Приложение № 15
к распоряжению Администрации
ЗАТО г. Железногорск
от 30.06.2014 № 132пр

Положение о разрешительной системе доступа в информационных системах персональных данных Администрации ЗАТО г. Железногорск

2013

1 Общие положения

Настоящее Положение разработано в соответствии с «Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденным приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». Положение определяет порядок установления уровня полномочий пользователей, а также правила разграничения доступа к защищенным техническим, программным средствам и информационным ресурсам информационных систем персональных данных (ИСПДн) «АРМ «Общественная приемная», «Бухгалтерия», «Гаражи и усадьбы», «Кадры», «АРМ «ЖФСИ», «СОТО», «АРМ «Договора», «АРМ «Учет карточек профсоюза», «АРМ «Административная комиссия», «АРМ «Спортсмены» и «АРМ «Формирование изменений списков избирателей» Администрации ЗАТО г. Железногорск (далее Администрация).

Положение определяет порядок установления уровня полномочий пользователей информационных систем персональных данных (ИСПДн) Администрации, в которых производится обработка сведений, содержащих персональные данные, а также правила разграничения доступа к защищаемым техническим, программным средствам и информационным ресурсам ИСПДн.

Под разрешительной системой доступа (РСД) понимается процесс определения для всех категорий пользователей соответствующей программно-аппаратной среды или информационных и программных ресурсов (узлов сети, автоматизированных рабочих мест (АРМ), внешних устройств, файлов, программ, процессов и т.п.), которые будут им доступны для конкретных операций (Read, Write, и т. п.) с помощью заданных программно-аппаратных средств доступа.

Правила разграничения доступа, регламентирующие права доступа пользователей к защищаемым ресурсам ИСПДн, основываются на задании множества разрешительных отношений доступа в виде триады: <объект, субъект, тип доступа>. Правила доступа пользователя к ИСПДн определяются ответственным за обработку ПДн и администратором безопасности ИСПДн и задаются с помощью настроек системы защиты информации (СЗИ) от несанкционированного доступа (НСД), установленной на объекте.

Администрирование системы защиты информации от несанкционированного доступа, управление процессом установления прав и полномочий в ИСПДн, а также установку (изменение) имен пользователей, их паролей и прочих атрибутов идентификации в ИСПД производит администратор безопасности ИСПДн по согласованию с ответственным за обработку ПДн.

При изменении (модернизации) действующих автоматизированных программных комплексов, появлении нового программного обеспечения, администратором безопасности разрабатываются предложения по изменению и

(или) дополнению перечня прав и полномочий пользователей. Процедура регистрации (создания учетной записи) пользователя для сотрудника и предоставления ему (или изменения его) прав доступа к ресурсам ИСПДн выполняется в соответствии с Регламентом предоставления прав доступа к персональным данным.

Уровень прав и полномочий пользователей ИСПДн, необходимый им для выполнения своих функций, уточняется и согласовывается с ответственным за обеспечение безопасности персональных данных.

Замена технических средств ИСПДн при проведении работ по устранению неисправностей, регламентных и других видов работ, осуществляется администратором безопасности ИСПДн только по согласованию с ответственным за обработку ПДн.

Техническое обслуживание и ремонт средств вычислительной техники, предназначенных для обработки персональных данных, рекомендуется проводить технически подготовленными сотрудниками предприятия, либо организациями, имеющими соответствующие лицензии.

При проведении технического обслуживания и ремонта запрещается передавать ремонтным организациям узлы и блоки с элементами накопления и хранения защищаемой информации. Они должны быть изъяты из системных блоков и оставлены для хранения в отделе системных администраторов или серверном помещении. При неисправности таких узлов и блоков - они уничтожаются установленным порядком.

Контроль за организацией и соблюдением пользователями систем установленного порядка разграничения доступа к разделяемым ресурсам ИСПДн осуществляется администратором безопасности.

Периодически проводится проверка разрешенных и запрещенных связей между субъектами и объектами доступа к защищаемым ресурсам с привязкой к конкретному АРМ ИСПДн и пользователю, а также их соответствие РСД.

2 Разрешительная система доступа пользователей к техническим и программным средствам и информационным ресурсам ИСПДн

Обработка ПДн осуществляется в ИСПДн, состав которой определен в Техническом паспорте ИСПДн. Пользователь, в соответствии со своими правами доступа к информации, осуществляет ее обработку с использованием программных средств, установленных в ИСПДн. Файлы с персональными данными, в процессе обработки и хранения, записываются на НЖМД. Подробное описание обработки информации в ИСПДн отражено в Описании технологического процесса обработки информации.

2.1 Доступ к информационным ресурсам работников Администрации

Доступ к персональным данным разрешает Глава администрации ЗАТО г. Железногорск только специально уполномоченным лицам с соблюдением требований «Положения по обработке персональных данных».

Фактом ознакомления с разрешением на доступ является подпись работника в листе ознакомления Инструкции пользователя ИСПДн.

2.2 Доступ к информационным ресурсам сторонних организаций, деятельность которых регламентируется законодательством Российской Федерации

К организациям, деятельность которых регламентируется законодательством РФ, могут относиться:

- правоохранительные органы;
- судебные органы;
- органы статистики;
- органы исполнительной и законодательной власти субъектов Российской Федерации:
- средства массовой информации и пр.

Допуск к информационным ресурсам таких организаций регламентируется законодательством Российской Федерации, договорами и соглашениями об информационном обмене и другими нормативными актами.

2.3 Доступ к информационным ресурсам Администрации сторонних организаций, выполняющих работы в Администрации на договорной основе

К организациям, выполняющим работы на договорной основе, могут относиться:

- организации, выполняющие строительные работы и осуществляющие ремонт зданий, систем инженерно-технического обеспечения (отопления, освещения, водоснабжения, канализации, электропитания, кондиционирования и т.п.);
- организации, осуществляющие монтаж и настройку ПЭВМ, сопровождение программно-прикладного обеспечения и технических средств;
- организации, оказывающие услуги в области защиты информации (проведение объектовых исследований, монтаж и настройка средств защиты информации, контроль эффективности системы защиты информации, аттестация объектов информатизации и т.п.);
- организации, осуществляющие поставку товаров для обеспечения повседневной деятельности (канцтоваров, оргтехники, расходных материалов, мебели и т.п.);

– организации и частные лица, оказывающие юридические услуги, услуги по информационно-техническому обеспечению, осуществляющие преподавательскую деятельность и т.п.

Порядок доступа к информационным ресурсам Администрации определяется в договоре на выполнение работ (оказание услуг).

Решением о предоставлении/не предоставлении доступа является подписанный в установленном порядке «Договор на выполнение работ или оказание услуг».

2.4 Перечень субъектов доступа

Субъектами, права доступа которых рассматриваются при работе в ИСПДн являются:

– администратор безопасности с правами полного доступа к техническим и программным средствам ИСПДн;
– пользователь ИСПДн, обрабатывающий ПДн в ИСПДн;
– процессы, выполняемые на АРМ от имени администратора безопасности;
– процессы, выполняемые на АРМ от имени пользователя.

Для работы в ИСПДн предусмотрены учетные записи с правами администратора или пользователя:

– Учетная запись администратора.
– Учетная запись пользователя, обрабатывающего ПДн в ИСПДн.

Вход в систему осуществляется с помощью персонального имени (логин) и пароля условно-постоянного действия.

2.5 Перечень объектов доступа.

Объектами доступа являются:

– ПЭВМ в целом;
– принтер;
– многофункциональное устройство;
– USB-порты;
– USB-накопители с защищаемой информацией;
– устройства чтения/записи оптических дисков;
– оптические диски с защищаемой информацией;
– НЖМД рабочих станций с защищаемой информацией;
– монитор с отображаемой на нем защищаемой информацией;
– оперативная память ПЭВМ;
– операционные системы (ОС) ПЭВМ;
– программы, предназначенные для разработки и печати документов, содержащих персональные данные;

– программные средства, осуществляющие функции по защите информации на ПЭВМ, а также функции контроля безопасности;
– бумажный носитель информации, на который/с которого выводится защищаемая информация.

2.6 Разрешительная система доступа

Присвоение конкретным пользователям прав доступа, а также закрепление за ними конкретных рабочих папок, директорий и файлов с обрабатываемой информацией в ИСПДн осуществляется по согласования с ответственным за обработку ПДн.

Права доступа различных пользователей к техническим и программным средствам и информационным ресурсам ИСПДн указаны в приложении 1.

2.7 Доступ к информационным ресурсам ИСПДн Администрации сторонних организаций, деятельность которых регламентируется законодательством Российской Федерации

Доступ (предоставление) сторонних организаций к информационным ресурсам организации регламентируется федеральными законами, приказами и распоряжениями министерств и служб, законодательно наделенных полномочиями на получение информации, а также настоящим Положением.

Доступ к информационным ресурсам организации сторонних организаций осуществляется на основании:

– письменных запросов;
– письменных соглашений (договоров) сторон об обмене информацией.

В письменном запросе (договоре) указывается:

– для каких целей необходима информация;
– ее конкретное наименование;
– способ доступа (предоставления).

Основанием для доступа (предоставления) к информации служит руководства на соответствующем документе.

При наличии официального соглашения со сторонней организацией о допуске (предоставлении) к информации доступ к ней осуществляется в порядке, указанном в подписанном соглашении (договоре).

Запрещается передача электронных копий баз данных любым сторонним организациям.

2.8 Доступ к информационным ресурсам ИСПДн Администрации сторонних организаций, выполняющих работы на договорной основе

Доступ к информационным ресурсам Администрации сторонних организаций, выполняющих работы на договорной основе, осуществляется на

основании подписанного договора на оказание услуг, а также настоящего Положения.

Дополнительно к договору на оказание услуг между Администрацией и сторонней организацией заключается соглашение о конфиденциальности и неразглашении сведений, содержащих персональные данные (и/или составляющих коммерческую тайну). В рамках данного соглашения, работники сторонней организации обязаны хранить в тайне сведения, содержащие персональные данные, а также служебную информацию, ставшие известными в ходе выполнения работ, если для их выполнения предусмотрено использование таких сведений.

3 Правила разграничения доступа

Каждому пользователю присваивается персональный идентификатор и пароль для входа в систему.

Разработка, редактирование защищаемых документов производится с применением установленного на рабочей станции программного обеспечения.

Правила работы пользователей ИСПДн регламентируются соответствующей «Инструкцией пользователя информационных систем персональных данных Администрации ЗАТО г. Железногорск», администратора безопасности «Инструкцией администратора безопасности информационных систем персональных данных Администрации ЗАТО г. Железногорск», ответственного за обработку ПДн - «Инструкцией ответственного за обработку персональных данных в информационных системах персональных данных Администрации ЗАТО г. Железногорск».

Контроль функционирования разрешительной системы допуска к информационным ресурсам организуется в соответствии с:

- планом основных мероприятий по защите информации на текущий год;
- функциональными обязанностями должностных лиц;
- распоряжениями руководства.

Контроль функционирования разрешительной системы допуска к информационным ресурсам осуществляется ответственными лицами. Организация контроля возлагается на администратора безопасности ИСПДн.

Права доступа различных пользователей к техническим и программным средствам и информационным ресурсам ИСПДн

Матрица доступа

Категория пользователя	Доступные ресурсы	Права доступа
Администратор безопасности	1. Средства ОС, необходимые для запуска и работы ПЭВМ	Полный доступ
	2. Основные конфигурационные файлы ОС	Полный доступ
	3. Средства настройки и управления СЗИ; Журналы работы пользователей	Полный доступ
	4. Разрабатываемые документы	Нет доступа (Доступ к рабочим папкам пользователей ограничен организационными мерами)
	5. Средства разработки документов	Полный доступ
	6. Внешние устройства: Принтер, МФУ	Полный доступ
Пользователь	1. Средства ОС, необходимые для запуска и работы ПЭВМ	Чтение, исполнение
	2. Основные конфигурационные файлы ОС	Нет доступа
	3. Средства настройки и управления СЗИ; Журналы работы пользователей	Нет доступа
	4. Разрабатываемые документы	Полный доступ
	5. Средства разработки документов	Полный доступ
	6. Внешние устройства: Принтер, МФУ	Печать, копирование, сканирование