**РОССИЙСКАЯ ФЕДЕРАЦИЯ**

**АДМИНИСТРАЦИЯ ТРУБЧЕВСКОГО МУНИЦИПАЛЬНОГО РАЙОНА**

**Р А С П О Р Я Ж Е Н И Е**

от 01.06.2021г. № 476-р

г. Трубчевск

Об утверждении Положения об управлении доступом субъектов доступа к объектам доступа в информационных системах персональных данных администрации Трубчевского муниципального района

В связи с осуществлением обработки персональных данных в информационных системах персональных данных администрации Трубчевского муниципального района, в соответствии  с [Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»](https://docs.cntd.ru/document/901990046), приказом Федеральной службы по техническому и экспортному контролю  от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке и информационных системах персональных данных», Приказом Федерального агентства правительственной связи и информации  при Президенте Российской Федерации [от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»](https://docs.cntd.ru/document/901790660), руководящим документом «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», утвержденным решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30.03.1992, иных нормативных документов по защите информации

1. Утвердить прилагаемые:

1.1. Положение об управлении доступом субъектов доступа к объектам доступа в информационных системах персональных данных администрации Трубчевского муниципального района (приложение 1);

1.2. Правила идентификации и аутентификации субъектов доступа и объектов доступа в информационных системах персональных данных администрации Трубчевского муниципального района (приложение 2);

1.3. Правила по ограничению программной среды в информационных системах персональных данных администрации Трубчевского муниципального района (приложение 3);

1.4. Правила регистрации событий безопасности в информационных системах персональных данных администрации Трубчевского муниципального района (приложение 4);

1.5. Перечень событий безопасности в информационных системах информационных системах персональных данных администрации Трубчевского муниципального района (приложение 5);

1.6. Регламент технологического процесса обработки защищаемой информации в информационных системах информационных системах персональных данных администрации Трубчевского муниципального района (приложение 6).

2. Начальнику организационно-правового отдела администрации Трубчевского муниципального района Москалевой О.А. довести настоящее распоряжение до сведения уполномоченных должностных лиц администрации Трубчевского муниципального района.

3. Администраторам безопасности ИСПДн администрации Трубчевского муниципального района в 2-хмесячный срок со дня принятия настоящего распоряжения обеспечить организацию обработки ПДн в ИСПДн администрации Трубчевского муниципального района в соответствии с нормативными документами по защите информации и настоящим распоряжением.

4. Настоящее распоряжение разместить на официальном сайте администрации Трубчевского муниципального района в сети Интернет по адресу: http://www.trubech.ru/ в течение 10 дней после его принятия.

5. Контроль за исполнением настоящего распоряжения возложить на заместителя главы администрации Трубчевского муниципального района С.Н. Тубол.

**Глава администрации**

**Трубчевского муниципального района И.И. Обыдённов**

Приложение 1

к распоряжению администрации

Трубчевского муниципального района

от 01.06.2021г. № 476-р

**ПОЛОЖЕНИЕ**об управлении доступом субъектов доступа к объектам доступа в информационных системах персональных данных администрации

Трубчевского муниципального района

I. Общие положения

1. Настоящее Положение определяет права и привилегии субъектов доступа, описывает разграничение доступа субъектов доступа к объектам доступа на основе совокупности правил разграничения доступа, установленных в информационных системах персональных данных администрации Трубчевского муниципального района (далее - Администрация), а также контроль соблюдения этих правил.

2. Разграничение прав осуществляется на основании Модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных (далее – ИСПДн) администрации Трубчевского муниципального района, а также исходя из характера и режима обработки персональных данных в ИСПДн Администрации.

3. Уровень прав доступа представлен в Таблице 1.

Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование ИСПДн, осуществляется в соответствии с их должностными обязанностями. Доступ к объектам доступа с учетом разделения полномочий (ролей) обеспечивается в соответствии с матрицей субъектов доступа по отношению к защищаемым информационным ресурсам в информационных системах Администрации (далее - матрица доступа).

Таблица 1

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| № п/п | Группа | Уровень доступа к ПДн, ТС, прикладному ПО и СЗИ | Разрешенные действия |
| 1 | Администратор ИСПДн | Доступ на правах администратора к ПДн, ТС и прикладному ПО. Без доступа к СЗИ | 1) модернизация, настройка и мониторинг работоспособности комплекса ТС (серверов, рабочих станций);  2) установка, модернизация, настройка и мониторинг работоспособности системного и базового ПО;  3) установка, настройка и мониторинг прикладного ПО;  4) соблюдение правил, оговоренных в инструкции администратора |
| 2 | Администратор ИБ ИСПДн | Доступ на правах администратора к СЗИ, сертифицированным СКЗИ. Без доступа на изменение к ПДн, ТС и прикладному ПО | 1) разработка, управление и реализация эффективной политики информационной безопасности системы;  2) управление (администрирование) системой защиты информации ИСПДн;  3) выявление инцидентов и реагирование на них;  управление конфигурацией ИСПДн и ее системы защиты;  4) контроль (мониторинг) за обеспечением уровня защищенности информации, содержащейся в ИСПДн;  управление правами доступа пользователей к функциям системы;  5) проверка состояния используемых СЗИ от НСД, проверка правильности их настройки;  6) обеспечение функционирования и поддержание работоспособности СЗИ;  проведение инструктажа эксплуатационного персонала и пользователей СВТ по правилам работы с используемыми СЗИ;  7) контроль и предотвращение несанкционированного изменения целостности ресурсов;  8) контроль аппаратной конфигурации защищаемых компьютеров и предотвращение попытки ее несанкционированного изменения;  9) поэкземплярный учет используемых криптосредств, эксплуатационной и технической документации к ним;  10) контроль за соблюдением условий использования криптосредств, установленных эксплуатационной и технической документацией на СКЗИ и настоящей инструкцией;  11) учет Пользователей криптосредств;  12) надежное хранение эксплуатационной и технической документации к криптосредствам, ключевых документов, носителей дистрибутивов криптосредств, бумажных и машинных носителей ПДн;  13) расследования и составление заключений по фактам нарушения условий использования СКЗИ, которые могут привести к снижению требуемого уровня безопасности информации |
| 3 | Администратор резервного копирования | Доступ на правах администратора к прикладному ПО. Без доступа на изменение ПДн, ТС и СЗИ | 1) настройка и контроль работы процедуры резервного копирования;  2) изготовление резервных копий информации;  3) анализ объемов данных резервного копирования;  4) контроль состояния оборудования системы резервного копирования;  5) замена неработоспособных или выработавших свой ресурс носителей резервной информации или оборудования системы резервного копирования;  6) восстановление программ и данных из резервных копий в случае порчи или утери данных |
| 4 | Ответственный за эксплуатацию СКЗИ | Доступ на правах пользователя к ПДн, ТС, прикладному ПО и СЗИ. Без доступа на изменение ПО, СЗИ и ТС | 1) осуществление контроля за целевым использованием ИСПДн, всех периферийных устройств и технических средств, входящих в состав ИСПДн;  2) контроль за отсутствием в период обработки защищаемой информации в помещении, где осуществляется обработка, посторонних лиц, не допущенных к обрабатываемой информации;  3) контроль использования сотрудниками структурных подразделений, эксплуатирующими ИСПДн, средств защиты информации, установленных на АРМ, входящих в состав ИСПДн;  4) контроль за правильностью использования и хранения сотрудниками структурных подразделений, эксплуатирующими ИСПДн, машинных носителей информации и документов, содержащих персональные данные;  5) представление заявок на пользователей, допускаемых к защищаемым ресурсам ИСПДн, с целью закрепления за ними носителей информации устройств блокировки, паролей и других средств разграничения доступа к информации, а также прав пользования средствами вычислительной техники;  7) организация повышения уровня осведомленности подчиненных должностных лиц по вопросам информационной безопасности;  8) разработка и принятие мер по предотвращению возможных негативных последствий нарушений |
| 5 | Пользователь | Доступ на правах пользователя к ПДн, ТС, прикладному ПО и СЗИ. Без доступа на изменение ПО, СЗИ и ТС | сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, предоставление записей, содержащих ПДн |

4. Доступ в помещения, в которых расположены технические средства ИСПДн Администрации (далее - Помещения), осуществляется в соответствии с перечнем лиц, утверждаемым правовым актом Администрации.

II. Правила разграничения доступа

5. В ИСПДн Администрации реализуется:

1) управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей, возлагается на администратора ИБ, путем следующих функций:

а) определение типа учетной записи (внутреннего пользователя, внешнего пользователя; системная, приложения; гостевая (анонимная), временная и (или) иные типы записей);

б) объединение учетных записей в группы (при необходимости);

в) верификация пользователя (проверка личности пользователя, его должностных (функциональных) обязанностей) при заведении учетной записи пользователя;

г) заведение, активация, блокирование и уничтожение учетных записей пользователей (при необходимости);

д) пересмотр и, при необходимости, корректировка учетных записей не реже одного раза в три месяца;

е) уничтожение временных учетных записей пользователей, предоставленных для однократного (ограниченного по времени) выполнения задач в информационной системе;

ж) предоставление пользователям прав доступа к объектам доступа ИСПДн, основываясь на задачах, решаемых пользователями в ИСПДн и взаимодействующими с ней ИСПДн.

Временная учетная запись может быть заведена для пользователя на ограниченный срок для выполнения задач, требующих расширенных полномочий, или для проведения настройки, тестирования информационной системы, для организации гостевого доступа (посетителям, сотрудникам сторонних организаций, стажерам и иным пользователям с временным доступом к информационной системе).

Заведение временных учетных записей осуществляется на основании подписанного администратором ИБ и ответственным за обработку и защиту персональных данных, соответствующего Акта, содержащего цель, место, наименование и сроки;

2) дискреционный метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе идентификационной информации субъекта и для каждого объекта доступа - списка, содержащего набор субъектов доступа (групп субъектов) и ассоциированных с ними типов доступа. Типы доступа должны включать операции по чтению, записи, удалению, выполнению и иные операции, разрешенные к выполнению пользователем (группе пользователей).

Правила разграничения доступа реализуются на основе матрицы доступа и обеспечивают управление доступом пользователей (групп пользователей) и запускаемых от их имени процессов при входе в систему, доступе к ТС, устройствам (в том числе внешним), объектам файловой системы, запускаемым и исполняемым модулям, объектам СУБД, параметрам настройки СЗИ, в том числе внутри виртуальных машин, информации о конфигурации системы защиты информации и иной информации о функционировании системы защиты информации.

В ИСПДн Администрации правила разграничения доступа должны обеспечивать:

а) управление доступом субъектов при входе в ИСПДн;

б) управление доступом субъектов к ТС, устройствам, внешним устройствам;

в) управление доступом субъектов к объектам, создаваемым общесистемным (общим) ПО;

г) управление доступом субъектов внутри виртуальной инфраструктуры;

3) в ИСПДн Администрации осуществляется управление информационными потоками при передаче информации между устройствами, сегментами в рамках информационной системы, включающее:

а) фильтрацию информационных потоков в соответствии с установленными правилами управления потоками;

б) разрешение передачи информации в ИСПДн Администрации только по установленному маршруту;

в) изменение (перенаправление) маршрута передачи информации в случаях необходимости, по согласованию с администратором информационной безопасности;

4) права и привилегии, назначаемые пользователям и запускаемым от их имени процессам, администраторам и лицам, обеспечивающим функционирование ИСПДн Администрации, являются минимально необходимыми для выполнения ими своих должностных обязанностей (функций);

5) ограничение неуспешных попыток входа в ИСПДн (доступа к ИСПДн), равное 5 (пяти), при этом обеспечивается блокирование устройства, с которого предпринимаются попытки доступа, и (или) учетной записи пользователя при превышении пользователем ограничения количества неуспешных попыток входа в ИСПДн (доступа к ИСПДн) не менее чем на 5 (пять) минут;

6) блокирование сеанса доступа в ИСПДн Администрации, после 15 минут времени бездействия (неактивности) пользователя или по его запросу.

Блокирование сеанса доступа пользователя в ИСПДн обеспечивает временное приостановление работы пользователя со СВТ или с виртуальной машиной, с которого осуществляется доступ к ИСПДн Администрации (без выхода из ИСПДн).

Для заблокированного сеанса осуществляется блокирование любых действий по доступу к информации и устройствам отображения, кроме необходимых для разблокирования сеанса.

Блокирование сеанса доступа пользователя в ИСПДн сохраняется до прохождения им повторной идентификации и аутентификации;

7) запрет всех действий пользователей до прохождения процедур идентификации и аутентификации в ИСПДн (кроме необходимых для прохождения процедур идентификации и аутентификации).

Администратору ИБ разрешаются действия в обход установленных процедур идентификации и аутентификации, необходимые только для восстановления функционирования ИСПДн в случае сбоев в работе или выходе из строя отдельных ТС (устройств).

Применяемые термины и сокращения:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  | Аутентификационная информация (информация аутентификации) | - | информация, используемая для установления подлинности (верификации) субъекта доступа в информационной системе |  |
|  | Аутентификация | - | проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности субъекта доступа в информационной системе) |  | |
|  | Идентификатор | - | представление (строка символов), однозначно идентифицирующее субъект и (или) объект доступа в информационной системе |  | |
|  | Идентификация | - | присвоение субъектам доступа, объектам доступа идентификаторов (уникальных имен) и (или) сравнение предъявленного идентификатора с перечнем присвоенных идентификаторов |  | |
|  | Локальный доступ | - | доступ субъектов доступа к объектам доступа, осуществляемый непосредственно через подключение (доступ) к компоненту информационной системы или через локальную вычислительную сеть (без использования информационно-телекоммуникационной сети) |  | |
|  | Многофакторная аутентификация | - | аутентификация с использованием двух (двухфакторная) или более различных факторов аутентификации |  | |
|  | Непривилегированная учетная запись | - | учетная запись пользователя (процесса, выполняемого от его имени) информационной системы |  | |
|  | Объект доступа | - | единица информационного ресурса информационной системы (файл, техническое средство, узел сети, линия (канал) связи, мобильное устройство, программа, том, каталог, запись, поле записей и иные объекты), доступ к которой регламентируется правилами разграничения доступа и по отношению к которой субъекты доступа выполняют операции |  | |
|  | Пользователь | - | лицо, которому разрешено выполнять некоторые действия (операции) по обработке информации в информационной системе или использующее результаты ее функционирования |  | |
|  | Привилегированная учетная запись | - | учетная запись администратора информационной системы |  | |
|  | Роль | - | предопределенная совокупность правил, устанавливающих допустимое взаимодействие между пользователем и информационной системой |  | |
|  | Субъект доступа | - | пользователь, процесс, выполняющие операции (действия) над объектами доступа и действия которых регламентируются правилами разграничения доступа |  | |
|  | Удаленный доступ | - | процесс получения доступа (через внешнюю сеть) к объектам доступа информационной системы из другой информационной системы (сети) или со средства вычислительной техники, не являющегося постоянно (непосредственно) соединенным физически или логически с информационной системой, к которой он получает доступ |  | |
|  | Управление доступом | - | ограничение и контроль доступа субъектов доступа к объектам доступа в информационной системе в соответствии с установленными правилами разграничения доступа |  | |
|  | ВИ | - | виртуальная инфраструктура |  | |
|  | ИБ | - | информационная безопасность |  | |
|  | ИСПДн | - | информационная система персональных данных |  | |
|  | НСД | - | несанкционированный доступ |  | |
|  | ПО | - | программное обеспечение |  | |
|  | СВТ | - | средство вычислительной техники |  | |
|  | СЗИ | - | средство защиты информации |  | |
|  | СКЗИ | - | средство криптографической защиты информации |  | |
|  | СУБД | - | система управления базой данных |  | |
|  | ТС | - | техническое средство |  | |

Приложение 2

к распоряжению администрации

Трубчевского муниципального района

от 01.06.2021г. № 476-р

**ПРАВИЛА**идентификации и аутентификации субъектов доступа и объектов доступа  
в информационных системах персональных данных администрации Трубчевского муниципального района

I. Общие положения

1. Настоящие Правила регламентируют порядок и процедуры присвоения субъектам и объектам доступа уникального признака (идентификатора), сравнения предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверки принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности), а также организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационной системе персональных данных (далее - ИСПДн) администрации Трубчевского муниципального района (далее - Администрация) и контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

II. Идентификация и аутентификация пользователей, являющихся внутренними пользователями

2. При доступе в информационную систему персональных данных (далее -ИСПДн) осуществляется идентификация и аутентификация пользователей, являющихся сотрудниками Администрации (внутренних пользователей), и процессов, запускаемых от имени этих пользователей, а также процессов, запускаемых от имени системных учетных записей. К внутренним пользователям относятся следующие должностные лица Администрации:

1) администратор ИСПДн;

2) администратор информационной безопасности (далее - ИБ) ИСПДн;

3) администратор резервного копирования;

4) ответственные сотрудники, выполняющие при эксплуатации ИСПДн свои должностные обязанности (функции) в соответствии с должностными инструкциями, утвержденными в Администрации и которым в ИСПДн присвоены учетные записи.

В качестве внутренних пользователей дополнительно рассматриваются должностные лица обладателя информации, заказчика, уполномоченного лица и (или) оператора иной информационной системы, а также лица, привлекаемые на договорной основе для обеспечения функционирования ИСПДн (ремонт, гарантийное обслуживание, регламентные и иные работы) в соответствии с организационно-распорядительными документами. Для каждого внутреннего пользователя в ИСПДн должны быть заведены учетные записи.

3. Пользователи ИСПДн однозначно идентифицируются и аутентифицируются для всех видов доступа, кроме тех видов доступа, которые определяются как действия, разрешенные до идентификации и аутентификации в соответствии с Положением об управлении доступом субъектов доступа к объектам доступа в ИСПДн Администрации.

4. Аутентификация пользователя в ИСПДн осуществляется с использованием паролей. Также на усмотрение администратора ИБ ИСПДн могут применяться аппаратные средства в случае многофакторной (двухфакторной) аутентификации.

5. В ИСПДн обеспечивается возможность однозначного сопоставления идентификатора пользователя с запускаемыми от его имени процессами.

III. Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов

6. В ИСПДн устанавливаются и реализуются следующие функции управления идентификаторами пользователей и устройств:

1) формирование идентификатора, который однозначно идентифицирует пользователя и (или) устройство;

2) присвоение идентификатора пользователю и (или) устройству;

3) предотвращение повторного использования идентификатора пользователя и (или) устройства в течение одного года;

4) блокирование идентификатора пользователя после 90 дней неиспользования;

5) В качестве ответственного за создание, присвоение и уничтожение идентификаторов пользователей и устройств определен Администратор ИБ ИСПДн.

IV. Управление средствами аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации

7. В ИСПДн устанавливаются и реализуются следующие функции управления средствами аутентификации (аутентификационной информацией) пользователей:

1) изменение аутентификационной информации (средств аутентификации), заданных их производителями и (или) используемых при внедрении системы защиты ИСПДн;

2) выдача средств аутентификации пользователям;

3) генерация и выдача начальной аутентификационной информации (начальных значений средств аутентификации);

4) установление характеристик пароля: длина пароля не менее шести символов, алфавит пароля не менее 6 символов, максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки 5 попыток, блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 15 минут, смена паролей не более чем через 120 дней;

5) блокирование (прекращение действия) и замена утерянных, скомпрометированных или поврежденных средств аутентификации;

6) назначение необходимых характеристик средств аутентификации (в том числе механизма пароля);

7) обновление аутентификационной информации (замена средств аутентификации) с периодичностью не более, чем через 120 дней;

8) защита аутентификационной информации от неправомерных доступа к ней и модифицирования.

8. В случае компрометации личного пароля пользователя ИСПДн должны быть немедленно предприняты меры в зависимости от полномочий владельца скомпрометированного пароля:

1) внеплановая смена личного пароля или удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение, переход на другую работу внутри организации и т.п.) должна производиться Администратором ИБ ИСПДн немедленно после окончания последнего сеанса работы данного пользователя с системой;

2) внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри организации и другие обстоятельства) Администратора ИБ ИСПДн и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой ИСПДн.

9. В качестве ответственного за хранение, выдачу, инициализацию, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации устройств определен Администратор ИБ ИСПДн.

V. Защита обратной связи при вводе аутентификационной информации

10. В ИСПДн осуществляется защита аутентификационной информации в процессе ее ввода для аутентификации от возможного использования лицами, не имеющими на это полномочий.

11. Защита обратной связи «система - субъект доступа» в процессе аутентификации обеспечивается исключением отображения для пользователя действительного значения аутентификационной информации и (или) количества вводимых пользователем символов аутентификационной информации. Вводимые символы пароля могут отображаться условными знаками«\*»,«» или иными знаками.

VI. Ответственность при организации идентификации и аутентификации

12. Ответственность за реализацию правил идентификации и аутентификации субъектов доступа и объектов доступа в соответствии с требованиями настоящих Правил возлагается на Администратора ИБ ИСПДн.

13. Ответственность за поддержание установленного порядка и соблюдение требований настоящих Правил возлагается на Администратора ИБ ИСПДн и пользователей ИСПДн.

14. Периодический контроль за выполнением всех требований настоящих Правил осуществляется комиссией по проведению мероприятий по защите персональных данных.

Приложение 3

к распоряжению администрации

Трубчевского муниципального района

от 01.06.2021г. № 476-р

**ПРАВИЛА**

по ограничению программной среды в информационных системах персональных данных администрации Трубчевского муниципального района

ОПС.1 Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения

Требования к реализации ОПС.1:

Оператором должны быть реализованы следующие функции по управлению запуском (обращениями) компонентов программного обеспечения:

- определение перечня (списка) компонентов программного обеспечения (файлов, объектов баз данных, хранимых процедур и иных компонентов), запускаемых автоматически при загрузке операционной системы средства вычислительной техники;

- разрешение запуска компонентов программного обеспечения, включенных в перечень (список) программного обеспечения, запускаемого автоматически при загрузке операционной системы средства вычислительной техники;

- ограничение запуска компонентов программного обеспечения от имени администраторов безопасности (например, разрешение такого запуска только для программного обеспечения средств защиты информации: сенсоры систем обнаружения вторжений, агенты систем мониторинга событий информационной безопасности, средства антивирусной защиты);

- настройка параметров запуска компонентов программного обеспечения от имени учетной записи администратора безопасности таким образом, чтобы текущий пользователь средства вычислительной техники не мог получить через данные компоненты доступ к объектам доступа, на доступ к которым у него нет прав в соответствии с УПД.2;

- контроль за запуском компонентов программного обеспечения, обеспечивающий выявление компонентов программного обеспечения, не включенных в перечень (список) компонентов, запускаемых автоматически при загрузке операционной системы средства вычислительной техники.

Правила и процедуры управления запуском программного обеспечения (в том числе списки программного обеспечения, ограничения запуска, параметры запуска компонентов программного обеспечения) регламентируются в организационно-распорядительных документах оператора по защите информации.

Требования к усилению ОПС.1:

1) в информационной системе обеспечивается разрешение запуска только тех программных компонентов, которые явно разрешены администратором безопасности;

2) в информационной системе обеспечивается использование средств автоматизированного контроля перечня (списка) компонентов программного обеспечения, запускаемого автоматически при загрузке операционной системы средства вычислительной техники;

3) в информационной системе обеспечивается использование автоматизированных механизмов управления запуском (обращениями) компонентов программного обеспечения;

4) в информационной системе обеспечивается управление удаленным запуском компонентов программного обеспечения (например, запрет запуска компонентов программного обеспечения на одном средстве вычислительной техники командой с другого средства вычислительной техники);

5) в информационной системе обеспечивается управление временем запуска и завершения работы компонентов программного обеспечения (например, ограничение запуска только в течение рабочего дня);

6) в информационной системе обеспечивается контроль целостности (состояния) запускаемых компонентов программного обеспечения (файлов (в том числе конфигурационных), объектов баз данных, подключаемых библиотек и др.) в соответствии с ОЦЛ.1;

7) в информационной системе обеспечивается контроль обновления запускаемых компонентов программного обеспечения;

8) в информационной системе обеспечивается регистрация событий, связанных с контролем состояния и обновлением запускаемых компонентов программного обеспечения;

9) в информационной системе обеспечивается запрет (блокирование) запуска определенных оператором компонентов программного обеспечения, не прошедших аутентификацию в соответствии с ИАФ.7.

Содержание базовой меры ОПС.1:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Мера защиты информации** | **Класс защищенности информационной системы** | | | |
|  | **4** | **3** | **2** | **1** |
| **ОПС.1** |  |  |  | **+** |
| **Усиление ОПС.1** |  |  |  | **1, 2, 3** |

ОПС. 2 Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения

Требования к реализации ОПС.2: Оператором должны быть реализованы следующие функции по управлению установкой (инсталляцией) компонентов программного обеспечения информационной системы:

- определение компонентов программного обеспечения (состава и конфигурации), подлежащих установке в информационной системе после загрузки операционной системы;

- настройка параметров установки компонентов программного обеспечения, обеспечивающая исключение установки (если осуществимо) компонентов программного обеспечения, использование которых не требуется для реализации информационной технологии информационной системы (например, при запуске установщика можно выбрать или не выбрать определенные опции и, тем самым, разрешить или запретить установку соответствующих компонентов программного обеспечения);

- выбор конфигурации устанавливаемых компонентов программного обеспечения (в том числе конфигурации, предусматривающие включение в домен, или невключение в домен);

- контроль за установкой компонентов программного обеспечения (состав компонентов, параметры установки, конфигурация компонентов);

- определение и применение параметров настройки компонентов программного обеспечения, включая программные компоненты средств защиты информации, обеспечивающих реализацию мер защиты информации, а также устранение возможных уязвимостей информационной системы, приводящих к возникновению угроз безопасности информации.

Правила и процедуры управления установкой (инсталляцией) компонентов программного обеспечения (в том числе управления составом и конфигурацией подлежащих установке компонентов программного обеспечения, параметрами установки, параметрами настройки компонентов программного обеспечения) регламентируются в организационно-распорядительных документах оператора по защите информации с учетом эксплуатационной документации.

Требования к усилению ОПС.2:

1) в информационной системе должно обеспечиваться использование средств автоматизации для применения и контроля параметров настройки компонентов программного обеспечения, влияющих на безопасность информации;

2) в информационной системе должны быть реализованы автоматизированные механизмы реагирования на несанкционированное изменение параметров настройки компонентов программного обеспечения, влияющих на безопасность информации, предусматривающие блокирование доступа к средству вычислительной техники и (или) информации, автоматическое восстановление параметров настройки или другие действия, препятствующие несанкционированному доступу к информации, который может быть получен вследствие несанкционированного изменения параметров настройки;

3) в информационной системе должно обеспечиваться использование средств автоматизации для инсталляции и централизованного управления процессами инсталляции, в том числе с применением пакетов соответствующих дистрибутивов программного обеспечения.

Содержание базовой меры ОПС.2:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Мера защиты информации** | **Класс защищенности информационной системы** | | | |
|  | **4** | **3** | **2** | **1** |
| **ОПС.2** |  |  | **+** | **+** |
| **Усиление ОПС.2** |  |  |  | **1** |

ОПС.3 Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов

Требования к реализации ОПС.3: Оператором должна быть обеспечена установка (инсталляция) только разрешенного к использованию в информационной системе программного обеспечения и (или) его компонентов.

Установка (инсталляция) в информационной системе программного обеспечения (вида, типа, класса программного обеспечения) и (или) его компонентов осуществляется с учетом перечня программного обеспечения и (или) его компонентов, разрешенных оператором к установке ("белый список"), и (или) перечнем программного обеспечения и (или) его компонентов, запрещенных оператором к установке ("черный список"). Указанные перечни программного обеспечения и (или) его компонентов разрабатываются оператором для информационной системы в целом или для всех ее сегментов или устройств в отдельности и фиксируются в организационно-распорядительной документации оператора по защите информации (документируются).

Установка (инсталляция) в информационной системе программного обеспечения и (или) его компонентов должна осуществляться только от имени администратора в соответствии с УПД.5.

Оператором должен обеспечиваться периодический контроль установленного (инсталлированного) в информационной системе программного обеспечения на предмет соответствия его перечню программного обеспечения, разрешенному к установке в информационной системе в соответствии с АНЗ.4, а также на предмет отсутствия программного обеспечения, запрещенного оператором к установке.

Требования к усилению ОПС.3:

Не установлены.

Содержание базовой меры ОПС.3:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Мера защиты информации** | **Класс защищенности информационной системы** | | | |
|  | **4** | **3** | **2** | **1** |
| **ОПС.3** | **+** | **+** | **+** | **+** |
| **Усиление ОПС.3** |  |  |  |  |

ОПС.4 Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов

Требования к реализации ОПС.4: В информационной системе должно осуществляться управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов.

Управление временными файлами должно обеспечивать перехват записи временной информации в файлы на системном (загрузочном) разделе машинного носителя информации средства вычислительной техники и ее перенаправление в оперативную память и (или) в другой раздел машинного носителя информации с последующей очисткой (стиранием).

Оператором должен быть определен и зафиксирован в организационно-распорядительной документации по защите информации (задокументирован) порядок очистки (стирания) временных файлов.

Требования к усилению ОПС.4:

1) в информационной системе должны осуществляться:

а) контроль доступа к временным файлам;

б) удаление временных файлов по завершении сеанса работы с ними.

Содержание базовой меры ОПС.4:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Мера защиты информации** | **Класс защищенности информационной системы** | | | |
|  | **4** | **3** | **2** | **1** |
| **ОПС.4** |  |  |  |  |
| **Усиление ОПС.4** |  |  |  |  |

Приложение 4

к распоряжению администрации

Трубчевского муниципального района

от 01.06.2021г. № 476-р

**ПРАВИЛА**  
регистрации событий безопасности в информационных системах персональных данных администрации Трубчевского муниципального района

I. Общие положения

1. Настоящие Правила регламентируют состав и содержание информации о событиях безопасности, подлежащих регистрации, правила и процедуры сбора, записи, хранения и защиты информации о событиях безопасности в информационной системе персональных данных (далее - ИСПДн) администрации Трубчевского муниципального района (далее - Администрация).

II. Определение событий безопасности, подлежащих регистрации,  
и сроков их хранения

2. В ИСПДн подлежат регистрации в текущий момент времени следующие события безопасности:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  | № п/п | События безопасности, подлежащие регистрации | Состав и содержание информации о событиях безопасности |  |
|  | 1 | Вход (выход), а также попытки входа субъектов доступа в информационную систему и загрузки (останова) операционной системы | Дата и время входа (выхода) в систему (из системы) или загрузки (останова) операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки (останова) операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа |  | |
|  | 2 | Подключение машинных носителей информации и вывод информации на носители информации | Дата и время подключения машинных носителей информации и вывода информации на носители информации, логическое имя (номер) подключаемого машинного носителя информации, идентификатор субъекта доступа, осуществляющего вывод информации на носитель информации |  | |
|  | 3 | Запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации | Дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный) |  | |
|  | 4 | Попытки доступа программных средств к защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей) | Дата и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого файла (логическое имя, тип) |  | |
|  | 5 | Попытки удаленного доступа | Дата и время попытки удаленного доступа с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), используемый протокол доступа, используемый интерфейс доступа и (или) иную информацию о попытках удаленного доступа к информационной системе |  | |
|  | 6 | Доступ субъектов доступа к компонентам виртуальной инфраструктуры | Дата и время доступа субъектов доступа к гипервизору и виртуальной машине, к хостовой операционной системе, результат попытки доступа субъектов доступа к указанным компонентам виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке доступа субъектов доступа к компонентам виртуальной инфраструктуры |  | |
|  | 7 | Изменения в составе и конфигурации компонентов виртуальной инфраструктуры во время их запуска, функционирования и аппаратного отключения | Дата и время изменения в составе и конфигурации виртуальных машин, виртуального аппаратного обеспечения, виртуализированного программного обеспечения, виртуального аппаратного обеспечения в гипервизоре и в виртуальных машинах, в хостовой операционной системе, виртуальном сетевом оборудовании, результат попытки изменения в составе и конфигурации указанных компонентов виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке изменения в составе и конфигурации компонентов виртуальной инфраструктуры |  | |
|  | 8 | Изменения правил разграничения доступа к компонентам виртуальной инфраструктуры | Дата и время изменения правил разграничения доступа к виртуальному и физическому аппаратному обеспечению, к файлам-образам виртуализированного программного обеспечения и виртуальных машин, к файлам-образам, используемым для обеспечения работы виртуальных файловых систем, к виртуальному сетевому оборудованию, к защищаемой информации, хранимой и обрабатываемой в гипервизоре и виртуальных машинах, в хостовой операционной системе, результат попытки изменения правил разграничения доступа к указанным компонентам виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке изменения правил разграничения доступа к компонентам виртуальной инфраструктуры |  | |

3. Сроки хранения соответствующих записей регистрационных журналов должны обеспечивать возможность обнаружения, идентификации и анализа инцидентов, возникших в ИСПДн, в течение 3-х месяцев.

III. Определение состава и содержания информации о событиях безопасности, подлежащих регистрации

4. Состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности, должны, как минимум, обеспечить возможность идентификации типа события безопасности, даты и времени события безопасности, идентификационной информации источника события безопасности, результат события безопасности (успешно или неуспешно), субъект доступа (пользователь и (или) процесс), связанный с данным событием безопасности.

5. Состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности, приведены в пункте 2 настоящих Правил.

IV. Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения

6. Процедуры сбора, записи и хранения информации о событиях безопасности в течение установленного времени хранения предусматривают:

1) возможность выбора администратором информационной безопасности событий безопасности, подлежащих регистрации в текущий момент времени из перечня событий безопасности, определенных в пункте 2 настоящих Правил;

2) генерацию (сбор, запись) записей регистрации (аудита) для событий безопасности, подлежащих регистрации (аудиту) в соответствии с пунктом 2 настоящих Правил, с составом и содержанием информации, установленными для соответствующего типа события;

3) хранение информации о событиях безопасности в течение времени, установленного в соответствии с пунктом 3 настоящих Правил.

7. Объем памяти для хранения информации о событиях безопасности рассчитывается и выделяется администратором информационной безопасности ИСПДн с учетом типов событий безопасности, подлежащих регистрации в соответствии с в пункте 2 настоящих Правил, составом и содержанием информации о событиях безопасности, подлежащих регистрации, прогнозируемой частоты возникновения подлежащих регистрации событий безопасности, срока хранения информации о зарегистрированных событиях безопасности.

V. Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них

8. Мониторинг (просмотр и анализ) записей регистрации (аудита) должен проводиться администратором информационной безопасности не реже двух раз в месяц для всех событий, подлежащих регистрации, и обеспечивать своевременное выявление признаков инцидентов безопасности в ИСПДн.

9. В случае выявления признаков инцидентов безопасности в ИСПДн администратор информационной безопасности осуществляет планирование и проведение мероприятий по реагированию на выявленные инциденты безопасности.

VI. Защита информации о событиях безопасности

10. Защита информации о событиях безопасности (записях регистрации (аудита)) в ИСПДн должна обеспечиваться применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования, определенных в проектной и организационно-распорядительной документации по защите информации, и в том числе включает защиту средств ведения регистрации (аудита) и настроек механизмов регистрации событий.

11. Доступ к записям аудита и функциям управления механизмами регистрации (аудита) предоставляется только администратору информационной безопасности и администратору виртуальной инфраструктуры.

Приложение 5

к распоряжению администрации

Трубчевского муниципального района

от 01.06.2021г. № 476-р

**ПЕРЕЧЕНЬ**событий безопасности в информационных системах персональных данных администрации Трубчевского муниципального района

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  | № п/п | Событие безопасности, подлежащее регистрации | Состав и содержание регистрационных записей |  |
|  | 1 | Вход (выход), а также попытки входа субъектов доступа в информационную систему и загрузки (останова) операционной системы | Дата и время входа (выхода) в систему (из системы) или загрузки (останова) операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки (останова) операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа |  | |
|  | 2 | Подключение машинных носителей информации и вывод информации на носители информации | Дата и время подключения машинных носителей информации и вывода информации на носители информации, логическое имя (номер) подключаемого машинного носителя информации, идентификатор субъекта доступа, осуществляющего вывод информации на носитель информации |  | |
|  | 3 | Запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации | Дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный) |  | |
|  | 4 | Попытки доступа программных средств к защищаемым объектам доступа | Дата и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого файла (логическое имя, тип) |  | |
|  | 5 | Попытки удаленного доступа | Дата и время попытки удаленного доступа с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), используемый протокол доступа, используемый интерфейс доступа и (или) иную информацию о попытках удаленного доступа к информационной системе |  | |
|  | 6 | Запуск (завершение) работы компонентов виртуальной инфраструктуры | Дата и время запуска (завершения) работы гипервизора и виртуальных машин, хостовой операционной системы, программ и процессов в виртуальных машинах, результат запуска (завершения) работы указанных компонентов виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке запуска (завершения) работы компонентов виртуальной инфраструктуры |  | |
|  | 7 | Доступ субъектов доступа к компонентам виртуальной инфраструктуры | Дата и время доступа субъектов доступа к гипервизору и виртуальной машине, к хостовой операционной системе, результат попытки доступа субъектов доступа к указанным компонентам виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке доступа субъектов доступа к компонентам виртуальной инфраструктуры |  | |
|  | 8 | Изменения в составе и конфигурации компонентов виртуальной инфраструктуры во время их запуска, функционирования и аппаратного отключения | Дата и время изменения в составе и конфигурации виртуальных машин, виртуального аппаратного обеспечения, виртуализированного программного обеспечения, виртуального аппаратного обеспечения в гипервизоре и в виртуальных машинах, в хостовой операционной системе, виртуальном сетевом оборудовании, результат попытки изменения в составе и конфигурации указанных компонентов виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке изменения в составе и конфигурации компонентов виртуальной инфраструктуры |  | |
|  | 9 | Изменения правил разграничения доступа к компонентам виртуальной инфраструктуры | Дата и время изменения правил разграничения доступа к виртуальному и физическому аппаратному обеспечению, к файлам-образам виртуализированного программного обеспечения и виртуальных машин, к файлам-образам, используемым для обеспечения работы виртуальных файловых систем, к виртуальному сетевому оборудованию, к защищаемой информации, хранимой и обрабатываемой в гипервизоре и виртуальных машинах, в хостовой операционной системе, результат попытки изменения правил разграничения доступа к указанным компонентам виртуальной инфраструктуры (успешная или неуспешная), идентификатор пользователя, предъявленный при попытке изменения правил разграничения доступа к компонентам виртуальной инфраструктуры |  | |

**Лист регистрации изменений**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  | |  | |  | |  | | |  | | |  |  |
|  |  |  |  |  |  | |  | |  | |  | | |  | | |  |  |
|  | Изм. | Номера пунктов | | | | | Всего пунктов в докум. | | N докум. | | Вх. N докум. и дата | | | Подп. | | | Дата |  |
|  |  | изменен-ных | заменен-ных | новых | аннулиро-ванных | |  | |  | |  | | |  | | |  |  |
|  |  |  |  |  | |  | |  | |  | |  |  | |  |
|  |  |  |  |  | |  | |  | |  | |  |  | |  |
|  |  |  |  |  | |  | |  | |  | |  |  | |  |
|  |  |  |  |  | |  | |  | |  | |  |  | |  |
|  |  |  |  |  |  | |  | |  | |  | | |  | | |  |  |
|  |  |  |  |  |  | |  | |  | |  | | |  | | |  |  |
|  |  |  |  |  |  | |  | |  | |  | | |  | | |  |  |
|  |  |  |  |  |  | |  | |  | |  | | |  | | |  |  |
|  |  |  |  |  |  | |  | |  | |  | | |  | | |  |  |
|  |  |  |  |  |  | |  | |  | |  | | |  | | |  |  |
|  |  |  |  |  |  | |  | |  | |  | | |  | | |  |  |
|  |  |  |  |  |  | |  | |  | |  | | |  | | |  |  |
|  |  |  |  |  |  | |  | |  | |  | | |  | | |  |  |

Приложение 6

к распоряжению администрации

Трубчевского муниципального района

от 01.06.2021г. № 476-р

**РЕГЛАМЕНТ**технологического процесса обработки защищаемой информации в информационных системах персональных данных администрации Трубчевского муниципального района

1. **Перечень использованных сокращений, единиц и терминов**

|  |  |  |
| --- | --- | --- |
| АИБ | – | администратор информационной безопасности. |
| АС | – | автоматизированная система. |
| АРМ | – | автоматизированное рабочее место. |
| ГМД | – | гибкий магнитный диск. |
| ИСПДн | – | информационная система персональных данных. |
| КИ | – | конфиденциальная информация. |
| ЛВС | – | локальная вычислительная сеть. |
| МНИ | – | отчуждаемые машинные носители информации. |
| МЭ | – | межсетевой экран. |
| НСД | – | несанкционированный доступ. |
| ОИ | – | объект информатизации. |
| ОС | – | операционная система. |
| ПДн | – | персональные данные |
| ПО | – | программное обеспечение. |
| ПЭВМ | – | персональная электронно-вычислительная машина. |
| СЗИ | – | средство защиты информации. |
| ЭВМ | – | электронно-вычислительная машина. |

Регламент технологического процесса обработки информации в информационных системах администрации Трубчевского муниципального района (далее – Администрация) разработан в соответствии с Федеральным законом от 26.07.2007 №152-ФЗ «О персональных данных».

Для целей настоящего Описания используются следующие основные понятия:

*Автоматизированная система* – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

*Администратор сети* – сотрудник или группа сотрудников, который выполняет функции администратора информационной безопасности, осуществляющие непосредственную организацию и выполнение работ по созданию (модернизации), техническому обслуживанию и управлению (администрированию) информационной управляющей ЛВС, включая технические аспекты информационной безопасности.

*Аутентификация* - проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности. Чаще всего аутентификация выполняется путем набора пользователем своего пароля на клавиатуре компьютера.

*Идентификатор доступа* – уникальный признак субъекта или объекта доступа.

*Идентификация* - присвоение субъектам доступа (пользователям, процессам) и объектам доступа (информационным ресурсам, устройствам) идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

*Администратор информационной безопасности* – специалист или группа специалистов, осуществляющие контроль за обеспечением защиты информации в ЛВС, а также осуществляющие организацию работ по выявлению и предупреждению возможных каналов утечки информации, потенциальных возможностей осуществления НСД к защищаемой информации.

*Информация* – сведения (сообщения, данные) независимо от формы их представления.

*Информационная безопасность* – состояние защищенности информационной среды, обеспечивающее ее формирование, использование и развитие в организации.

*Информационная система* - совокупность программного обеспечения и технических средств, используемых для хранения, обработки и передачи информации, с целью решения различных задач подразделений. В организации используются различные типы информационных систем для решения различных задач.

*Информационные ресурсы* – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий, используемая в процессах организации.

*Конфиденциальная информация* - информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

*Локальная вычислительная сеть (ЛВС)* - группа ЭВМ, а также периферийное оборудование, объединенные одним или несколькими автономными высокоскоростными каналами передачи цифровых данных в пределах одного или нескольких близлежащих зданий.

*Межсетевой экран (МЭ)* - программно-аппаратный комплекс, используемый для контроля доступа между ЛВС, входящими в состав корпоративной сети, а также между корпоративной сетью и внешними сетями (сетью Интернет).

*Несанкционированный доступ к информации (НСД)* – доступ к информации, нарушающий правила разграничения уровней полномочий пользователей.

*Обработка персональных данных* – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

*Операционная система* – системная программа, осуществляющая взаимодействие пользователя и прикладных программ с аппаратной частью ЭВМ.

*Оператор* – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных;

*Пароль* – идентификатор субъекта доступа, который является его (субъекта) секретом.

*Персональные данные* – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

*Пользователь ЛВС* – сотрудник Администрации (штатный, временный, работающий по контракту и т.п.), а также прочие лица (подрядчики, аудиторы и т.п.), зарегистрированный в корпоративной сети в установленном порядке и получивший права на доступ к ресурсам корпоративной сети в соответствии со своими функциональными обязанностями.

*Программное обеспечение* – совокупность прикладных программ, установленных на сервере или ЭВМ.

*Рабочая станция* – персональный компьютер, на котором пользователь сети выполняет свои служебные обязанности.

*Сервер* – выделенный компьютер, имеющий разделяемые ресурсы, выполняющий определенный перечень задач и предоставляющий пользователям ЛВС ряд сервисов.

*Структурное подразделение* – отраслевой (функциональный) орган, структурное подразделение Администрации с самостоятельными функциями, задачами и ответственностью.

2. Назначение и задачи применения АС

2.1. АС Администрации предназначена для разработки, распечатки, хранения в электронном виде КИ и ПДн.

С документами, содержащими сведения ограниченного распространения, работают сотрудники Администрации, имеющие соответствующую форму допуска и доступ к ресурсам АС и ИСПДн.

Технологический процесс обработки информации в АС и ИСПДн включает в себя:

внесение КИ и ПДн в базы данных, просмотр и редактирование необходимой информации, печать документов на бумажном носителе, обмен файлами на МНИ по каналам связи;

обеспечение необходимого уровня безопасности обработки, хранения и передачи КИ и ПДн.

2.2. Задачами применения АС и ИСПДн являются:

* работа с базами данных КИ и ПДн, внесение в них изменений, их хранение и уничтожение;
* работа с файлами конфиденциальных документов;
* подготовка и работа с МНИ для передачи их по каналам связи;
* распечатка документов, содержащих КИ и ПДн;
* размножение необходимого числа экземпляров документов на принтере;
* обеспечение необходимого уровня безопасности обработки, хранения КИ и ПДн;
* обеспечение в АС и ИСПДн разграничения доступа к КИ и ПДн;
* антивирусная защита программной среды и данных;
* регистрация пользователей СЗИ от НСД перед началом сеанса работы на ПЭВМ, входящей в состав АС и ИСПДн, назначение им прав доступа к защищаемым ресурсам;
* резервное копирование информации на МНИ, учтенные в установленном порядке в соответствии с требованиями инструкции по обращению с носителями АС и ПДн;
* восстановление информации, поврежденной или стертой при сбоях в работе ПЭВМ с резервных копий.

3. Расположение ОИ. Организация охраны и контроля доступа

3.1. АС, обрабатывающая КИ, расположена в здании по адресу: 242220, Брянская область, Трубчевский район, г.Трубчевск, ул.Брянская, д.59.

Помещения Администрации оборудованы техническими средствами защиты (сигнализация), ведется физическая охрана помещений.

Доступ сотрудников и других лиц в помещения Администрации, в которых осуществляется обработка КИ, осуществляется в соответствии с утвержденным списком лиц, имеющих доступ к КИ.

3.2. ИСПДн, обрабатывающая ПДн, расположена в здании по адресу 242220, Брянская область, Трубчевский район, г.Трубчевск, ул.Брянская, д.59.

Помещения Администрации оборудованы техническими средствами защиты (сигнализация), ведется физическая охрана помещений.

Доступ сотрудников и других лиц в помещения Администрации, в которых осуществляется обработка ПДн, осуществляется в соответствии с утвержденным списком лиц, имеющих доступ к ПДн.

4. Состав АС, обрабатывающих ПДн

4.1. В состав АС Администрации, обрабатывающих КИ, входят «\_\_\_\_\_» АРМ, которые функционируют без подключения к локальной сети, и не имеют подключение к сети Интернет.

4.2. В состав ИСПДн Администрации, обрабатывающих ПДн, входят «\_\_\_\_\_» АРМ, которые функционируют в рамках локальной сети, и имеют подключение к сети Интернет.

Питание ПЭВМ и принтера обеспечивается от сети электропитания 220В. Трансформаторная подстанция находится за пределами контролируемой зоны. К трансформаторной подстанции подключены сторонние потребители. Контур заземления оборудован в непосредственной близости от здания.

5. Источники данных АС

5.1. Источниками данных для АС Администрации являются:

Данные на бумажных носителях.

Данные на МНИ - файлы, подготовленные в другой АС.

Вводимые пользователями данные - сведения, вводимые с клавиатуры операторами (пользователями).

Источниками данных для ИСПДн Администрацииявляются:

Данные на бумажных носителях.

Данные на МНИ - файлы, подготовленные в другой ИСПДн.

Вводимые пользователями данные - сведения, вводимые с клавиатуры операторами (пользователями).

5.2. Входными данными является информация, поступающая в АС и ИСПДн на различных носителях: данные на бумажных носителях, данные на МНИ, данные, вводимые операторами (пользователями) с клавиатуры.

Исходные данные поступают в АС и ИСПДн Администрацииот сотрудников, сторонних организаций и клиентов, обращающихся вАдминистрацию.

Все носители информации регистрируются, хранятся и передаются в соответствии с требованиями инструкции по обращению с носителями КИ и ПДн.

5.2. Выходными данными являются подготовленные и распечатанные в АС и ИСПДн конфиденциальные и неконфиденциальные текстовые документы, файлы, содержащие КИ и ПДн, передаваемые по каналам связи.

6. Используемые программные средства

На ПЭВМ Администрации установлена ОС Windows, дистрибутивы версии ОС хранятся у АИБа.

Функции, права и обязанности, ответственных за эксплуатацию объекта информатизации регламентируются инструкцией о порядке технического обслуживания, ремонта, модернизации технических средств, входящих в состав АС и ИСПДн.

Разрешенное к использованию ПО указывается в перечне разрешенного к использованию в АС и ИСПДн ПО, который разрабатывается АИБом совместно с системным администратором. Пользователям запрещено приносить и устанавливать на рабочие станции АС и ИСПДн ПО без согласования с АИБом.

7. Ресурсы АС

К ресурсам АС иИСПДн Администрацииотносятся файлы, каталоги, тома, диски, устройства вывода информации (СD-RW, COM и LPT порты, порты USB, ГМД).

Информационные ресурсы, предназначенные для хранения и обработки КИ и ПДн, перечислены в утвержденном перечне защищаемых информационных ресурсов.

Разграничение доступа пользователей к портам ввода-вывода информации в АС иИСПДн Администрации реализовано в разрешительной системе доступа.

Если доступ пользователя к конкретному информационному ресурсу не определен, то доступа к нему он не имеет.

Запрещается хранить КИ и ПДн на ресурсах, отличных от перечисленных в утвержденном перечне защищаемых ресурсов.

8. Антивирусная защита

Антивирусная защита осуществляется с применением разрешенных программных средств в соответствии с инструкцией по проведению антивирусного контроля в АС и ИСПДн.

Используемые антивирусные средства указываются в Перечне разрешенного к использованию в АС и ИСПДн программного обеспечения.

9. Обеспечение безопасности информации

Оператор должен обеспечивать надлежащие условия защиты КИ и ПДн, хранящихся в используемых АС и ИСПДн, от несанкционированного доступа, использования, распространения, искажения и уничтожения. Сотрудники, уполномоченные осуществлять обработку персональных данных, несут ответственность за защиту КИ и ПДн в порядке, предусмотренном действующим законодательством Российской Федерации.

Настройку СЗИ от НСД для конкретных пользователей, контроль её работы, обновление антивирусных баз, диагностику и устранение неисправностей или сбоев в работе программного или аппаратного обеспечения осуществляет АИБ с обязательным подписанием совместного протокола об установке ПО с указанием даты установки, фамилии, имени, отчества, должности получателя - ответственного лица оператора.

Функции, права, обязанности АИБа, а также порядок ремонта и модернизации регламентируются специально разработанными инструкцией о порядке технического обслуживания, ремонта, модернизации технических средств, входящих в состав ИСПДн и должностной инструкцией АИБа.

Повседневный контроль защищенности АС и ИСПДн от НСД проводится АИБом. Контроль осуществляется с помощью штатных средств СЗИ от НСД. Основным средством контроля является анализ системного журнала.

Доступ пользователей к работе в АС и ИСПДн осуществляется строго в соответствии со списком постоянных пользователей АС и ИСПДн, разрабатываемым АИБом.

Допускается наличие только пользователей, указанных в списке постоянных пользователей АС и ИСПДн, имеющих доступ к КИ и ПДн.

При необходимости исполнителям может быть выдан персональный электронный идентификатор СЗИ, предназначенный для идентификации при входе в систему.

Программирование, учет выдачи персональных электронных идентификаторов от СЗИ и контроль за их наличием возлагается на АИБа.

Права доступа пользователей к программам, каталогам, файлам определены в списке постоянных пользователей АС и ИСПДн (матрица доступа к защищаемым ресурсам).

Порядок работы пользователя определены в инструкции по работе пользователя в АС Администрации.

10. Задачи технологического процесса обработки информации в АС и ИСПДн

10.1. Технологический процесс обработки информации в АС и ИСПДн Администрации включает в себя задачи:

- получения исходных данных, их подготовка, оформление, регистрация и выдача пользователям АС и ИСПДн Администрации;

**-** оформления, регистрации и передачи выходных данных;

- ввода, подготовки, обработки, хранения и вывода информации в АС и ИСПДн;

- настройку, управление и техническое сопровождение СЗИ.

10.2. Задача получения исходных данных, их подготовка, оформление, регистрация и выдача пользователям АС и ИСПДн Администрации состоит из следующих этапов:

получение ПДн на бумажных носителях и в электронном виде от сторонних организаций, клиентов, и выдача пользователям АС и ИСПДн Администрации;

распечатка электронных файлов документов, содержащих ПДн на принтере АС и ИСПДн;

передача сведений на бумажных носителях и в электронном виде, обработанных пользователями АС и ИСПДн Администрации в сторонние организации по каналам передачи данных.

Полученные МНИ регистрируются, ставятся на учет и хранятся в соответствии с требованиями инструкции по обращению с носителями КИ, а затем используются сотрудниками Администрациидля обработки информации.

10.3. Задач оформления, регистрации и передачи выходных данных выполняются сотрудниками, ответственными за ведение конфиденциального делопроизводства в подразделениях.

Они регистрируют МНИ в соответствии с требованиями инструкции по обращению с носителями конфиденциальной информации. В соответствии с указанной инструкцией происходит оформление МНИ.

10.4. Задачи ввода, подготовки, обработки, хранения и вывода информации в АС и ИСПДн выполняются сотрудниками ответственными за ведение конфиденциального делопроизводства в подразделениях.

Задачи выполняются с помощью, установленного на рабочей станции АС и ИСПДн ПО, указанного в утвержденном перечне разрешенного к использованию в ПО.

Все файлы, содержащие ПДн, хранятся и обрабатываются только в специальных каталогах, входящих в утвержденный перечень защищаемых информационных ресурсов. Права доступа назначаются АИБом в соответствии с разрешительной системой доступа.

Копирование файлов с МНИ в специальные каталоги на жестком диске ПЭВМ, а также (в случае необходимости) предварительное изменение скопированных файлов. Файлы содержат текстовую информацию (техническую документацию, электронные документы и т.д.).

Создание сотрудниками ответственными за ведение конфиденциального делопроизводства в подразделениях конфиденциальных документов, их редактирование, уничтожение, хранение в специальных каталогах на жестком диске ПЭВМ или учтенных МНИ.

Запись созданных текстовых файлов на учтенные МНИ осуществляется сотрудниками в соответствии с его функциональными обязанностями и разрешительной системой доступа.

Регистрация созданных текстовых файлов.

Задачи выполняется пользователями АС и ИСПДн вручную сразу после подготовки конфиденциальных файлов и сохранения их на жесткий диск ПЭВМ, копирования конфиденциальных файлов на МНИ.

Удаление файлов с жестких магнитных дисков или МНИ осуществляется специальными средствами удаления информации, несколькими циклами затирания информации. В случае если МНИ выводится из обращения он подлежит физическому уничтожению в соответствии с требованиями инструкции по обращению с носителями КИ.

10.5. Настройка, управление и техническое сопровождение СЗИ проводится АИБом и включает следующие операции:

установка и настройка безопасной операционной среды для пользователей АС и ИСПДн. На этом этапе производится: установка и настройка операционной системы рабочих станций, подключение и конфигурирование устройств ввода-вывода информации в/из АС и ИСПДн, установка и настройка СЗИ, регистрация в СЗИ пользовательских учетных записей и настройка прав доступа для каждого пользователя в соответствии с его функциональными обязанностями (в том числе программирование, регистрация и выдача пользователям АС и ИСПДн персональных идентификаторов, а также учет и контроль за наличием их у пользователей), создание, предварительное наполнение информацией (не содержащей сведения, составляющие государственную тайну) и конфигурирование ресурсов АС и ИСПДн, реализация правил разграничения доступа к этим ресурсам в соответствии с разрешительной системой доступа, настройка парольной политики, политики затирания данных и т.д. Права доступа пользователей к программам, каталогам, файлам определены в разрешительной системе доступа к защищаемым ресурсам АС и ИСПДн Администрации.

непрерывный мониторинг безопасности в АС и ИСПДн с целью выявления нарушений правил разграничения доступа пользователями АС и ИСПДн, диагностики и последующего устранения выявленных неисправностей или ошибок в работе программно-аппаратного обеспечения операционной среды АС и ИСПДн. Данная задача выполняется администратором информационной безопасности путем регулярного анализа системных журналов операционной системы и СЗИ от НСД, регулярных проверок соответствия реализованных в АС и ИСПДн правил разграничения доступа к ресурсам, требованиям разрешительной политики доступа, регулярных проверок правильности соблюдения пользователями требований по защите информации.

регулярное сопровождение подсистемы безопасности с целью обеспечения эффективности работы пользователей АС и ИСПДн и обеспечения защиты информации. Данная задача выполняется администратором информационной безопасности и ответственным за эксплуатацию ПЭВМ (в части касающейся организационных мероприятий по защите информации) регулярно (по расписанию) или при обнаружении внештатных ситуаций и регламентируется инструкцией о порядке технического обслуживания, ремонта, модернизации технических средств, входящих в состав АС и ИСПДн. Задача включает следующие операции: регулярное проведение инструктажа пользователей по безопасной работе в АС и ИСПДн, устранение выявленных неисправностей и ошибок (осуществляется администратором информационной безопасности), регулярные обновление прикладного ПО и обеспечение его целостности.

11. Этапы технологического процесса

11.1. Доступ пользователей к работе в АС и ИСПДн

Доступ пользователей к информационным ресурсам определяется на основании списка постоянных пользователей АС и ИСПДн и перечня защищаемых информационных ресурсов, Администрации.

Права доступа к информационным ресурсам назначаются каждому пользователю на основании разрешительной системы доступа, разрабатываемой АИБом.

Разграничение прав доступа пользователей к информационным ресурсам и установление полномочий этим пользователям реализуется АИБом средствами ОС и дополнительными средствами СЗИ от НСД.

Вход в систему осуществляется по персональному имени (персональному идентификатору) и паролю конкретного пользователя. При успешном входе в систему пользователь получает права доступа к устройствам, каталогам, файлам и программам, установленные АИБом.

При увольнении пользователя или переходе в другое подразделение, АИБом или системным администратором на основании приказа, в последний день работы пользователя (или иной день, указанный в приказе), производится удаление учетной записи пользователя и всех его ресурсов (за исключением необходимых для работы других пользователей).

11.2. Начало сеанса работы.

Перед началом сеанса работы пользователь включает свою рабочую станцию и проходит процедуру аутентификации.

В процессе аутентификации пользователь использует свои личные логин и пароль. Смена личного пароля производится не реже 1 раза в три месяца. Контроль данного процесса осуществляется АИБом.

11.3. Регистрация пользователей и назначение прав доступа.

Регистрация пользователей и назначение прав доступа производится администратором информационной безопасности на основании заявления «На создание (продление) учетной записи пользователя».

Зарегистрированный пользователь устанавливает свой личный пароль.

Права доступа устанавливаются пользователю средствами ОС в соответствии с разрешительной системой доступа.

Удаление пользователя выполняется однократно при необходимости выведения сотрудника из числа пользователей АС и ИСПДн Администрации.

11.4. Работа с файлами документов, внесение изменений, хранение

Файлы документов разрабатываются на рабочем месте пользователем, зарегистрированным в АС и ИСПДн Администрации.

Работа пользователя при подготовке файла документа возможна только после успешного прохождения процедуры аутентификации в АС и ИСПДн.

Пользователи имеют право постоянного хранения файлов с конфиденциальными и не конфиденциальными данными, ПДн на жестком магнитном диске только в специально выделенных АИБом каталогах.

Разработка и подготовка к печати документов производится с применением, установленных на рабочей станции, текстовых и табличных редакторов.

Распечатка документов производится на принтере, размещенном на ОИ и включенном в технический паспорт на этот ОИ.

По окончании сеанса подготовки документа производится его сохранение в виде файла в разрешенном каталоге или на закрепленный за пользователем МНИ, соответствующим образом зарегистрированный.

В случае отсутствия необходимости дальнейшей работы с документом, впервые набранным с клавиатуры, пользователь может отказаться от сохранения его в виде файла.

Также пользователь может отказаться от сохранения внесенных в файл изменений.

11.5. Уничтожение файлов, содержащих конфиденциальные данные

Удаление данных (файлов) и временных файлов производится штатными средствами ОС при включенном режиме затирания данных или СЗИ от НСД (в том числе автоматическое обнуление файла подкачки).

Уничтожение файла может быть произведено без распечатки документа, если в документе отпала необходимость.

При установке операционной системы должна быть отключена функция удаления файлов через «корзину».

При установке СЗИ от НСД в ней должна быть активирована функция затирания данных с применением не менее 3-х циклов затирания.

Факт удаления КИ и ПДн с МНИ регистрируется в специальном журнале. Запись в журнал производит пользователь, уничтоживший эту информацию.

11.6. Работа с МНИ

11.6.1 Общие понятия

Для разработки и хранения файлов с КИ и ПДн могут использоваться МНИ, учтенные в установленном порядке в соответствии с требованиями инструкции по обращению с носителями КИ.

В качестве МНИ в АС и ИСПДн Администрации могут использоваться (разрешены к использованию) следующие накопители информации:

гибкие магнитные диски;

оптические (лазерные) диски;

USB flash накопители (накопители информации, подключаемые к USB порту ввода–вывода ПЭВМ).

USB flash накопители учитываются в установленном порядке в соответствии с требованиями инструкции по обращению с носителями конфиденциальной информации.

МНИ при необходимости выдаются каждому пользователю из числа сотрудников, обрабатывающих конфиденциальные сведения и персональные данные. Выданный носитель предназначен только для хранения файлов подготовленных документов. Операции с МНИ для КИ и ПДн могут проводиться только на ПЭВМ, входящей в состав АС и ИСПДн аттестованных для работы с информацией соответствующей категории.

11.6.2. Подготовка МНИ. Выведение из обращения МНИ

При необходимости создания нового МНИ, пользователь регистрирует его в соответствии с требованиями инструкции по обращению с КИ.

При необходимости пользователь сдает зарегистрированный МНИ администратору информационной безопасности с целью его подготовки для дальнейшего использования на ПЭВМ, входящей в состав АС.

Выведение МНИ из обращения производится путем его физического уничтожения, при этом составляется акт соответствующей формы, предусмотренной инструкцией по обращению с носителями КИ.

11.6.3. Создание файлов на МНИ.

Условиями, необходимыми для выполнения данной процедуры, являются:

пользователю разрешено самостоятельно копировать файлы на МНИ и обратно;

наличие у пользователя подготовленного и зарегистрированного соответствующим образом МНИ.

11.6.4. Хранение МНИ пользователя.

Хранение МНИ пользователя должно осуществляться в соответствии с требованиями инструкции по обращению с носителями КИ и ПДн.

11.7. Распечатка документов на печатающем устройстве компьютера (принтере).

Условием, необходимым для распечатки документов, является наличие у пользователя:

* прав доступа к защищаемым ресурсам АС и ИСПДн;
* подготовленных и зарегистрированных соответствующим образом листов.

Регистрация листов, используемых для распечатки конфиденциальных документов, осуществляется пользователем в соответствии с требованиями инструкции по обращению с носителями КИ.

Пользователь, распечатавший конфиденциальный документ, немедленно регистрирует его у сотрудника, ответственного за ведение конфиденциального делопроизводства.

Оформление, распечатка, учёт и уничтожение документов производится в соответствии с требованиями настоящего технологического процесса, инструкцией по работе пользователя в АС и ИСПДн, инструкции по обращению с носителями КИ.

Контроль за распечаткой документов возлагается на ответственного за эксплуатацию ОИ.

11.8. Резервное копирование.

Резервное копирование информационных ресурсов производится АИБом или системным администратором в соответствии с правами доступа на МНИ, учтенные в порядке, установленным инструкцией по резервному копированию.

11.9. Передача информации

Передача файлов КИ и ПДн на МНИ в другие подразделения Администрации, а также организации иной ведомственной подчинённости, производится по каналам связи, в соответствии с требованиями законодательства РФ по обеспечению защиты КИ и инструкции по обращению с носителями КИ.

11.10. Завершение сеанса работы

По завершении работы пользователь выполняет штатную процедуру завершения работы в Windows, выключает рабочую станцию и сдаёт имеющиеся МНИ сотруднику, ответственному за работу пользователей с МНИ.

12. Заключительные положения

Всем сотрудникам, допущенным к работе с КИ и ПДн, разъясняется ответственность за нарушение правил получения, обработки, защиты КИ и ПДн.

Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту ПДн субъектов ПДн, несут ответственность в соответствии с действующим законодательством.