АДМИНИСТРАЦИЯ РОССОШАНСКОГО МУНИЦИПАЛЬНОГО РАЙОНА ВОРОНЕЖСКОЙ ОБЛАСТИ

# РАСПОРЯЖЕНИЕ

От 28.10.2016 года № 298-р

г.Россошь

О внесении изменений в распоряжение от 15.04.2015 №120-р «Об утверждении документов, регламентирующих обработку и обеспечение безопасности персональных данных»

В соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановлением Правительства Российской Федерации от 21.03.2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных», а также в связи с произошедшими в администрации Россошанского муниципального района кадровыми изменениями:

1. Внести следующие изменения в распоряжение от 15.04.2105 №120-р:
   1.1 слова инженер-программист МКУ «Служба технического обслуживания» М. В. Хорин (по согласованию) читать: инженер-программист администрации Россошанского муниципального района М. В. Хорин;
   1.2 изложить приложение №7 в новой редакции, согласно приложению № 1;
   1.3 изложить приложение №19 в новой редакции, согласно приложению № 2;

1.4 дополнить распоряжение от 15.04.2015 № 120-р приложением №20, согласно приложению № 3;

1.5 дополнить распоряжение от 15.04.2015 № 120-р приложением №21, согласно приложению № 4;

1.6 дополнить распоряжение от 15.04.2015 № 120-р приложением №22, согласно приложению № 5;

1.7 дополнить распоряжение от 15.04.2015 № 120-р приложением №23, согласно приложению № 6;

1.8 дополнить распоряжение от 15.04.2015 № 120-р приложением №24, согласно приложению № 7;

1.9 дополнить распоряжение от 15.04.2015 № 120-р приложением №25, согласно приложению № 8;

1.10 дополнить распоряжение от 15.04.2015 № 120-р приложением №26, согласно приложению № 9;

1.11 дополнить распоряжение от 15.04.2015 № 120-р приложением №27, согласно приложению № 10.

2 Контроль за исполнением настоящего распоряжения возложить на руководителя аппарата Л. А. Кушнареву.

Приложения: № 1 на 19 л. в 1 экз.;
№ 2 на 1 л. в 1 экз.;
№ 3 на 2 л. в 1 экз.;
№ 4 на 3 л. в 1 экз.;
№ 5 на 2 л. в 1 экз.;
№ 6 на 1 л. в 1 экз.;
№ 7 на 4 л. в 1 экз.;
№ 8 на 7 л. в 1 экз.;
№ 9 на 2 л. в 1 экз.;
№ 10 на 5 л. в 1 экз..

Исполняющий обязанности главы администрации С.Л.Нефедов

Приложение №3 к
распоряжению администрации
Россошанского муниципального
района Воронежской области
от г. №

**Инструкция**
**по организации антивирусной защиты в ИСПДн администрации Россошанского муниципального района Воронежской области**

## 1. Общие положения

Компьютерный вирус является разрушающей программной закладкой и характеризуется значительным деструктивным потенциалом для программ, данных и любой информации, хранящейся на компьютерах и магнитных носителях. Особую опасность представляет то обстоятельство, что компьютерные вирусы могут скрытно и постепенно уничтожать, либо мгновенно разрушать хранящуюся в компьютере и на носителях информацию, при этом также могут пострадать аппаратные средства.

Основными путями вирусного вторжения являются неквалифицированное обращение пользователей с компьютерной техникой при использовании ими зараженных носителей и программ, либо целенаправленное спланированное воздействие извне с использованием компьютерных вирусов. При любых обстоятельствах это затрагивает вопросы защиты информации и интересы администрации Россошанского муниципального района Воронежской области.

## 2.Порядок обеспечивающий безопасную работу на компьютере с носителями информации

1. Вновь поступающее программное обеспечение должно быть подвергнуто входному контролю - проверке на отсутствие вирусов и проверке соответствия длины и контрольных сумм, если таковые указаны в сопроводительных документах, полученным длинам и контрольным суммам.
2. Допуск сотрудников к самостоятельной работе на компьютерах и с внешними носителями осуществляется только после овладения ими навыками работы с компьютером, антивирусными

пакетами программ.

3. На компьютерах может использоваться программное и аппаратное обеспечение, необходимое только для выполнения служебной деятельности. Запрещается использовать на компьютерах программные и аппаратные средства, не согласованные с целями обработки информации ограниченного доступа.

4. В обязательном порядке должен быть установлен и активирован пакет антивирусных программ. Ответственность за это несет администратор безопасности ИСПДн. Установка средств антивирусного
контроля (в том числе настройка параметров средств антивирусного контроля) осуществляется в соответствии с руководствами по применению конкретных антивирусных средств. Антивирусные средства устанавливаются при вводе в эксплуатацию ИСПДн или при их плановой замене.

5. Периодически пользователь проверяет его дисковое пространство с использованием анти-

6. Пользователь (в случае необходимости совместно с администратором безопасности) обязан проводить антивирусный контроль любой электронной информации (текстовые файлы любых форматов, файлы данных, исполняемые файлы, архивируемые/разархивируемые файлы и т.д.), получаемой на съемных носителях (магнитных дисках, оптических носителях, Flash - память и т.п.).

7. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора безопасности ИСПДн, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;
- совместно с администратором безопасности провести анализ необходимости дальнейшего использования зараженных вирусом файлов;
- провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь администратора безопасности).

Все факты обнаружения зараженных вирусом файлов администратор безопасности заносит в «Журнал регистрации работ по антивирусной защите и выявления вирусного заражения в ИСПДн» (приложение 1), где отображается тип зараженного файла, характер содержащейся в файле информации, название вируса, тип вируса и выполненные антивирусные мероприятия.

3. Ответственность

Ответственность за поддержание установленного порядка проведения антивирусного контроля возлагается на администратора безопасности ИСПДн.

Пользователь и администратор безопасности несут ответственность за качество и своевременность выполнения задач и функций, возложенных на них в соответствии с настоящей Инструкцией.

Начальник отдела организационной работы
и делопроизводства П. А. Бочаров

Приложение №4 к
распоряжению администрации
Россошанского муниципального
района Воронежской области
от г. №

**Инструкция**
**при возникновении чрезвычайных ситуаций в ИСПДн администрации Россошанского муниципального района Воронежской области.**

**1. Общие положения**

Настоящая Инструкция определяет возможные аварийные ситуации, связанные с функционированием ИСПДн, меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн после возникновений аварийных ситуаций.

Задачей данной Инструкции является:

- определение мер защиты от прерывания работоспособности;
- определение действий восстановления в случае прерывания.

Действие настоящей Инструкции распространяется на всех пользователей, имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

Пересмотр настоящего документа осуществляется по мере необходимости.

В настоящем документе под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн. Аварийная ситуация становится возможной в результате реализации одной из угроз, приведенных ниже:

- технологические угрозы (пожар в здании, повреждение водой, взрыв, химический выброс в атмосферу);
- внешние угрозы (массовые беспорядки, сбои общественного транспорта, эпидемия, массовое отравление персонала);
- стихийные бедствия (удар молнии, сильный снегопад, сильные морозы, просадка грунта с частичным обрушением здания,

затопление водой в период паводка, наводнение, вызванное проливным дождем, торнадо);

- телекоммуникационные и информационно-технические угрозы (сбой системы кондиционирования, сбой ИТ - систем);
- угроза, связанная с человеческим фактором (ошибка персонала, имеющего доступ к серверной, нарушение конфиденциальности, целостности и доступности конфиденциальной информации);
- угрозы, связанные с внешними поставщиками (отключение электроэнергии, сбой в работе интернет-провайдера, физический разрыв внешних каналов связи).
- Все действия в процессе реагирования на аварийные ситуации, возникающие в ИСПДн, должны документироваться администратором безопасности.

В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование сотрудники (Администратор и пользователи ИСПДн) предпринимают меры по восстановлению работоспособности. Предпринимаемые меры по возможности согласуются с вышестоящим руководством. По необходимости, иерархия может быть нарушена, с целью получения высококвалифицированной консультации в кратчайшие сроки.

**2. Уровни реагирования на инцидент.**

При реагировании на инцидент, важно, чтобы пользователь правильно классифицировал критичность инцидента. Критичность оценивается на основе следующей классификации:

1) **Незначительный инцидент.** Незначительный инцидент определяется как локальное событие с ограниченным разрушением, которое не влияет на общую доступность элементов ИСПДн и средств защиты. Эти инциденты решаются пользователями и администратором безопасности ИСПДн.

Сбой программного обеспечения. Администратор безопасности выясняет причину сбоя программного обеспечения (далее - ПО). Если исправить ошибку своими силами (в том числе после консультации с разработчиками ПО) не удалось, копия акта и сопроводительных материалов (а также файлов, если это необходимо) направляются разработчику ПО.

Отключение электричества. Администратор безопасности проводит анализ на наличие потерь и (или) разрушения данных и ПО, а так же проверяет работоспособность оборудования. В случае необходимости, производится восстановление ПО и данных из последней резервной копии с составлением акта.

Потеря данных. При обнаружении потери данных администратор безопасности проводит мероприятия по поиску и устранению причин потери данных (антивирусная проверка, целостность и работоспособность ПО, целостность и работоспособность оборудования и др.). При необходимости, производится восстановление ПО и данных из резервных копий с составлением акта.

Обнаружена утечка информации (уязвимость в системе защиты). При обнаружении утечки информации ставится в известность администратор безопасности и начальник подразделения.

Проводится служебное расследование. Если утечка информации произошла по техническим причинам, проводится анализ защищённости системы и, если необходимо, принимаются меры по устранению уязвимостей и предотвращению их возникновения.

Физическое повреждение ПЭВМ. Ставится в известность администратор безопасности. Проводится анализ на утечку или повреждение информации. Определяется причина повреждения ПЭВМ и возможные угрозы безопасности информации. В случае возникновения подозрения на целенаправленный вывод оборудования из строя проводится служебное расследование. Проводится проверка ПО на наличие вредоносных программ-закладок, целостность ПО и данных. Проводится анализ электронных журналов. При необходимости проводятся меры по восстановлению ПО и данных из резервных копий с составлением акта.

2) **Авария.** Любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов ИСПДн и средств защиты. Эти инциденты решаются администратором безопасности совместно с руководством. К авариям относятся следующие инциденты:

- отказ элементов ИСПДн и средств защиты из-за повреждения водой, сбоя системы кондиционирования;
- отсутствие администратора безопасности более чем на сутки из-за химического выброса в атмосферу, сбоев общественного транспорта, эпидемии, массового отравления персонала, сильного снегопада, торнадо, сильных морозов.

3) **Катастрофа.** Любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИСПДн и средств защиты, а также к угрозе жизни пользователей ИСПДн, классифицируется как катастрофа. Обычно к катастрофам относят обстоятельства непреодолимой силы (пожар, взрыв), которые могут привести к неработоспособности ИСПДн и средств защиты на сутки и более.

К катастрофам относятся следующие инциденты:

- пожар в здании;
- взрыв;
- просадка грунта с частичным обрушением здания;
- массовые беспорядки.

**3. Меры обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций.**

К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения аварийных ситуаций, такие как:

- системы жизнеобеспечения;
- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.
- Системы жизнеобеспечения ИСПДн включают:
- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания.

Помещения, в которых размещаются элементы ИСПДн и средства защиты должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

Администратор безопасности ознакомляет всех пользователей, находящихся в его зоне ответственности, с данной инструкцией в срок, не превышающий 3-х рабочих дней с момента выхода нового сотрудника на работу.

Должно быть проведено обучение сотрудников Управления, имеющих доступ к ресурсам ИСПДн, порядку действий при возникновении аварийных ситуаций. Должностные лица должны получить базовые знания в следующих областях:

- оказание первой медицинской помощи;
- пожаротушение;
- эвакуация людей;
- защита материальных и информационных ресурсов;
- методы оперативной связи со службами спасения и лицами, ответственными за реагирование сотрудниками на аварийную ситуацию;
- выключение оборудования, электричества, водоснабжения, газоснабжения.

Администратор безопасности ИСПДн должен быть дополнительно обучен методам

частичного и полного восстановления работоспособности элементов ИСПДн.

Навыки и знания должностных лиц по реагированию на аварийные ситуации должны регулярно проверяться. При необходимости должно проводиться дополнительное обучение должностных лиц порядку действий при возникновении аварийной ситуации. Сроки и порядок их обучения согласуется с Администратором безопасности

Начальник отдела организационной работы
и делопроизводства П. А. Бочаров

Приложение №5 к
распоряжению администрации
Россошанского муниципального
района Воронежской области
от г. №

# ИНСТРУКЦИЯ
## о порядке технического обслуживания и ремонта технических средств ИСПДн администрации Россошанского муниципального района Воронежской области

### Общие положения

Настоящая инструкция определяет правила работ по техническому обслуживанию, ремонту, модернизации технических средств, входящих в состав ИСПДн, защищенных от несанкционированного доступа (НСД) и предназначенных для обработки и хранения персональных данных.

Данные работы проводятся только с разрешения руководителя администрации Россошанского муниципального района Воронежской области, после согласования с администратором безопасности ИСПДн.

### Порядок проведения работ по техническому обслуживанию, ремонту, модернизации

В случае, когда необходимо провести работы по техническому обслуживанию (ремонту, модернизации) технических средств, входящих в состав ИСПДн, администратор безопасности ИСПДн представляет служебную записку, в которой:

- указывает название (ПЭВМ, технического средства, системы), техническое обслуживание (ремонт, модернизацию) которой необходимо провести и с какой целью;
- обосновывает необходимость технического обслуживания (модернизации);
- указывает планируемые место и сроки работ, режим их проведения;
- перечисляет меры безопасности, которые будут реализованы при техническом обслуживании (ремонте, модернизации) с целью недопущения доступа к персональным данным посторонних лиц.

В случае если для проведения работ необходимо привлекать лиц, не имеющих постоянного допуска к работе на ПЭВМ или в помещение, составляется список сотрудников, который согласовывается с руководителем администрации Россошанского муниципального района Воронежской области.

Запрещается выносить технические средства и системы (ТСС), входящие в состав ИСПДн, с территории здания без согласования с администратором безопасности ИСПДн и разрешения руководителя администрации Россошанского муниципального района Воронежской области

При вскрытии печатей и пломб на технических средствах (системах), последующее опечатывание производится комиссионно в присутствии администратора безопасности информации, о чём составляется акт.

В акте указывается:

- номер (название) помещения, в котором проводились работы.
- дата и время начала и окончания работ,
- лица, присутствовавшие при вскрытии и обслуживании (ремонте, модернизации),
- наличие, целостность и места размещения печатей (пломб, специальных защитных знаков) до вскрытия ПЭВМ (технического средства, системы),
- установленные неисправности,
- виды и результаты проведенных работ,
- замененные или отремонтированные узлы (детали), наличие на этих узлах специальных защитных знаков,
- какими печатями (пломбами и т.д.) и в каких местах ПЭВМ (устройство) опечатано по окончании работ,
- необходимость проведения дополнительной специальной проверки и специальных исследований (сертификации) ПЭВМ (технического средства, системы) или её отдельных узлов,
-иная необходимая для дальнейшей работы и обеспечения безопасности информация.

Если для ремонта (модернизации) ИСПДн (другого технического средства, системы, узла ПЭВМ в составе ИСПДн) необходимо направить в специализированную организацию, то комиссией составляется заключение.

Перед отправкой ПЭВМ (другого технического средства, системы, узла ПЭВМ) администратор безопасности информации обязан гарантированно удалить персональные данные с жесткого диска и иных устройств памяти ПЭВМ (другого технического средства, системы) сертифицированными средствами, о чем он составляет акт. По запросу из специализированной организации копия акта передаётся и ей.

В случае если не имеется возможности гарантировано удалить персональные данные с жесткого диска и иных устройств памяти ПЭВМ (другого технического средства, системы) сертифицированными средствами, эти устройства опечатываются и хранятся в ИСПДн с соблюдением требований, предъявляемым к хранению персональных данных.

Ремонт и замена жесткого диска производится в присутствии администратора безопасности информации. При диагностике и ремонте жесткого диска должны быть реализованы меры безопасности, исключающие несанкционированный доступ к хранящимся на нём данным.

Начальник отдела организационной работы
и делопроизводства П. А. Бочаров

Приложение №6 к
распоряжению администрации
Россошанского муниципального
района Воронежской области
от г. №

# ИНСТРУКЦИЯ

## по маркировке съемных носителей информации, содержащих персональные данные

Носители информации (съемные магнитные диски, CD и DVD диски, дискеты и USB флеш-накопители), предназначенные для хранения на них конфиденциальной информации, берутся на учет до записи на них персональных данных.

Для записи информации, содержащей персональные данные, должны использоваться специально выделенные диски, дискеты и USB флеш-накопители.

При постановке на учет съемного диска его маркировка производится на металлической пластине, прикрывающей нерабочую поверхность нижнего диска, посредством нанесения записей механическим путем или красящим веществом, имеющим хорошую механическую стойкость. На дискеты и USB флеш-накопители с двух сторон наносится красящее стойкое вещество. На CD и DVD дисках наносится на нерабочую поверхность красящее стойкое вещество.

К работе с персональными данными должны допускаться только те лица, которые указаны в разрешении на автоматизированную обработку информации, и только в те интервалы рабочего времени, которые отведены для решения указанной задачи в графике рабочего времени.

Инвентарный номер персональному компьютеру, съемному диску, CD и DVD дискам, USB флеш-накопители или дискете присваивается один раз при их первичном учете и может быть изменен только при проведении инвентаризации и заведении нового учета, о чем делается отметка в соответствующих учетных формах.

Персональные компьютеры, используемые для хранения информации на длительное время, подлежат инвентарному учету с отражением содержащейся информации. В этих случаях указанные компьютеры на период, пока они не используются в работе, опечатываются администратором безопасности. Включение этих компьютеров в работу в соответствии с заказом (заданием, запросом) производится исполнителем (пользователем) в присутствии администратора безопасности.

Жесткие магнитные диски при обработке на них персональных данных используются, как правило, в качестве рабочих магнитных носителей информации,

которая должна обязательно стираться по окончании выполнения каждого конкретного расчета.

Начальник отдела организационной работы
и делопроизводства П.А.Бочаров

Приложение №7 к
распоряжению администрации
Россошанского муниципального
района Воронежской области
от г. №

# ИНСТРУКЦИЯ
## по порядку учета и хранению съемных носителей персональных данных в администрации Россошанского муниципального района

### Общие положения

1.1. Настоящая Инструкция разработана в соответствии с Федеральным законом № 149-ФЗ от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации», ГОСТ Р ИСО/МЭК 17799-2005 «Практические правила управления информационной безопасностью» и другими нормативными правовыми актами, и устанавливает порядок использования носителей информации.

1.2. Действие настоящей Инструкции распространяется на сотрудников администрации Россошанского муниципального района Воронежской области, подрядчиков и третью сторону.

### 2. Основные термины, сокращения и определения

- **Администратор ИС** - технический специалист, обеспечивает ввод в эксплуатацию, поддержку и последующий вывод из эксплуатации ПО и оборудования вычислительной техники.
- **АРМ** - автоматизированное рабочее место пользователя (ПК с прикладным ПО) для выполнения определенной производственной задачи.
- **ИБ** - информационная безопасность - комплекс организационно-технических мероприятий, обеспечивающих конфиденциальность, целостность и доступность информации.

ИС- информационная система - система, обеспечивающая хранение, обработку, преобразование и передачу информации с использованием компьютерной и другой техники.

- **Носитель информации** - любой материальный объект, используемый для хранения и передачи электронной информации.
- **Паспорт ПК** - документ, содержащий полный перечень оборудования и

программного обеспечения АРМ.

- **ПК -** персональный компьютер.
- **ПО -** Программное обеспечение вычислительной техники.
- **ПО вредоносное** - ПО или изменения в ПО, приводящие к нарушению конфиденциальности, целостности и доступности критичной информации.
- **ПО коммерческое -** ПО сторонних производителей (правообладателей). Предоставляется в пользование на возмездной (платной) основе.
- **Пользователь -** работник Организации, использующий мобильные устройства и носители информации для выполнения своих служебных обязанностей.

## 3. Порядок использования носителей информации

Под использованием носителей информации в ИС Государственной инспекции труда в Воронежской области понимается их подключение к инфраструктуре ИС с целью обработки, приема/передачи информации между ИС и носителями информации, администрации Россошанского муниципального района Воронежской области

В ИС допускается использование только учтенных носителей информации, которые являются собственностью администрации Россошанского муниципального района Воронежской области и подвергаются регулярной ревизии и контролю.

К предоставленным носителям персональных данных предъявляются те же требования ИБ, что и для стационарных АРМ (целесообразность дополнительных мер обеспечения ИБ определяется ответственным за защиту персональных данных).

Носители персональных данных предоставляются сотрудникам администрации Россошанского муниципального района Воронежской области по инициативе Руководителей структурных подразделений в случаях:

- необходимости выполнения вновь принятым работником своих должностных обязанностей;
- возникновения у сотрудника администрации Россошанского муниципального района Воронежской области производственной необходимости.

Порядок учета, хранения и обращения со съемными носителями персональных данных, твердыми копиями и их утилизация:

- Все находящиеся на хранении и в обращении съемные носители с персональными данными подлежат учёту. Каждый съемный носитель с записанными на нем персональными данными должен иметь этикетку, на которой указывается его уникальный учетный номер.
- Учет и выдачу съемных носителей персональных данных осуществляют сотрудники структурных подразделений, на которых возложены функции хранения носителей персональных данных. Факт выдачи съемного носителя фиксируется в «журнале учета съемных носителей с персональными

данными».

- Сотрудники администрации Россошанского муниципального района Воронежской области получают учтенный съемный носитель от уполномоченного сотрудника для выполнения работ на конкретный срок. При получении делаются соответствующие записи в журнале учета. По окончании работ пользователь сдает съемный носитель для хранения уполномоченному сотруднику, о чем делается соответствующая запись в журнале учета.
- При использовании сотрудниками носителей с персональными данными

**необходимо:**

- Соблюдать требования настоящей Инструкции.
- Использовать носители информации исключительно для выполнения своих служебных обязанностей.
- Ставить в известность ответственного за защиту персональных данных о любых фактах нарушения требований настоящей Инструкции.
- Бережно относится к носителям персональных данных.
- Обеспечивать физическую безопасность носителей информации всеми разумными способами.
- Извещать ответственного за защиту персональных данных о фактах утраты (кражи) носителей персональных данных.

При использовании носителей персональных данных запрещено:

- Использовать носители персональных данных в личных целях.
- Передавать носители персональных данных лицам, не имеющим доступ к обработке персональных данных в данной информационной системе персональных данных.
- Хранить съемные носители с персональными данными вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;
- Выносить съемные носители с персональными данными из служебных помещений для работы с ними на дому и т. д.

Любое взаимодействие (обработка, прием/передача информации) инициированное сотрудником администрации Россошанского муниципального района Воронежской области между ИС и неучтенными (личными) носителями информации, рассматривается как **несанкционированное** (за исключением случаев оговоренных с ответственным за защиту персональных данных заранее). Ответственный за защиту персональных данных оставляет за собой право блокировать или ограничивать использование носителей информации.

Информация об использовании сотрудником администрации Россошанского муниципального района Воронежской области носителей информации в ИС протоколируется и, при необходимости, может быть предоставлена Руководителю администрации Россошанского

муниципального района Воронежской области.

В случае выявления фактов несанкционированного и/или нецелевого использовании носителей персональных данных инициализируется служебная проверка, проводимая комиссией, состав которой определяется Руководителем администрации Россошанского муниципального района Воронежской области.

По факту выясненных обстоятельств составляется акт расследования инцидента и передается Руководителю администрации Россошанского муниципального района Воронежской области для принятия мер согласно локальным актам администрации Россошанского муниципального района Воронежской области и действующему законодательству.

Информация, хранящаяся на носителях персональных данных, подлежит обязательной проверке на отсутствие вредоносного ПО.

При отправке или передаче персональных данных адресатам на съемные носители записываются только предназначенные адресатам данные. Отправка персональных данных адресатам на съемных носителях осуществляется в порядке, установленном для документов для служебного пользования.

Вынос съемных носителей персональных данных для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя структурного подразделения.

В случае утраты или уничтожения съемных носителей персональных данных либо разглашении содержащихся в них сведений немедленно ставится в известность начальник соответствующего структурного подразделения. На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы учета съемных носителей персональных данных.

Съемные носители персональных данных, пришедшие в негодность, или отслужившш установленный срок, подлежат уничтожению. Уничтожение съемных носителей с персональными данными осуществляется «уполномоченной комиссией». По результатам уничтожения носителей составляется акт по прилагаемой форме

В случае увольнения или перевода работника в другое структурное подразделение, предоставленные носители персональных данных изымаются.

## 4. Ответственность

Работники, нарушившие требования настоящей Инструкции, несут ответственность в соответствии с действующим законодательством и локальными актами администрации Россошанского муниципального района Воронежской области.

Начальник отдела организационной работы
и делопроизводства П. А. Бочаров

Приложение №8 к
распоряжению администрации
Россошанского муниципального
района Воронежской области
от г. №

**Инструкция**
**пользователям локальной вычислительной сети по порядку пользования в сети международного информационного обмена**
(ИНТЕРНЕТ)

**1**. Общие положения

Инструкция разработана на основании федерального закона «Об информации информатизации и защите информации» от 27 июля 2006 года №149-ФЗ, «Доктрины информационной безопасности Российской Федерации», утвержденной Президентом Российской Федерации 9 сентября 2000 года№ Пр-1895, «Специальных требований и рекомендаций по защите конфиденциальной информации» (СТР-К) утвержденных приказом Гостехкомиссии России 30 августа 2002 года № 282, указа Президента «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» от 17 марта 2008 года № 35 1 и других нормативно правовых документов в области защиты информации.

Настоящая Инструкция определяет основные требования по организации работы в области защиты информации, общий порядок обращения с документами и другими материальными носителями информации при подключении и использовании международных информационных сетей (МИС) общего пользования, в том числе сети Интернет.

Интернет - всемирная компьютерная сеть, которая использует для взаимодействия стек протоколов TCP/IP (протокол управления передачи сообщений / Интернет протокол). Работа в Интернет осуществляется в режиме реального времени (on-line). Существует ряд протоколов и служб, связанных с TCP/IP и Интернетом. Наиболее распространенными из них являются:

SMTP - протокол приема - передачи электронной почты.

TELNET - протокол для подключения к удаленным системам, присоединенным к МИС общего пользования в режиме удаленного терминала.

FTP - протокол предназначенный для передачи файлов с одного компьютера на другой в вычислительной сети.

DNS - служба сетевых имен используемых для протоколов TELNET, FTP и т.д.

WWW - служба (всемирная паутина), использующая гипертекстовый формат HTML (язык разметки гипертекста), предназначенная для передачи тестовой, графической, аудио и видео информации, а также ссылок на другие

документы (гипертекстовые ссылки - выделенные области документа, позволяющие переходить к другому документу, содержащему связанную информацию).

Помимо перечисленных, существует ряд служб и протоколов для удаленной печати, предоставления удаленного доступа к файлам и дискам, работы с распределенными базами данных и т.д.

Основная цель обеспечения информационной безопасности - предотвращение несанкционированного уничтожения, искажения. копирования, блокирования информации в компьютерных и телекоммуникационных системах

3. Источники угроз информационной безопасности

Подключение средств вычислительной техники к МИС общего пользования представляет реальную угрозу создания разветвленных систем регулярного несанкционированного контроля информационных процессов и ресурсов, несанкционированного доступа (НСД) в автоматизированные системы (АС).

Информационные вычислительные сети общего пользования являются открытыми системами передачи информации, при работе в которых могут возникнуть следующие основные угрозы безопасности информации:

- проникновение в систему незаконных пользователей, которое происходит вследствие ошибок в конфигурации программных средств (ошибок администрирования), дефектов в средствах обеспечения защиты информации от НСД операционных систем;
- перенос вАС разрушающего программного обеспечения (внедрение программных закладок, вирусов);
- выбор и использование законным пользователем системы неудачных паролей;
- несанкционированная передача служебной информации ограниченного распространения пользователями в МИС общего пользования и т.д.

При непосредственном подключении локальной вычислительной сети к МИС общего пользования любой пользователь МИС имеет возможность:

- получить информацию об адресной структуре сети;
- установить типы и версии используемого сетевого программного обеспечения (сетевое оборудование, операционные системы, прикладные и служебные сервисы);
- получить информацию о пользователях сети;
- попытаться подключиться к информационным ресурсам сети;
- вызвать отказ в обслуживании легальных пользователей.

Кроме явных, то есть непосредственно направленных на сеть организации, внешних угроз информационной безопасности, существуют угрозы, связанные с неумышленным распространением зловредного программного кода самими сотрудниками организации. К зловредному программному коду относят вирусы, троянские программы, «опасные» компоненты прикладных протоколов.

По этим причинам самым опасным с точки зрения безопасности информации является несанкционированное использование модемов, подключенных к рабочим станциям пользователя. Причем подключение не обязательно может использоваться для доступа в Интернет (возможны соединения к серверам других организаций, и к отдельным компьютерам, например домашним).

## 4. Технические средства защиты информации

К техническим средствам защиты информации при работе с информационными сетями общего пользования, в том числе Интернет относятся: системы разграничения прав доступа, межсетевые экраны, системы построения защищенных виртуальных сетей (VirtualPrivateNetwork - VPN), системы обнаружения атак, системы анализа защищенности, системы антивирусной защиты и т.д.

### 4.1. Системы разграничения доступа

Система разграничения доступа запрещает посторонним лицам доступ к ресурсам автоматизированной системы и позволяет разграничить права пользователей при работе на компьютере, при этом контролируются права локальных, удаленных и терминальных пользователей.

### 4.2 Межсетевые экраны (МСЭ)

Межсетевой экран представляет собой локальное (однокомпонентное) или функционально-распределенное средство, реализующее контроль за информацией, поступающей в автоматизированную систему (АС) и/или выходящей из АС, и
обеспечивает защиту АС посредством фильтрации информации, то есть ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АС.

Межсетевые экраны позволяют осуществить: контроль доступа на межсетевом уровне, протоколирование информационных потоков, сокрытие топологии защищаемой сети, реагирование на несанкционированные действия.

Средствами МСЭ могут быть выявлены следующие виды атак: сканирование сетевых портов, атаки на отказ в обслуживании, изучение топологии внутренней сети, использование слабостей протоколов прикладного уровня, распространение вирусов и спама.

К дополнительным службам МСЭ относятся: средства резервного копирования и восстановления, средства обеспечения высокой доступности, сетевая служба имен.

Основные показатели защищенности МСЭ: управление доступом, идентификация и аутентификация, регистрация событий и оповещение, контроль целостности, восстановление работоспособности.

Межсетевые экраны делятся на пять классов в соответствии с руководящим документом «Средства вычислительной техники. Межсетевые экраны. Защите от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» - М.: Гостехкомиссиия России, 1997.

### 4.3. Системы построения защищенных виртуальных сетей

Системы построения защищенных виртуальных сетей позволяют организовать прозрачное для пользователей соединение локальных вычислительных сетей с помощью шифрования.

### 4.4. Системы обнаружения атак

К системам обнаружения атак можно отнести: системы обнаружения атак на уровне сети, системы обнаружения атак на уровне хоста. Системы обнаружения атак используют:

- системы обнаружения аномального поведения пользователя (большое число соединений за короткий промежуток времени, высокая загрузка центрального процессора, использование периферийных устройств, которые обычно пользователем не используются и т.д.);

- системы обнаружения злоупотребления (обнаружение уже известной атаки по шаблону или «сигнатуре»).

**4.5. Системы анализа защищенности**

Средства анализа защищенности предназначены для поиска в вычислительной технике и ее компонентах различных уязвимостей, которые могут быть использованы злоумышленниками для реализации атак;

**5. Организация работы с международными информационными сетями**

**5.1 Общие требования**

АС МИС общего пользования должны быть автономны, не иметь логических и физических каналов (линий) связи с объектами вычислительной техники, на которых ведется обработка информации ограниченного распространения, а также для которых установлены особые правила доступа к информационным ресурсам.

На технических средствах абонентского пункта должно находиться только программное обеспечение, необходимое для его функционирования системы. Владельцам открытых и общедоступных государственных информационных ресурсов необходимо осуществлять их включение в состав объектов международного информационного обмена только при использовании сертифицированных средств защиты информации, обеспечивающих ее целостность и доступность, в том числе криптографических для подтверждения достоверности информации.

Владельцам и пользователям указанных ресурсов необходимо осуществлять размещение технических средств, подключаемых к открытым информационным системам, сетям и сетям связи, используемым при международном информационном обмене, включая сеть "Интернет", вне помещений, предназначенных для ведения закрытых переговоров, в ходе которых обсуждаются вопросы, содержащие сведения, составляющие государственную тайну.

**5.2 Резервное копирование**

При размещении информации в сетях общего пользования, необходимо иметь копию такой информации, для ее восстановления в случае разрушения, изменения или блокирования по причине несанкционированного доступа либо неисправности оборудования. Также необходимо иметь резервную копию системы для восстановления информации в случае ее разрушения.

**5.3 Аппаратно - программная защита**

Для фильтрации входящих и исходящих сообщений, а также обнаружения атак, рекомендуется использовать межсетевые экраны.

Для работы с открытыми информационными ресурсами в режиме реального времени (on-line) как правило, используют технологию VPN. Для передачи информации конфиденциального характера по открытым каналам связи необходимо использовать сертифицированные средства криптографической защиты.

Программное обеспечение, устанавливаемое наАС МИС общего пользования, должно быть сертифицировано и иметь все последние обновления.

### 5.4 Организационные меры

Приказом по предприятию, подразделению, учреждению, организации назначаются должностные лица, ответственные за эксплуатацию АС МИС, допущенные к работам в МИС общего пользования (в том числе администратор АС МИС, должностные лица, имеющие право подписи документов для отправки по МИС общего пользования, должностные лица, ответственные за прием/отправку электронных сообщений и т.д.).

Пользователь АС МИС обязан:

строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами АС;

знать и строго выполнять правила работы со средствами защиты информации (средствами разграничения доступа), используемых на персональных компьютерах;

хранить в тайне свой аутентификатор (пароль доступа в автоматизированную систему), а также информацию о системе защиты установленной на АС;

Администратор АС МИС обязан:

перед работой пользователей в МИС обеспечить обновление антивирусных баз;

после окончания работы проверить технические средства на наличие/отсутствие вредоносного кода и целостность АС (запрещается использование АС при отключенных или неисправных средствах защиты информации).

Администратор обеспечивает выдачу аутентификаторов (имя пользователя/электронный адрес) и идентификаторов (пароль) пользователя, а также регулярную смену идентификаторов. В случае прекращения полномочий пользователя по работе с МИС (перевод на другую должность, не предусматривающую работу с МИС или увольнение), администратор удаляет учетную запись пользователя из АС МИС.

Администратор обеспечивает ведение журнала приема-передачи информации средствами МИС на бумажных или электронных носителях, который должен содержать следующие обязательные поля: дата работы в сети, ФИО пользователя, время (продолжительность) работы в сети, подпись (в случае ведения журнала на бумажном носителе) или аутентификатор (при ведении электронного журнала). Данная информация используется для сверки времени работы в сети со счетом предъявленным организацией предоставляющей услуги связи с МИС, и выявления злоупотреблений работы в сети, а также для обнаружения факта компрометации пароля пользователя сети.

Пользователи, работающие на АС МИС общего пользования, обязаны: знать порядок входа в МИС общего пользования и регистрации в сети; знать данную инструкцию;

знать правила работы со средствами защиты информации установленными на АС; передачу документированной информации, производить только по письменному разрешению должностного лица, имеющего право подписи документов для отправки по МИС общего пользования, и после учета в несекретном делопроизводстве;

материальные носители информации с записанной на них входящей документированной информации полученной в процессе работы с информационными ресурсами МИС общего пользования передавать для учета в несекретное делопроизводство;

при пользовании электронной почтой запрещается передача сведений, содержащих конфиденциальную информацию без применения специальных

мер защиты (сертифицированных средств криптографической защиты информации);

запрещается копирование или распространение информации с нарушением авторских прав или условий программных лицензий;

запрещается распространение противозаконных материалов;

С целью предотвращения заполнения почты ненужной почтовой (рекламной и др.) информацией - спамом не рекомендуется размещать адрес своего электронного ящика на досках (доски объявлений или BBS) объявлений. Для фильтрации данных сообщений необходимо использование белого и черного списка для настройки почтовой службы, а также сообщить о наличии спама администратору сети, провайдеру.

Ежемесячно необходимо проверять фактически отработанное время работы в сети Интернет со счетом, представленным провайдером.

### 5.5 Антивирусная защита

АС МИС общего пользователя оснащаются, в обязательном порядке, антивирусным программным обеспечением, обновление антивирусной базы которого производится непосредственно перед каждым началом работы. Антивирусное программное обеспечение настраивается на проверку всех файлов без исключения. При использовании съемных накопителей информации для передачи информации, каждый из них должен быть проверен на отсутствие вредоносного программного обеспечения. АС МИС общего пользования регулярно, не реже одного раза в неделю, проверяются на отсутствие вредоносного программного кода.

При отправке электронных сообщений необходимо заполнять поле тема. Не рекомендуется открывать для чтения почтовые сообщения, адресат которых неизвестен или почтовое отправление носит подозрительный характер (реклама или запрос информации неизвестной фирмы, спам, и т.д.)

Если обнаружено, что почтовое отправление, пришедшее от адресата, заражено вредоносным кодом, администратору необходимо:

срочно принять все меры по предотвращению дальнейшего распространения заражения путем прекращения приема передачи сообщений данной АС МИС;

провести сканирование и лечение системы антивирусными средствами (при необходимости обновить базы данных антивирусного программного обеспечения);

отметить данный факт в журнале учета с указанием названия вредоносного программного обеспечения и адресата, от которого оно получено;

поставить в известность руководителя подразделения Правительства области, а также абонента с которыми осуществлялась связь в период заражения для проверки АС антивирусными средствами.

сообщить адресату о наличии у него заражения, для последующего принятия адресатом срочных мер.

Запрещается хранение вредоносного кода, на каких либо носителях информации.

При обнаружении вредоносного кода необходимо произвести его удаление антивирусными средствами. Удаление зараженных файлов средствами операционной системы может привести к безвозвратному разрушению информации.

**6. Учет АС, подключенных к международным сетям общего пользования и контроль за обеспечением защиты от несанкционированного доступа**

Ведение учета АС, подключенных к МИС общего пользования в Правительстве области, организуется администратором АС МИС.

Сведения о наличии и особенностях функционирования АС МИС общего пользования представляются в отдел защиты информации Правительства области в установленном порядке.

Отдел по защите информации имеет право вносить предложения по порядку и ограничениям использования АС МИС общего пользования, а также выдавать рекомендации и предъявлять дополнительные требования по защите информации от несанкционированного доступа.

Начальник отдела организационной работы
и делопроизводства П. А. Бочаров

Приложение №9 к
распоряжению администрации
Россошанского муниципального
района Воронежской области
от г. №

**ИНСТРУКЦИЯ**
**по организации парольной защиты в ИСПДн администрации Россошанского муниципального района Воронежской области**

## 1. Общие положения

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в ИСПДн администрации Россошанского муниципального района Воронежской области а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

## 2. Порядок парольной защиты

1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей в ИСПДн возлагается на администратора безопасности. Контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями возлагается на администратора безопасности.

2. Личные пароли должны генерироваться и распределяться централизованно с учетом следующих требований:

- длина пароля должна быть не менее 6 символов;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 3 позициях;
- личный пароль пользователь не имеет права сообщать никому.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

3. Формирование личных паролей пользователей осуществляется централизованно. Ответственность за правильность их формирования и распределения возлагается на администратора безопасности. Для генерации «стойких» значений паролей могут применяться специальные программные средства. Система централизованной генерации и распределения паролей должна исключать возможность ознакомления (самих уполномоченных сотрудников, а также руководителей подразделений) с паролями других пользователей.

4. Списки паролей пользователей хранятся в сейфе.

5. Полная плановая смена паролей пользователей должна проводиться регулярно.

6. Внеплановая смена личного пароля или удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение, переход на другую работу и т.п.) должна производиться администратором безопасности немедленно после окончания последнего сеанса работы данного пользователя с системой.

7. В случае компрометации личного пароля пользователя ИСПДн должны быть немедленно предприняты меры в соответствии с п.6 настоящей Инструкции.

8. Хранение сотрудником значений своих паролей на материальном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у руководителя подразделения в опечатанном конверте или пенале (возможно вместе с персональным носителем информации и идентификатором).

9. Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены и использования в подразделениях возлагается на администратора безопасности.

## 3. Ответственность

Пользователь и администратор безопасности несут ответственность за качество и своевременность выполнения задач и функций, возложенных на них в соответствии с настоящей Инструкцией.

Начальник отдела организационной работы
и делопроизводства П. А. Бочаров

Приложение №10к
распоряжению администрации
Россошанского муниципального
района Воронежской области
от г. №

**ИНСТРУКЦИЯ**
**администратору безопасности ИСПДн Администрации Россошанского муниципального района Воронежской области**
**Общие положения.**

Настоящая инструкция определяет основные функции и порядок работы администратора безопасности в технологическом процессе обработки конфиденциальной информации на объекте информатизации ИСПДн Администрации Россошанского муниципального района Воронежской области с применением комплекса средств защиты информации (СЗИ) от несанкционированного доступа (НСД) Dallas Lock и VIP NET CUSTOM.

В процессе выполнения своих служебных обязанностей администратор безопасности должен выполнять требования нормативных документов по защите информации и требования эксплуатационной документации на комплекс Dallas Lock и YIP NET CUSTOM.

1.**Функции администратора безопасности.**

1.1. Администратор безопасности обязан выполнять начальную установку и настройку комплекса СЗИ НСД на ПЭВМ объекта информатизации.
1.2. Администратор обязан вести учет электронных идентификаторов комплексов СЗИ НСД, выполнять действия по их регистрации на ПЭВМ, организовывать их выдачу пользователям и периодически контролировать их наличие.
1.3. Администратор безопасности обязан проводить работы по генерации и регулярной смене паролей пользователей.
1.4. Администратор безопасности обязан выполнять действия по настройке комплексов СЗИ НСД на ПЭВМ объекта информатизации в соответствии с утвержденными правилами разграничения доступа (матрицей доступа).
1.5. Администратор безопасности обязан осуществлять оперативный контроль над функционированием комплекса СЗИ НСД на ПЭВМ объекта информатизации, проводить его периодическое тестирование и осуществлять контроль целостности резервных копий программного обеспечения комплекса на носителях.
1.6. Администратор безопасности обязан проводить проверки целостности программного обеспечения.
1.7. Администратор безопасности обязан осуществлять постоянный контроль над соблюдением операторами (пользователями) технологии обработки

конфиденциальной информации, анализировать содержимое регистрационных журналов, формируемых комплексами СЗИ НСД и принимать конкретные меры по выявленным нарушениям.
1.8. Администратор безопасности обязан организовывать и контролировать проведение работ по ремонту, наладке и сервисному обслуживанию ПЭВМ и вспомогательных технических средств объекта информатизации.

Администратор безопасности обязан контролировать сохранность и целостность эта тонных копий программного обеспечения.
1.9. Администратор безопасности обязан оказывать методическую и консультационную помощь операторам (пользователям) объекта информатизации в процессе эксплуатации комплексов СЗИ НСД.

## 2.УСТАНОВКА И НАСТРОЙКА КОМПЛЕКСА СЗИ НСД

2.1. Установка (повторная установка) комплексов СЗИ НСД выполняется в следующих ситуациях:
- на этапе ввода в действие объекта информатизации;
- в случае выхода из строя накопителей с конфиденциальной информацией;
- в случае возникновения сбойных и аварийных ситуаций, повлекших нарушения в работе программного обеспечения (ПО) ПЭВМ;
- в случае ввода новых ПЭВМ в состав объекта информатизации.

2.2. Установка комплекса СЗИ НСД на ПЭВМ объекта информатизации должна выполняться администратором безопасности в строгом соответствии с инструкциями, приведенными в эксплуатационной документации.
2.3. Установка ПО комплекса СЗИ НСД должна производиться с эталонных носителей (CD- дисков). Перед установкой комплекса ПО ПЭВМ должно быть проверено на отсутствие вирусного заражения.
2.4. Регистрация электронных идентификаторов пользователей и установка правил разграничения доступа производится в соответствии с утвержденными правилами разграничения доступа (матрицей доступа). Регистрация дополнительных (не указанных) в матрице доступа пользователей запрещена

## 3.СОПРОВОЖДЕНИЕ СЗИ НСД В ПРОЦЕССЕ ЭКСПЛУАТАЦИИ

### 3.1 **Ведение служебной информации *СЗИ НСД***

### 3.1.1 **Регистрация пользователей**

3.1.1.1. Действия по регистрации пользователей выполняются администратором безопасности на основании оформленных установленным порядком приказов и распоряжений о допуске пользователей к обработке конфиденциальной информации.
3.1.1.2. В соответствии с установленными уровнями полномочий операторов (пользователей) и эксплуатационной документацией на комплекс СЗИ НСД администратор безопасности разрабатывает правила разграничения доступа (ПРД) и оформляет матрицу доступа.
3.1.1.3. На основании утвержденной матрицы доступа администратор безопасности, в соответствии с эксплуатационной документацией выполняет действия по настройке системы защиты ПЭВМ от НСД.

3.1.1.4. В процессе регистрации пользователей и настройки системы защиты администратор безопасности должен соблюдать следующие правила:

- все информационные ресурсы, к которым разрешен доступ пользователя (логические диски, каталоги и файлы) должны быть явно указаны;
- каталогам, в которых планируется размещать конфиденциальную информацию должны быть заранее присвоены соответствующие метки конфиденциальности;
- все запускаемые программы и подгружаемые модули должны быть явно указаны и включены в список контроля при запуске;
- должна быть обеспечена регистрация в системном журнале операций чтения, записи и удаления;
- журнал регистрации должен вестись для всех пользователей;
- должен быть активизирован режим ограничения времени действия пароля по количеству попыток неправильного ввода;
- должен быть активизирован режим полного удаления файлов;
- должен быть активизирован режим очистки освобождаемой памяти;

3.1.1.5. доступ к портам ввода-вывода должен быть максимально ограничен.Регистрация электронных идентификаторов пользователей, установка правил разграничения доступа выполняются средствами СЗИ НСД.
3.1.1.6. Контроль целостности файлов системы защиты обеспечивается средствами СЗИ НСД.
3.1.1.7. Контроль файловой системы, в том числе обнаружение изменения и создания новых файлов обеспечивается средствами программы контроля целостности файловой системы СЗИ НСД.
3.1.1.8. По окончании работ по регистрации пользователей администратор безопасности выполняет проверки функционирования общесистемной программной среды каждого зарегистрированного пользователя, тестирует работоспособность комплекса СЗИ НСД. и корректность реализации ПРД.
3.1.1.9. После выдачи идентификаторов каждому пользователю администратор (возможно совместно с пользователем) осуществляет генерацию пароля и контролирует установку пароля пользователем.

### **3.1.2** ***Генерация и смена паролей***

3.1.2.1. Действия по генерации и смене паролей пользователей должны организовываться администратором безопасности.
3.1.2.2. Для организации работ по смене паролей администратор безопасности устанавливает ограничения на время действия пароля.
3.1.2.3. Процедура генерации паролей должна исключать задание в качестве паролей комбинаций критичных с точки зрения их подбора.
3.1.2.4. Смена паролей выполняется, в соответствии с эксплуатационной документацией на комплекс СЗИ НСД.
3.1.2.5. Установленные (новые) пароли администратор безопасности должен лично сообщать каждому конкретному пользователю. Администратор безопасности несет ответственность за разглашение личных паролей пользователей.

#### ***3.1.3Сопровождение ПРД***

3.1.3.1. Администратор безопасности обеспечивает реализацию разрешительной системы доступа в виде наборов правил разграничения доступа к техническим, программным средствам и информационным

ресурсам формируемых для каждого регистрируемого пользователя.
3.1.3.2. Распределение и изменение прав доступа пользователей к конкретным программам и информационным ресурсам должно осуществляться на основании Заявок.
3.1.3.3. Правила разграничения доступа разрабатываются в соответствии с требованиями разрешительной системы доступа на основании заявок на доступ пользователей и документально оформляются в виде матрицы доступа или в виде дополнений и изменений матрицы доступа и физически реализуются настройками подсистемы разграничения доступа к объектам файловой системы.
3.1.3.4. Заявки на доступ пользователей к техническим средствам объекта должны содержать перечень (список) программ и информационных ресурсов, доступ к которым должен быть предоставлен каждому конкретному пользователю с указанием дисков и каталогов, на которых размещены данные ресурсы.

### *3.2 Оперативный контроль над функционированием СЗИ НСД*

3.2.1. Администратор безопасности несет ответственность за нормальное функционирование комплекса СЗИ НСД на ПЭВМ объекта информатизации.
3.2.2. Администратор безопасности должен осуществлять периодическое тестирование работоспособности комплекса СЗИ НСД и корректности реализации ПРД.
3.2.4. В случае, когда средства комплекса СЗИ НСД отказывают в доступе легальным пользователям, администратор безопасности должен анализировать причины отказа в доступе и предпринимать оперативные действия по выявлению возможных нарушений.Администратор безопасности должен предпринимать оперативные действия в случае возникновения внештатных ситуаций при работе ПЭВМ, анализировать причины их возникновения и предпринимать необходимые меры по восстановлению работоспособности комплекса СЗИ НСД и программного обеспечения.
3.2.5. Администратор безопасности должен постоянно контролировать уровень защищенности информации от НСД и, в случае выявления возможных каналов утечки информации за счет НСД, предпринимать оперативные меры по их устранению за счет изменения параметров настройки подсистемы разграничения доступа комплекса СЗИ НСД.

### *3.3 Контроль соответствия программной среды эталону*

3.3.1. Контроль соответствия общесистемной программной среды эталону осуществляется администратором безопасности с использованием средств комплекса. Для этого администратор средствами администрирования формирует для каждого зарегистрированного пользователя списки файлов, входящих в состав общесистемного программного обеспечения, целостность которых контролируется и включает режим проверки целостности «до запуска» ОС.
3.3.2. Все исполняемые модули (файлы, содержащие исполняемый или интерпретируемый программный код), входящие в состав общесистемной программной среды доступ к которым разрешен конкретному пользователю, должны быть включены в список контроля целостности.
3.3.3. В случае выявления фактов нарушения целостности компонентов, входящих в состав общесистемного программного обеспечения, администратором безопасности должны предприниматься действия по

анализу причин таких нарушений и действия по восстановлению данных компонент с эталонных копий.

3.3.4. Администратор безопасности должен обеспечивать контроль над сохранностью эталонных копий ПО и периодически проверять состояние учтенных носителей, на которых оно расположено.

### 3.4 *Приемка и ввод в эксплуатацию программных средств*

3.4.1. Администратор безопасности организует и контролирует выполнение работ по установке новых программных средств, включаемых в состав ИСПДн.

3.4.2. Перед установкой дистрибутивные носители с новыми программными средствами, вводимыми в состав объекта информатизации, должны быть соответствующим образом проверены.

3.4.3. Установка новых программных средств допускается только с проверенных носителей.

3.4.4. Перед установкой новых программных средств ПЭВМ должна быть физически отключена от ИСПДн. Если физическое отключение ПЭВМ не возможно (в силу специфики устанавливаемого ПО), выполнение работ по установке новых программных средств допускается только после полного прекращения обработки конфиденциальной информации в ИСПДн.

3.4.5. После выполнения работ по установке новых программных средств администратор безопасности проверяет их работоспособность и средствами администрирования комплекса СЗИ НСД выполняет необходимые действия по их настройке. По результатам выполненных работ оформляется акт приемки нового программного обеспечения и утверждаются дополнения и изменения матрицы доступа.

3.4.6. Допуск пользователей к работе на ПЭВМ, на которых проводились работы по установке нового программного обеспечения, разрешается только после утверждения акта приемки и матрицы доступа.

### *3.5 Контроль за ходом технологического процесса обработки информации*

3.5.1. Контроль хода технологического процесса обработки информации администратор безопасности осуществляет путем регистрации и анализа действий операторов (пользователей) по системному журналу.

3.5.2. Обработка и анализ системных журналов должны осуществляться регулярно, но не реже чем один раз в неделю.

3.5.3. В случае выявления нарушений администратор безопасности проводит мероприятия по выявлению виновников и причин нарушения. Результаты расследования доводятся до сведения руководства.

### 3.6 *Оказание методической и консультационной помощи пользователям*

3.6.1. Администратор безопасности организует и проводит инструктаж пользователей правилам применения и эксплуатации комплексов СЗИ НСД и периодически контролирует их знания.

3.6.2. Администратор безопасности должен оказывать методическую и консультационную помощь пользователям при применении и эксплуатации комплексов СЗИ НСД.

Начальник отдела организационной работы

и делопроизводства

П. А. Бочаров