Экз. №\_\_\_

ООО «Ромашка»

**Описание технологического процесса обработки информации ограниченного доступа**

автоматизированной системы «АС»

**ОГЛАВЛЕНИЕ**

[Термины и определения 3](#_Toc506306083)

[1. Общие положения 4](#_Toc506306084)

[2. Описание объекта информатизации 5](#_Toc506306085)

[2.1. Общие сведения 5](#_Toc506306086)

[2.2. Назначение и решаемые задачи 6](#_Toc506306087)

[2.3. Состав программного обеспечения, участвующего в технологическом процессе обработки информации 6](#_Toc506306088)

[2.4. Класс защищенности автоматизированной системы 6](#_Toc506306089)

[3. Организация работы с конфиденциальной информацией 7](#_Toc506306090)

[3.1. Доступ пользователя к работе в автоматизированной системе 7](#_Toc506306091)

[3.1.1. Режим доступа пользователей 7](#_Toc506306092)

[3.1.2. Регистрация пользователей и назначение прав доступа 7](#_Toc506306093)

[3.1.3. Начало работы 7](#_Toc506306094)

[3.2. Настройка средств защиты информации от несанкционированного доступа для конкретных пользователей 8](#_Toc506306095)

[3.3. Обработка информации, содержащей сведения конфиденциального характера 8](#_Toc506306096)

[3.4. Хранение документов конфиденциального характера 9](#_Toc506306097)

[3.5. Хранение съемных носителей 9](#_Toc506306098)

[3.6. Печать, сканирование и копирование с бумажных носителей 9](#_Toc506306099)

[3.7. Удаление электронных документов, содержащих конфиденциальную информацию, со съемных носителей и жестких дисков 9](#_Toc506306100)

[3.8. Уничтожение съемных носителей 10](#_Toc506306101)

[4. Описание технологического процесса обеспечения информационной безопасности 11](#_Toc506306102)

[4.1. Защита от несанкционированного доступа 11](#_Toc506306103)

[4.2. Антивирусная защита 14](#_Toc506306104)

[4.3. Обеспечение целостности и доступности информации 14](#_Toc506306105)

Термины и определения

**Автоматизированное рабочее место** – программно-технический комплекс автоматизированной системы, предназначенный для автоматизации деятельности определенного вида (ГОСТ 34.003-90).

**Безопасность информации** - Состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность (ГОСТ Р 50922-2006).

**Защита информации** – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию (ГОСТ Р 50922-2006).

**Защищаемая информация** - Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации. (ГОСТ Р 50922-2006).

**Информационная система** – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств (Федеральный закон Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»).

**Информация ограниченного доступа** – информация, доступ к которой ограничен федеральными законами (Федеральный закон Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»).

**Средство вычислительной техники** – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

**Средство защиты информации** – техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации (ГОСТ Р 50922-2006).

1. Общие положения

Настоящий документ представляет собой описание технологического процесса обработки и защиты информации в автоматизированной системе АС «Pharmacy» ООО «Ромашка» (далее – АС).

1. Описание объекта информатизации
   1. Общие сведения

Автоматизированная система АС «Pharmacy» расположена по адресу: Российская федерация, г. Клин, р-н Клинский, 8 и представляет собой выделенное автоматизированное рабочее место на базе ПЭВМ, подключенное к корпоративной вычислительной сети ООО «Ромашка».

Перечень основных технических средств и систем АС представлен в Таблице 2

| **№**  **п/п** | **Наименование и тип ОТСС** | **Модель** | **Заводской (инвентарный) номер** | **Размещение ОТСС на объекте** |
| --- | --- | --- | --- | --- |
|  | **АРМ в составе:** | | | Помещение № 10 |
| Системный блок |  |  |
| Монитор |  |  |
| Клавиатура |  |  |
|  | Системный блок |  |  |  |
| Монитор |  |  |
| Клавиатура |  |  |
|  | Системный блок |  |  |  |
| Монитор |  |  |
| Клавиатура |  |  |

АРМ АС функционирует под управлением операционной системы Windows 10.

Защита АС осуществляется сертифицированными СЗПДн «Pharmacy» и антивирусным программным обеспечением Kaspersky Endpoint Security 10, а также встроенными средствами системного и прикладного программного обеспечения.

В АС не осуществляется прием и (или) передача информации конфиденциального характера по каналам связи.

Все субъекты доступа АС являются работниками компании и подразделяются  
на 3 категории:

* пользователи – ответственные за обработку конфиденциальной (содержащей сведения ограниченного распространения) и открытой информации в АС.
  1. Назначение и решаемые задачи

Автоматизированная система «АС» «Pharmacy» предназначена для обработки конфиденциальных документов ООО «Ромашка».

К основным задачам АС относятся:

* Учет лекарств в аптеке;
* Учет проданного товара;

В АС не осуществляется обработка составляющей государственную тайну.

* 1. Состав программного обеспечения, участвующего в технологическом процессе обработки информации

В составе АС применяется следующее программное обеспечение:

| **№ п.п** | **Наименование и тип программного средства** | **Серийный номер (номер лицензии)** | **Сведения о сертификате** | **Дата установки** |
| --- | --- | --- | --- | --- |
| 1 | Операционная система Windows 10 |  | Нет |  |
| 2 | Приложение АС |  | Нет |  |
| 3 | База данных |  |  |  |
| 4 | Kaspersky Endpoint Security 10 |  |  |  |

* 1. Класс защищенности автоматизированной системы

Автоматизированная система «АС» «Pharmacy» классифицирована по классу 2Б в соответствии с Руководящим документом ФСТЭК России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (Гостехкомиссия России, 1992г.).

1. Организация работы с конфиденциальной информацией
   1. Доступ пользователя к работе в автоматизированной системе
      1. Режим доступа пользователей

Режим обработки информации в АС - многопользовательский, пользователи имеют равные права доступа к защищаемым информационным ресурсам АС.

Все субъекты доступа АС являются работниками компании и относятся к одной категории:

* пользователи – ответственные за обработку конфиденциальной (содержащей сведения ограниченного распространения) и открытой информации в АС.
  + 1. Регистрация пользователей и назначение прав доступа

Регистрация пользователей и назначение прав доступа производится в соответствии с занимаемой должностью и в объеме, необходимом для выполнения ими должностных обязанностей. Зарегистрированный пользователь обладает уникальным идентификатором.

* + 1. Начало работы

Перед началом работы пользователь АС включает ПЭВМ и проходит процедуры идентификации и аутентификации с использованием персонального имени и пароля. Требования к парольной защите изложены в «Инструкции по организации парольной защиты автоматизированной системы «АС» «Pharmacy»

Процессы идентификации и аутентификации реализуются СЗПДн «Pharmacy». В качестве идентификационной информации используются доменные учетные записи.

* 1. Настройка средств защиты информации от несанкционированного доступа для конкретных пользователей

С помощью СЗПДн «Pharmacy», а также встроенных в операционную систему Microsoft Windows 10 функций системы разграничения доступа, всем субъектам доступа присвоены полномочия для допуска к информации в соответствии с принятой разрешительной системой разграничения доступа.

В АС системе средствами установленной СЗПДн реализованы правила, при которых каждый пользователь имеет доступ:

* к средствам общесистемного программного обеспечения операционной системы, обеспечивающим запуск и функционирование автоматизированной системы;
* к средствам разработки (редакторы, встроенные в операционную систему, прикладные программы пакета для разработки документов);
* к средствам антивирусной защиты;
* к персональным оптическим дискам и разделам ЖМД, предназначенным для хранения информации;
* специально выделенному Администратором безопасности каталогу общего пользования, предназначенному для временного хранения информации на ЖМД;
* к устройствам и средствам их программной поддержки, необходимым для работы с документами.

Всем пользователям, кроме Администратора безопасности, запрещен доступ к средствам настройки и изменения полномочий доступа.

Операции доступа субъектов к объектам доступа документируются средствами регистрации и учета установленной на автоматизированной системе системы защиты персональных данных.

* 1. Обработка информации, содержащей сведения конфиденциального характера

В АС обрабатывается открытая информация и информация конфиденциального характера. К информации конфиденциального характера, подлежащей защите, относятся сведения, содержащие коммерческую тайну Компании в соответствии с «Положением о коммерческой тайне ООО «Ромашка» (утверждено приказом Генерального директора ООО «Ромашка»).

К защищаемой информации в АС относится:

* Информация о системе защиты АС;
* Параметры настройки средств защиты АС;
* Документы, содержащие конфиденциальную информацию.

Обработка информации, содержащей сведения конфиденциального характера, заключается в следующем:

* Создание базы хранения информации о товарах;
* Изменение базы хранения информации о товарах;
  1. Хранение документов конфиденциального характера

Документы конфиденциального характера хранятся в электронном виде на учтенных в установленном порядке носителях.

* 1. Хранение съемных носителей

В АС не используются съемные (отчуждаемые) носители.

* 1. Печать, сканирование и копирование с бумажных носителей

Вывод на печать информации конфиденциального характера осуществляется пользователями АС в соответствии с функциональными обязанностями.

* 1. Удаление электронных документов, содержащих конфиденциальную информацию, со съемных носителей и жестких дисков

Уничтожение информации конфиденциального характера со съемных носителей и жестких дисков осуществляется в следующих случаях:

* информация подлежит удалению по причине устаревания и отсутствия необходимости ее дальнейшего хранения;
* планируется дальнейшее использование носителя в других целях, не связанных с хранением информации конфиденциального характера;
* необходимость ремонта носителя в сторонней организации.

Удаление информации со съемных носителей информации осуществляется в АС с помощью СЗПДн «Pharmacy».

* 1. Уничтожение съемных носителей

Утилизация съемных носителей информации конфиденциального характера осуществляется в случае выхода носителя из строя путем физического уничтожения. В иных случаях носитель может быть использован для хранения информации неконфиденциального характера после гарантированного уничтожения информации на носителе с помощью СЗПДн «Pharmacy».

1. Описание технологического процесса обеспечения информационной безопасности
   1. Защита от несанкционированного доступа

Защита АС от несанкционированного доступа при подключении к локальной сети обеспечивается с помощью СЗПДн «Pharmacy».

Управление доступом и регистрация действий пользователей задаются следующими параметрами настройки СЗПДн «Pharmacy»:

Таблица 1 Защитные механизмы «Library»

|  |  |
| --- | --- |
| **Параметр** | **Значение** |
| Механизм контроля устройств | Включен |
| Механизм полномочного управления доступом | Выключен |
| Механизм шифрования управляющего сетевого трафика | Выключен |
| Механизм контроля печати | Включен |
| Механизм затирания данных | Включен |
| Механизм дискреционного управления доступом | Включен |
| Механизм замкнутой программной среды | Выключен |

Таблица 2 Настройки подсистем

|  |  |
| --- | --- |
| **Параметр** | **Значение** |
| Администрирование: Локальное оповещение об НСД | определяется пользователем |
| Вход в систему: Запрет вторичного входа в систему | включен |
| Вход в систему: Количество неудачных попыток аутентификации | 3 попыток |
| Вход в систему: Максимальный период неактивности до блокировки экрана | 20 минут |
| Вход в систему: Реакция на изъятие идентификатора | нет |
| Вход в систему: Режим аутентификации пользователя | стандартная аутентификация |
| Вход в систему: Режим идентификации пользователя | смешанный |
| Журнал: Максимальный размер журнала системы защиты | 2048 кБ |
| Журнал: Политика перезаписи событий | затирать по необходимости |
| Контроль печати: Перенаправление принтеров в RDP-подключениях | разрешено |
| Контроль приложений: Перенаправление буфера обмена в RDP-подключениях | разрешено |
| Контроль приложений: Режим аудита | аудит пользовательских приложений |
| Контроль устройств: Перенаправление устройств в RDP-подключениях | разрешено |

Таблица 3 Регистрация событий

| **Параметр** | **Значение** |
| --- | --- |
| Администрирование: Включена защитная подсистема | включена |
| Администрирование: Добавлен пользователь | включена |
| Администрирование: Изменен ключ пользователя | включена |
| Администрирование: Изменен пароль пользователя | включена |
| Администрирование: Изменены параметры действующей политики безопасности | включена |
| Администрирование: Изменены параметры пользователя | включена |
| Администрирование: Отключена защита для диска | включена |
| Администрирование: Отключена защитная подсистема | включена |
| Администрирование: Удален ключ пользователя | включена |
| Администрирование: Удален пользователь | включена |
| Администрирование: Установлена защита для диска | включена |
| Вход/выход: Вход пользователя в систему | включена |
| Вход/выход: Завершение работы пользователя | включена |
| Вход/выход: Запрет входа пользователя | включена |
| Вход/выход: Идентификатор не зарегистрирован | включена |
| Вход/выход: Компьютер заблокирован системой защиты | включена |
| Вход/выход: Компьютер разблокирован | включена |
| Вход/выход: Ошибка выполнения функционального контроля | включена |
| Вход/выход: Пароль пользователя не соответствует требованиям безопасности | включена |
| Вход/выход: Пользователь возобновил сеанс работы на компьютере | включена |
| Вход/выход: Пользователь приостановил сеанс работы на компьютере | включена |
| Вход/выход: Система защиты инициировала блокировку сессии пользователя | включена |
| Вход/выход: Успешное завершение функционального контроля | включена |
| Дискреционное управление доступом: Доступ к файлу или каталогу | отключена |
| Дискреционное управление доступом: Запрет доступа к файлу или каталогу | включена |
| Дискреционное управление доступом: Изменение прав доступа | включена |
| Контроль приложений: Доступ к буферу обмена | отключена |
| Контроль приложений: Доступ к содержимому окна процесса | отключена |
| Контроль приложений: Завершение процесса | включена |
| Контроль приложений: Запрет доступа к буферу обмена | включена |
| Контроль приложений: Запрет доступа к содержимому окна процесса | отключена |
| Контроль приложений: Запрет операции перетаскивания (drag-n-drop) между процессами | отключена |
| Контроль приложений: Запуск процесса | включена |
| Контроль приложений: Операция перетаскивания (drag-n-drop) между процессами | отключена |
| Контроль целостности: Для ресурса отсутствует эталонное значение | включена |
| Контроль целостности: Изменение группы ресурсов | отключена |
| Контроль целостности: Изменение задания | включена |
| Контроль целостности: Изменение задачи | отключена |
| Контроль целостности: Исправление ошибок в базе данных | отключена |
| Контроль целостности: Нарушение целостности ресурса | включена |
| Контроль целостности: Начало обработки задания на контроль целостности | включена |
| Контроль целостности: Обнаружено нарушение целостности при обработке задания | включена |
| Контроль целостности: Ошибка при восстановлении ресурса по эталонному значению | включена |
| Контроль целостности: Ошибка при открытии базы данных контроля целостности | включена |
| Контроль целостности: Ошибка при принятии текущего значения ресурса в качестве эталонного | включена |
| Контроль целостности: Ошибка при расчете эталона | отключена |
| Контроль целостности: Ресурс восстановлен по эталонному значению | включена |
| Контроль целостности: Снятие задания КЦ с контроля | включена |
| Контроль целостности: Создание группы ресурсов | отключена |
| Контроль целостности: Создание задания | включена |
| Контроль целостности: Создание задачи | отключена |
| Контроль целостности: Текущее значения ресурса принято в качестве эталонного | включена |
| Контроль целостности: Удаление группы ресурсов | отключена |
| Контроль целостности: Удаление задания | включена |
| Контроль целостности: Удаление задачи | отключена |
| Контроль целостности: Удаление устаревших эталонных значений | включена |
| Контроль целостности: Успешная проверка целостности ресурса | включена |
| Контроль целостности: Успешное завершение задания на контроль целостности | включена |
| Контроль целостности: Установка задания КЦ на контроль | включена |
| Общие события: Информационное событие | включена |
| Общие события: Несанкционированное действие | включена |
| Общие события: Ошибка | включена |
| Общие события: Предупреждение | включена |
| Общие события: Событие | включена |
| Сеть: Запрет сетевого подключения под другим именем | включена |
| Служба репликации: Ошибка создания контекста пользователя | включена |

* 1. Антивирусная защита

Антивирусная защита на рабочих станциях и серверах АС обеспечивается лицензионным антивирусным программным обеспечением (далее – ПО) Kaspersky Total Security 10 (Компонент Kaspersky Endpoint Security для Windows).

Организация антивирусной защиты в АС производится в соответствии с «Положением об антивирусной политике» (утверждено Генеральным директором ООО «Ромашка»).

* 1. Обеспечение целостности и доступности информации

Целостность средств защиты и программных средств обработки информации обеспечивается в АС с помощью сертифицированного СЗПДн «Pharmacy». Контроль целостности выполняется путем расчета контрольных сумм файлов при загрузке ОС. Факты нарушения целостности записываются в журнал работы СЗПДн «Pharmacy».

При выходе ПЭВМ в составе АРМ из строя в результате программного сбоя или аппаратной неисправности пользователь АРМ осуществляет настройку/переустановку программного обеспечения или замену аппаратных компонентов АРМ, соответственно. Администратор информационной безопасности осуществляет установку и настройку СЗПДн в АС с имеющихся у него в наличии дистрибутивных носителей. Параметры настройки СЗПДн устанавливаются вручную в соответствии с утвержденной документацией либо автоматически путем импорта сохраненных ранее настроек СЗИ.