|  |  |
| --- | --- |
|  | УТВЕРЖДАЮ  Генеральный директор  ООО "БД Безопасность"  « » \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2025 г. |

ТЕХНИЧЕСКИЙ ПАСПОРТ

объекта вычислительной техники

автоматизированная система АРМ РСП ОО моб.№21

ООО "БД Безопасность"

1. Общие сведения об объекте вычислительной техники

1.1. Наименование и назначение объекта вычислительной техники: информационная система АРМ РСП ОО моб.№21, предназначена для обработки информации, содержащую сведения уровня секретности не выше «Совершенно секретно».

1.2. Расположение объекта вычислительной техники: в Кабинет 201 на этаже -этажного административного здания по у: .

1.3. Установленная категория объекта вычислительной техники: 2  
(Акт категорирования объекта вычислительной техники от ).

1.4. Установленный класс защищенности от несанкционированного доступа: 2А   
(Акт классификации АС АРМ РСП ОО моб.№21№ от )

1.5. Сведения о вводе объекта вычислительной техники в эксплуатацию: Автоматизированная система АРМ РСП ОО моб.№21 ООО "БД Безопасность" введена в эксплуатацию с « » \_\_\_\_\_\_\_\_\_20\_\_ г., приказ № \_\_\_\_\_   
от « » \_\_\_\_\_\_\_\_ 20\_\_ г.

2. Условия расположения и эксплуатации объекта вычислительной техники

2.1. Сведения об объекте вычислительной техники и его структурная (топологическая) схема

ОТСС объекта информатизации представляют собой автоматизированное рабочее место, состоящее из ПЭВМ (моноблока, манипулятора «мышь», клавиатура) и МФУ, подключенные к сети электропитания. Объект размещен компактно в Кабинет 201 на этаже -этажного административного здания по у: , .



Рисунок 1. Структура схема объекта вычислительной техники

2.2. Описание технологического процесса обработки информации:

Технологический процесс обработки информации, составляющей сведения, содержащие государственную тайну, в автоматизированной системе АРМ РСП ОО моб.№21 ООО "БД Безопасность" (АС) организуется в целях:

- автоматизации сбора, обработки, хранения информации, составляющей сведения, содержащие государственную тайну;

- разработки, оформления документов, содержащих сведения, составляющие государственную тайну;

- обеспечения в АС необходимого уровня безопасности при обработке и хранении информации, составляющей сведения, содержащие государственную тайну.

Основными задачами являются:

- обеспечение в АС ограничения доступа к защищаемым сведениям;

- антивирусная защита операционной системы (далее ОС) и прикладного программного обеспечения;

- регистрация пользователей в СЗИ НСД перед началом сеанса работы на ПЭВМ и назначение им прав доступа к защищаемым ресурсам;

- работа с файлами документов, содержащими сведения, составляющие государственную тайну, внесение корректировок, их уничтожение и хранение;

- работа с внешними носителями информации ограниченного доступа;

- резервное копирование, восстановление информации;

- архивное хранение информации, содержащей сведения, составляющие государственную тайну.

Объектами доступа к защищаемой информации являются технические средства АС:

- оперативная память ПЭВМ;

- CD/DVD-ROM Drive;

- дисковые накопители, экран монитора с отображаемой на нем информацией, распечатки c принтера, флеш-накопители;

- оптические диски с расположенными на них файлами.

Субъектами доступа к защищаемой информации являются:

- администратор безопасности информации;

- пользователи, работающие на ПЭВМ;

- процессы, выполняемые на ПЭВМ от имени администратора безопасности информации и пользователей при обработке информации и настройке СЗИ.

К работе на ПЭВМ допущены три категории пользователей:

- сотрудники, обрабатывающие информацию ограниченного доступа;

- обслуживающий персонал (системный администратор и др.);

- администратор безопасности.

Состав сотрудников, перечень информационных ресурсов, программных и технических средств, с указанием полномочий доступа, изложены в разрешительной системе доступа к информационным ресурсам, программным и техническим средствам автоматизированной системы «АРМ-1».

Штатными средствами доступа к информации являются общесистемные и прикладные программы из перечня программных средств (см. выше).

Полномочия пользователей по доступу к объектам штатными средствами реализованы средствами системы защиты и организационно-режимными мерами. Настройку системы защиты от НСД и для конкретных пользователей и контроль ее работы осуществляет администратор безопасности.

Структурная схема АС с указанием информационных потоков представлена на Рисунке 2.



Рисунок 2. Схема информационных потоков

Перед началом сеанса работы пользователь включает ПЭВМ и проходит процедуру идентификации и аутентификации в СЗИ НСД. Т. е. загрузка ПЭВМ осуществляется по имени и паролю конкретного пользователя с регистрацией в журнале учета программного средства защиты от НСД. По окончании загрузки компьютера пользователь получает установленные администратором безопасности права доступа к устройствам, каталогам, файлам и программам.

Файлы документов готовятся, хранятся на рабочем месте пользователя, на носителях информации, в каталогах, перечисленных в Описании системы разграничения доступа и настроек системы защиты информации от несанкционированного доступа АС АРМ РСП ОО моб.№21 ООО "БД Безопасность".

Работа с документами (письма, отчеты и т.д.) производится с применением штатных средств АС.

Для хранения файлов с секретными данными могут также использоваться CD/DVD диски, имеющие соответствующий гриф секретности и учтенные соответствующим образом.

Удаленные файлы уничтожаются специальной программой для очистки областей памяти на магнитных носителях информации, входящей в состав, установленной на ПЭВМ СЗИ от НСД . Информация гарантированно уничтожается двумя циклами затирания.

Резервное копирование информационных ресурсов (баз данных) производится администратором безопасности на оптический диск (CD/DVD), вторую копию - на съёмный ЖМД в отдельные папки. При хранении резервных копий выполняются требования «Инструкции по обеспечению режима секретности в Российской Федерации», утвержденной Постановлением Правительства РФ от 05.01.2004 г. № 3-1. В случае сбоев в работе ПЭВМ, которые привели к искажению или удалению информации, восстановление информации производится администратором безопасности из каталога жесткого диска, либо с CD/DVD.

Завершение сеанса работы пользователь производит выполнением процедуры завершения сеанса работы в , выключает ПЭВМ и сдает имеющиеся рабочие диски и дискеты в специально оборудованное хранилище.

Функции, права, обязанности и порядок работы на ПЭВМ пользователей регламентируется Инструкцией по обеспечению режима секретности при обработке секретной информации (по обеспечению безопасности информации) в автоматизированной системе АРМ РСП ОО моб.№21 ООО "БД Безопасность", инструкциями по работе пользователей в автоматизированной системе.

2.3. Сведения и расположение основных технических средств и систем и средств защиты информации относительно границ контролируемой зоны

Границы контролируемой зоны проходят по ограждающим конструкциям административного здания администрации по адресу: , (см. рис. 3).

Рисунок 3. Размещение ОТСС относительно границ контролируемой зоны

Размещение расположение линий и коммуникаций представлены на рисунке (см. рис. 4, 5).

Через помещение проходят трубы системы отопления, выходящие за пределы контролируемой зоны; линии охранной и пожарной сигнализации, не выходящие за пределы контролируемой зоны.

Рисунок 4. Расположение линий коммуникаций

2.4. Сведения и схемы системы электроснабжения и заземления объекта вычислительной техники

Электропитание АС осуществляется от трансформаторной подстанции, расположенной вне контролируемой зоны. К фидеру, питающему здание, подключены посторонние потребители электроэнергии. Кабели питания разведены к этажному электрическому щиту, откуда питание подается на объект.

Контур заземления находится вне контролируемой зоны. Сопротивление заземления составляет менее 4 Ом.

Схемы электропитания розеточной и осветительной сети объекта представлены на рисунке (см. рис. 5).

Рисунок 5. Системы электропитания и заземления

3. Состав объекта вычислительной техники

3.1. Состав основных технических средств и систем объекта вычислительной техники представлен в таблице 1\*

Таблица 1

| №  п/п | Наименование основного технического средства | Заводской (инвентарный) номер | Минимальное расстояние до границы контролируемой зоны, м | Номер помещения, в котором размещено ОТСС |
| --- | --- | --- | --- | --- |
| {{DYNAMIC\_TABLE::HardwareList}} |  |  |  |  |

\* В таблицу 1 не включаются машинные носители информации, содержащие контроллеры (флеш-накопители, съемные жесткие диски).

3.2. Состав средств защиты информации, используемых на объекте вычислительной техники, представлен в таблице 2.

Таблица 2

| №  п/п | Наименование и тип средства защиты информации | Заводской (инвентарный) номер | Сведения о сертификате соответствия, знак соответствия | Место установки |
| --- | --- | --- | --- | --- |
| {{DYNAMIC\_TABLE::SZIList}} |  |  |  |  |

3.3. Состав программного обеспечения основных технических средств и систем объекта вычислительной техники представлен в таблице 3

Таблица 3

| № п/п | Наименование программного средства | Место (основное техническое средство и система) установки |
| --- | --- | --- |
| {{DYNAMIC\_TABLE::SoftwareList}} |  |  |

4. Сведения о соответствии объекта вычислительной техники требованиям по безопасности информации

4.1. Сведения о соответствии основных технических средств и систем требованиям по безопасности информации приведены в таблице 4

Таблица 4

| № п/п | Наименование, модель, заводской номер | Сведения о сертификатах соответствия | Сведения о специальных проверках \* | Сведения о специальных исследованиях \* |
| --- | --- | --- | --- | --- |
| {{DYNAMIC\_TABLE::SPSIList}} |  |  |  |  |

\* Документы, содержащие сведения о специальных исследованиях и проверках (номера пунктов соответствуют номерам документов):

4.2. Сведения об оценке эффективности принятых мер по технической защите информации на объекте вычислительной техники:

Таблица 5

|  |  |  |  |
| --- | --- | --- | --- |
| №  п/п | Дата проведения | Наименование организации, проводившей исследования | Номер и дата заключения |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

4.3. Сведения об аттестации объекта вычислительной техники на соответствие требованиям по безопасности информации:

Таблица 6

|  |  |  |  |
| --- | --- | --- | --- |
| №  п/п | Наименование аттестатов, заключений, протоколов | № и дата документа | Наименование организации, проводившей испытания |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

5. Сведения о внутреннем контроле состояния технической защиты информации на объекте вычислительной техники приведены в таблице 7

Таблица 7

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| №  п/п | Наименование организации, проводившей контроль | Дата проведения контроля | Реквизиты акта | Вывод по результатам контроля |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

6. Сведения об изменениях состава, условий размещения и эксплуатации объекта вычислительной техники и средств защиты информации приведены в таблице 8.

Таблица 8

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № п/п | Дата введения изменений | Документ, на основании которого внесены изменения | Пункт технического паспорта, в который внесены изменения | Краткая характеристика изменений | Подпись лица, внесшего изменения |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

Ответственный за эксплуатацию объекта вычислительной техники

|  |  |
| --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (должность) | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (подпись, фамилия, инициалы) |
| « »\_\_\_\_\_\_\_\_\_\_\_\_\_20\_\_\_ г. |  |