Security 10 for Windows\x86					
111	expsrv.dll	17.04.12 08-29	380957	1454	be24d021
112	mfc42.dll	17.04.12 08-29	1019959	1470	574bbba1
113	msvbvm50.dll	17.04.12 08-29	1355776	4267	b2e3e0be
114	msvbvm60.dll	17.04.12 08-29	1392671	3480	007fa56b
115	msvcp60.dll	17.04.12 08-29	401462	165	86843a57
116	msvcr80.dll	17.04.12 08-29	626688	1309	28289ab9
итого: файлов - 6			**5177513**	**12145**	**757fe6fe**
ВСЕГО: файлов - 116			**43974604**	**116650**	**720eb73b**

Конец

СЗИ от НСД «Secret Net 7» (для «Сервер»)
(Уровень-1, программно)

№ пп	Имя файла	Дата создания	Длина, байт	Длина, строк	КС
Каталог C:\Program Files\Secret Net\Client					
1	BCGCBPRO100u90.dll	23.03.16 23-11	5546264	7534	9e42099eef0355133eead8501d759e2572
2	BCGCBProResRUS.dll	23.03.16 23-11	272664	766	8e8a6892a0f619531e9fbf53ff16173bf7
3	dpp.dll	23.03.16 23-12	170776	152	f315cf2e35da3681182f992011dc350373
4	lc.dll	23.03.16 23-14	695576	776	9cb77c91a9aa09f37fbefdbe1e7921d959
5	OMSLogManager.exe	23.03.16 23-07	2546456	6304	e1270a7308a981d1c358478ca893b63664
6	OmsServices.dll	23.03.16 23-16	739608	3229	a60fdbc09982019a31815993e8c93ef145
7	OneLookFeatRes.dll	23.03.16 23-16	53528	186	9d7ed007a6f139bb99d17d966b378afa92
8	Setup Security.inf	23.03.16 17-33	5519	220	9af60725747cca9a05bc057d871924f6ee
9	SnAsAdm.exe	23.03.16 23-08	15128	60	3584ec10794b77d923ec737256aa38787b
10	sncontrol.dll	23.03.16 23-17	123160	182	44cb76f3de24a998f9466584390f7b4c98
11	SnCpCom.dll	23.03.16 23-17	1526040	2072	2ae927801959ccce26ffc0228ed415b5b0
12	SnCtxVChannelClient.dll	23.03.16 23-18	74008	165	db1764a23b106b8060c48d06a73e969b91
13	sndc.dll	23.03.16 23-18	348440	542	cf00866406b1d2bb7c80d4bbcb2f033645
14	SnDCDesc.dll	23.03.16 23-18	81176	134	afc5d4b36996eb00a6f7735fbd8eb452e3
15	SnDrvSupport.dll	23.03.16 23-18	196376	252	d22e53975385de065efe50ef977ea20aed
16	SnEsmart.dll	23.03.16 23-18	112920	179	ab25d90d21e525aec84a0593cfc92758c8
17	SnEtalonsDB.Dll	23.03.16 23-19	161048	182	9ba2630525a168d9d8d96fc9e093bd5115
18	SnEtokenEx.dll	23.03.16 23-19	131352	186	0519d3e9c99ec714b42a1299a31344e720
19	SnEtokenSC.dll	23.03.16 23-19	130840	202	85da4a9ee25520eb72d4c0311f79b7dcd9
20	SnFileExt.dll	23.03.16 23-19	527128	1538	8ada2bdf4e5614e859226e6c21d8eb51b3
21	SnFloppy.dll	23.03.16 23-19	108312	219	d90a5fbc63c7c109a3f45eb6d1eda14968
22	SnGpeUpd.dll	23.03.16 23-20	294168	287	6ebccad4d359ca390a48e448a9512840e5
23	SnHWc.dll	23.03.16 23-20	443160	475	b55949d827af99c83ab4206706d190c47d
24	SnHwSrv.exe	23.03.16 23-08	331032	488	a2aebf222c8cf63ee38c4abb111fe926ee
25	SnICheckAdm.exe	23.03.16 23-09	2068760	3387	9ee04a6fba506393cfade8d3052eb00afe
26	SnIcheckCmdTool.exe	23.03.16 23-09	60184	139	51b4ba401d8d1efdc12bf734cc69c7c3b8
27	SNICheckLDB.dll	23.03.16 23-20	304408	319	5f98609b7fdf9d6dcc378a564c82c4efb0
28	SnicheckSrv.Exe	23.03.16 23-09	1167640	1383	b57ee4449ccda75b9ed2c28ecdb2c411a4
29	SnIcon.exe	23.03.16 23-09	608536	521	7829376bf0a283a9ff2482245512f81521
30	SniKey.dll	23.03.16 23-21	56088	105	6abe9fe6bcd82ccef653d243320e4c21d0
31	SnJacarta.dll	23.03.16 23-21	131864	191	b53e6d645f70c1b9f721bc2c99a4677475
32	snldb.dll	23.03.16 23-21	185624	250	9197553f99db19eb7cf71c214f113fe124
33	SnMCTune.exe	23.03.16 23-10	826136	1652	515e4f9fde086001281545324be5ca5f78
34	SnOptions.dll	23.03.16 23-22	6183192	9508	581fe20ffa63721af099f7b3720733d100
35	SnOptionsCtrls.dll	23.03.16 23-22	701720	2081	b1fa9cc039a60ca530a012126f1dac18cb
36	SnPC.dll	23.03.16 23-22	1354008	1988	607872fd9a2171275c0480c5735d9215f1
37	SnPrint.exe	23.03.16 23-10	121624	174	264c4762c5b69e514fb4d8abc85dee9ef2
38	SnPrintConfig.dll	23.03.16 23-22	241432	691	b9bdb5f1ba00e1000689c65e30b8d6e27e
39	SnPrintlib.dll	23.03.16 23-22	926488	3911	e1403757d2c018099e02b1cb759a534002
40	SnPrintLIbNG.dll	23.03.16 23-23	763672	5747	1607e1c1b34922258f07c56c3812cd70b2
41	SnReportBuilder.dll	23.03.16 23-23	77080	155	a9b6af67e7764f025227b7d676f6786187
42	SnReportForms.dll	23.03.16 23-23	400152	661	eaa495214faad05ad66afe6f38bdbea900

43	SnRuToken.dll	23.03.16 23-23	132376	198	f7867a9b836f24f28443dba597efc6a662
44	SnSable.dll	23.03.16 23-24	106264	237	9ed8d32dde28546e090a5aa668249f4d6c
45	SnServerObjects.dll	23.03.16 23-24	1005848	6890	1dc1aeefa113f7d8d930d5274cc47d378d
46	SnSrv.exe	23.03.16 23-10	213272	275	98f049b59096cc4ea2fc4cda3ed4e1a708
47	snsrvalarm.dll	23.03.16 23-25	351512	318	3c7cdc7a8acf9ef47544c3f270caa5281e
48	SnSrvGpe.dll	23.03.16 23-25	503064	529	0d29e4b8b4d90b0e59d1ade22899f0630f
49	SnSrvKrn.dll	23.03.16 23-25	178968	205	aa22ecfd30334da4d956c32f9b48a8d73f
50	SnSrvLib.dll	23.03.16 23-25	1067288	1655	9a9777d79398b06dcf9f5a8bcbd2be66e9
51	SnSrvLog.dll	23.03.16 23-25	188184	216	0bf977e18ecebf030b4e0b6a51ede63eae
52	SnTmCard.dll	23.03.16 23-25	109336	226	e773c76f788130dbca5d0e35aba02f09a3
53	SnTmlEdit.exe	23.03.16 23-10	1235224	2107	08c35cd3ca9737295887de31cb2dcaa7ae
54	SnUsers.dll	23.03.16 23-26	2026264	3326	54116e96ab6ce5d460fc72f996cceb6b46
55	SnVChannelClient.dll	23.03.16 23-26	82200	124	ff2874a0181a0b7cfab7da543c12aa0c95
56	TblRescue.exe	23.03.16 23-11	2501400	3761	ec57a12e897a2f35fcc5191f22bdafa84d
57	uc.dll	23.03.16 23-26	1111320	2250	9f434dcdd37d90f95cd267744f0983d04d
58	xerces-c_2_5_0.dll	23.03.16 23-26	1896728	7670	6e7f7202d35c5595d49c1c63245929b1ae
59	XmlDocument.dll	23.03.16 23-26	280856	689	9b044b0597895a58dbb780a55cbbdfa092
итого: файлов - 59			**43803391**	**89869**	**45d6ccd0c43da0104cf09bfe2f941adfe7**
Каталог C:\Program Files\Secret Net\Client\Grouppolicy					
60	Setup Security.inf	23.03.16 17-33	5519	220	9af60725747cca9a05bc057d871924f6ee
итого: файлов - 1			**5519**	**220**	**9af60725747cca9a05bc057d871924f6ee**
Каталог C:\Program Files\Secret Net\Client\virtualprinter					
61	SnXpsfsf.dll	23.03.16 23-05	242968	378	65e2c420cd1513e518cc574d1ca6c572da
62	SnXpsVP.dll	23.03.16 23-05	2098968	2514	93a786f685a68a3c2f7126e73239e4d158
63	SnXpsVP.inf	23.03.16 23-05	3090	75	fc74e24d5a2e738868aa99d1ab2f4f92d5
итого: файлов - 3			**2345026**	**2967**	**f4fd2c63ace910a9afe71605f90ef8d507**
Каталог C:\Program Files\Secret Net\TmCardDrv					
64	SnTmCardDrv.inf	23.03.16 23-04	3395	126	6032837802e3b4fd0ee37bd4416b400e30
65	SnTmCardDrv.sys	23.03.16 23-04	23792	99	ac9f1c299e5ac8e94793449ea812bd47fa
66	WdfCoInstaller01009.dll	14.07.09 13-27	1461992	5663	cdd332effaf81000cb34c9a637335fc7d1
67	WUDFUpdate_01009.dll	14.07.09 13-21	1837296	7055	73066616c3ba48de31163293a81bac7e7c
итого: файлов - 4			**3326475**	**12943**	**4caa37a65defd4c451c0baabc8cb089a77**
ВСЕГО: файлов - 67			**49480411**	**105999**	**1f7336fe41914e175153702b77863e4453**
Конец					

Антивирусное СЗИ «Kaspersky Endpoint Security 8 для Windows» (для «Сервер»)
(Уровень-2, программно)

№	Имя файла	Дата создания	Длина, байт	Длина, строк	КС
Каталог C:\Program Files\Kaspersky Lab\Kaspersky Endpoint Security 10 for Windows SP1					
1	ACAssembler.dll	10.11.15 20-16	359344	969	833be1b2
2	ac_facade.dll	10.11.15 20-16	171440	302	e6395a17
3	ac_meta.dll	10.11.15 20-16	442288	474	33551d1e
4	am_facade.dll	10.11.15 20-16	370096	492	cd548b98
5	am_meta.dll	10.11.15 20-16	284080	280	34c4b8cc
6	application_categorizer.dll	10.11.15 20-16	187824	364	667b469c
7	app_core_legacy.dll	10.11.15 20-16	1106864	2082	3cd02547

8	app_core_meta.dll	10.11.15 20-16	352688	311	bb4df77b
9	attestation_task.dll	10.11.15 20-16	113584	244	d6754b4b
10	avp.exe	10.11.15 20-20	1194320	1950	382572f1
11	AVPCon.dll	10.11.15 20-15	1536432	1896	5b7796bb
12	avpsus.exe	10.11.15 20-16	2481072	3805	32fc3757
13	avzkrnl.dll	10.11.15 20-16	2146736	4175	a7d60248
14	cbi.dll	10.11.15 20-42	30224	80	82eec019
15	ckahcomm.dll	10.11.15 20-15	59824	98	2b72d100
16	ckahrule.dll	10.11.15 20-16	119216	99	40cbde06
17	ckahum.dll	10.11.15 20-15	241072	633	9d76db77
18	clldr.dll	10.11.15 20-17	23472	74	1321346a
19	dblite.dll	10.11.15 18-50	478904	1410	41c12025
20	dns_client.dll	10.11.15 20-17	131504	300	0743f8b1
21	dtp_lib.dll	10.11.15 20-15	58288	492	73ba9281
22	DumpWriter.dll	10.11.15 20-15	776112	2100	11e90622
23	ekasyswatch.dll	10.11.15 20-17	111536	235	b72ccd2a
24	eka_meta.dll	10.11.15 20-17	244144	413	d0d6dc71
25	EncryptionCommon.dll	10.11.15 20-15	360368	566	699107ce
26	EncryptionGeneral.dll	10.11.15 20-15	17328	69	963da0b5
27	excludemanager.dll	10.11.15 20-17	169904	308	28be0ba6
28	filesystem_services.dll	10.11.15 20-17	445872	809	314103a0
29	format_recognizer.dll	10.11.15 20-17	589744	1269	74b4517b
30	fssync.dll	10.11.15 20-20	100656	203	c171d7a7
31	fssync_s.dll	10.11.15 20-20	145712	347	38ced133
32	ftbridge.dll	10.11.15 20-17	233904	329	aa8e5a4c
33	GetSI.dll	10.11.15 20-15	206768	332	dbe9cb37
34	ichecker.dll	10.11.15 20-17	168880	362	22f54016
35	instrumental_meta.dll	10.11.15 20-17	97712	223	3bf02f78
36	integrity_control.dll	10.11.15 20-17	108464	262	ed85549a
37	key_value_storage.dll	10.11.15 20-17	611760	1801	6a4caabd
38	kldw.exe	10.11.15 20-20	778712	2109	dbb508c1
39	klifpp.dll	10.11.15 20-17	1508784	3218	7fdc859e
40	klifpp_meta.dll	10.11.15 20-17	123312	210	bbf6a0f6
41	ksn_facade.dll	10.11.15 18-52	1359616	2398	0d97b235
42	ksn_meta.dll	10.11.15 18-52	206080	219	5bd15841
43	libeay32.dll	10.11.15 20-17	1357744	3928	f30b1497
44	libola.dll	10.11.15 20-17	597936	1462	14291f7f
45	licensing_meta.dll	10.11.15 20-17	185776	286	b6e45265
46	licensing_product_facade.dll	10.11.15 20-17	992176	3998	38b17385
47	localization_manager.dll	10.11.15 20-17	525232	556	77b44411
48	mailer.dll	10.11.15 20-17	76208	158	48dc45a0
49	MAPIEDK.dll	10.11.15 20-16	97712	235	746004e1
50	memmon.dll	10.11.15 20-17	86448	185	97276249
51	modify_watcher.exe	10.11.15 20-18	278448	398	e20a403a
52	msvcp100.dll	10.11.15 18-50	421200	769	a6486ef6
53	msvcr100.dll	10.11.15 18-50	773968	1691	ecd1406f
54	network_services.dll	10.11.15 20-18	634288	1529	633dde6e

55	packed_io.dll	10.11.15 20-18	47024	122	ff374bd0
56	patch_management_facade.dll	10.11.15 20-18	660912	1103	f7925177
57	patch_management_meta.dll	10.11.15 20-18	336304	402	c4b808ba
58	persistent_queue.dll	10.11.15 20-18	588208	1697	879a2b40
59	platform_metainfo.dll	10.11.15 20-18	561072	456	9dfd9926
60	prloader.dll	10.11.15 20-18	366000	524	9eb37663
61	ProcessMonitor.dll	10.11.15 20-18	665520	1151	70611c7d
62	prremote.dll	10.11.15 20-18	228784	350	9fc46616
63	remote_eka_prague_loader.dll	10.11.15 20-18	208304	424	5e8813e1
64	sax_xml_parser.dll	10.11.15 20-18	148400	415	a2b4ad01
65	self_defence.dll	10.11.15 20-18	150448	271	7997bf14
66	service.dll	10.11.15 20-18	634288	1196	2196db76
67	shellex.dll	10.11.15 20-16	177072	209	9cad0832
68	ssleay32.dll	10.11.15 20-18	286640	652	4f7997e5
69	storage.dll	10.11.15 20-18	254384	447	2e2c6bbe
70	swpragueplugin.dll	10.11.15 20-18	102320	206	ccf53965
71	tcg_log_provider.dll	01.07.15 20-25	77056	152	e4a15a32
72	ThreatsManager.dll	10.11.15 20-16	207792	311	0cc6bf1f
73	threats_disinfection.dll	10.11.15 20-18	525232	768	368d11a7
74	updater.dll	10.11.15 20-16	1048496	1415	27045d9a
75	updater_facade.dll	10.11.15 20-18	1412528	2149	6a17f499
76	updater_meta.dll	10.11.15 20-18	507824	600	b60ed60b
77	ushata.dll	10.11.15 20-16	71088	204	dced2cee
78	vul_scan.dll	10.11.15 20-18	285104	584	fe84053a
79	vul_strg.dll	10.11.15 20-18	278960	412	68bd3154
80	win8_api.dll	15.10.13 16-24	82112	180	6bf8d685
81	wmi32.exe	10.11.15 20-20	19600	71	e2cc55e0
итого: файлов - 81			**36213248**	**69978**	**43ba92c8**
Каталог C:\Program Files\Kaspersky Lab\Kaspersky Endpoint Security 10 for Windows SP1\kl1_x86					
82	kl1.inf	18.06.15 21-58	1663	84	7fdc94a8
83	kl1.sys	11.09.15 20-30	155304	347	9b15d440
итого: файлов - 2			**156967**	**431**	**1af268e9**
Каталог C:\Program Files\Kaspersky Lab\Kaspersky Endpoint Security 10 for Windows SP1\klif_x86_nt501					
84	klflt.sys	30.09.15 16-55	92528	284	0b38357a
85	klif.inf	25.09.15 12-17	4020	141	68703c1e
86	klif.sys	30.09.15 16-55	660872	1517	34a901b5
итого: файлов - 3			**757420**	**1942**	**a751734d**
Каталог C:\Program Files\Kaspersky Lab\Kaspersky Endpoint Security 10 for Windows SP1\KLIMX86					
87	klim5.inf	15.05.15 14-18	2435	97	4781fb9f
88	klim5.sys	13.08.15 14-22	41824	177	fee588be
89	klim5_m.inf	15.05.15 14-18	1594	79	9af6f8a3
итого: файлов - 3			**45853**	**353**	**df5d7d02**
Каталог C:\Program Files\Kaspersky Lab\Kaspersky Endpoint Security 10 for Windows SP1\klogon_x86					

90	klogon.dll	10.11.15 20-17	201136	603	0b76642f
91	klogon.inf	10.11.15 18-50	1641	80	6f4c52d7
итого: файлов - 2			**202777**	**683**	**7ac2b606**
Каталог C:\Program Files\Kaspersky Lab\Kaspersky Endpoint Security 10 for Windows SP1\kltdi_x86					
92	kltdi.inf	10.06.15 15-28	1371	71	43795159
93	kltdi.sys	11.06.15 15-52	54328	189	30eec124
итого: файлов - 2			**55699**	**260**	**7367137e**
Каталог C:\Program Files\Kaspersky Lab\Kaspersky Endpoint Security 10 for Windows SP1\kneps_x86					
94	kneps.inf	10.08.15 18-03	1283	66	89308971
95	kneps.sys	11.09.15 18-18	155304	329	f3988256
итого: файлов - 2			**156587**	**395**	**7cc90bc8**
Каталог C:\Program Files\Kaspersky Lab\Kaspersky Endpoint Security 10 for Windows SP1\Skin\loc\en					
96	fdert_loc.dll	10.11.15 20-40	62384	243	70506e89
97	pmv_loc.dll	10.11.15 20-40	22960	77	60ffffe2
98	sfx_loc.dll	10.11.15 20-40	13744	56	09f6fbea
итого: файлов - 3			**99088**	**376**	**d9456a57**
Каталог C:\Program Files\Kaspersky Lab\Kaspersky Endpoint Security 10 for Windows SP1\Skin\loc\ru					
99	fdert_loc.dll	10.11.15 20-40	70576	257	26842892
100	pmv_loc.dll	10.11.15 20-40	23984	74	b0dc677a
101	sfx_loc.dll	10.11.15 20-40	13744	55	65ad1371
итого: файлов - 3			**108304**	**386**	**3b0ea47d**
Каталог C:\Program Files\Kaspersky Lab\Kaspersky Endpoint Security 10 for Windows SP1\x86					
102	expsrv.dll	10.11.15 18-50	380957	1454	be24d021
103	mfc42.dll	10.11.15 18-50	1019959	1470	574bbba1
104	msvbvm50.dll	10.11.15 18-50	1355776	4267	b2e3e0be
105	msvbvm60.dll	10.11.15 18-50	1392671	3480	007fa56b
106	msvcp60.dll	10.11.15 18-50	401462	165	86843a57
107	msvcp80.dll	10.11.15 18-50	548864	596	728f22bf
108	msvcr80.dll	10.11.15 18-50	626688	1309	28289ab9
итого: файлов - 7			**5726377**	**12741**	**e70e09be**
ВСЕГО: файлов - 108			**43522320**	**87545**	**47b2d9e1**
Конец					

7. ВЫВОДЫ АТТЕСТАЦИОННОЙ КОМИССИИ

По результатам аттестационных испытаний комиссия считает, что:

7.1. Перечень представленных нормативных и организационно-распорядительных документов достаточен и их содержание соответствует требованиям стандартов и других нормативных документов по безопасности информации ФСТЭК России, ФСБ и иных органов государственного управления в пределах их компетенции;

7.2. Реализация требований предписания на эксплуатацию ОТСС и применение сертифицированных СЗИ от НСД обеспечивает выполнение установленных требований по защите информации при использовании технических и программных средств вычислительной техники;

7.3. Состав и структура программно-технических средств автоматизированной системы соответствует представленной документации;

7.4. Классификация автоматизированной системы проведена без нарушений требований руководящих документов ФСТЭК (Гостехкомиссии) России;

7.5. Помещение, в котором расположены ОТСС, отвечает требованиям руководящих документов, предъявляемым к рабочим помещениям, в которых устанавливаются СВТ для обработки информации с ограниченным доступом;

7.6. Допуск персонала к работе обеспечивается в рамках действующей в организации разрешительной системой и в соответствии с возложенными на персонал функциями;

7.7. Уровень подготовки персонала позволяет реализовать установленные для данного объекта информатизации требования по безопасности информации.

8. ЗАКЛЮЧЕНИЕ

Учитывая вышеизложенное, комиссия считает, что реализованные средства и меры защиты информации на объекте информатизации ГИС «Аэропорт», размещенной по адресу: г. Челябинск, Аэропорт, второй этаж здания УралАэронавигации, кабинет № 202, достаточны и соответствуют требованиям действующих нормативных документов по безопасности информации, предъявляемых к государственным информационным системам класса защищенности «**К3».**

Комиссия считает возможным выдать на аттестуемый объект информатизации «Аттестат соответствия…» на право обработки информации ограниченного доступа в соответствии с установленным классом защищенности ГИС и классом защищенности АС от НСД сроком на 5 лет.

Председатель комиссии	_____	К.С. Рыжов
Члены комиссии	_____	С.В. Евдокимов
	_____	Л.О. Овчинникова

ПРИЛОЖЕНИЕ Г
Аттестат соответствия

АКЦИОНЕРНОЕ ОБЩЕСТВО
ГРАНИТ ИНФОРМ

454006, г. Челябинск, ул. Красноармейская, 55
тел (351) 218 28 28, эл. почта: info@g-inform.ru

УТВЕРЖДАЮ
Руководитель органа по аттестации
объектов информатизации
АО «Гранит Информ»

_____ Н.В. Узбеков

«____»_____ 2017 г.

АТТЕСТАТ СООТВЕТСТВИЯ

на объект информатизации

государственная информационная система

«Аэропорт»

Челябинского центра ОВД «Аэронавигация Урала»

ФГУП «Госкорпорация по ОрВД».

Выдан: 1 мая 2017 г.

Действителен до: 1 мая 2020 г.

2017 г.

1. Настоящим Аттестатом удостоверяется, что объект информатизации (ОИ) государственная информационная система «Аэропорт» Челябинского центра ОВД «Аэронавигация Урала» ФГУП «Госкорпорация по ОрВД» (далее ГИС) класса защищенности государственных информационных систем «К3», размещенная по адресу: г. Челябинск, Аэропорт, второй этаж здания УралАэронавигации, кабинет № 202, соответствует требованиям нормативной документации по безопасности информации.

Состав комплекса технических средств ГИС, схема размещения в помещении и относительно границ контролируемой зоны, перечень используемых программных средств, а также средств защиты приведены в техническом паспорте на объект информатизации.

2. Организационная структура, уровень подготовки специалистов, нормативно-методическое обеспечение и техническая оснащённость организации обеспечивают контроль эффективности мер и средств защиты и поддержание уровня защищённости ГИС в процессе эксплуатации в соответствии с установленными требованиями.

3. Аттестация ГИС выполнена в соответствии с программой и методикой аттестационных испытаний, утвержденными руководителем органа по аттестации.

4. С учетом результатов аттестационных испытаний ГИС разрешается обработка информации ограниченного доступа.

5. При эксплуатации ГИС запрещается:

- нарушать требования предписаний на эксплуатацию оборудования;
- заменять размещенные технические средства, изменять их комплектацию.

6. Контроль за эффективностью реализованных мер и средств защиты возлагается на ответственного за обеспечение безопасности персональных данных.

7. Подробные результаты аттестационных испытаний приведены в заключении по результатам аттестационных испытаний.

8. «Аттестат соответствия» выдан на три года, в течение которых должна быть обеспечена неизменность условий функционирования ГИС и технологии обработки защищаемой информации, способных повлиять на характеристики, указанные в п. 10.

9. При окончании срока действия сертификата соответствия ФСТЭК России на средство защиты информации, должна проводиться процедура продления срока действия сертификата соответствия. Эта процедура осуществляется производителем средства защиты информации (разработчиком). Если производитель не осуществляет продление срока действия сертификата соответствия, продление должно осуществляться организацией, эксплуатирующей средство защиты информации, в индивидуальном порядке. Порядок продления срока действия сертификатов соответствия организациями, эксплуатирующими средства защиты информации,

определен в документе ФСТЭК России «Информационное сообщение по вопросу продления сроков действия сертификатов соответствия на средства защиты информации, эксплуатируемые на объектах информатизации» № 240/24/223 от 23 января 2015 г.

10. Перечень характеристик, об изменении которых требуется обязательно извещать орган по аттестации:

- состав оборудования ОИ;
- условия размещения ОИ и его технических средств;
- характеристики систем (защиты информации, электропитания, заземления, сигнализации) обеспечения эксплуатации ОИ.

11. При эксплуатации ГИС запрещается:

- вносить изменения в комплектность ГИС, которые могут снизить уровень защищенности информации;
- проводить обработку защищаемой информации без выполнения всех мероприятий по защите информации;
- подключать к основным техническим средствам нештатные блоки и устройства;
- допускать к обработке защищаемой информации лиц, не оформленных в установленном порядке;
- производить копирование защищаемой информации на неучтенные носители информации, в том числе для временного хранения информации;
- обрабатывать на ПЭВМ защищаемую информацию при обнаружении каких-либо неисправностей.

Руководитель аттестационной комиссии _____ К.С. Рыжов

«_____»_____2017 г.

Отметки органов контроля:
