Приложение 1

к приказу комитета

от 16.01.2023 № 200/151/ПР-41

ПОЛОЖЕНИЕ

о разрешительной системе допуска к информационным системам персональных данных комитета жилищно-коммунального хозяйства города Барнаула

1. Перечень используемых определений, обозначений и сокращений

АИБ – администратор информационной безопасности.

АРМ – автоматизированное рабочее место.

ИБ – информационная безопасности.

ИС – информационная система.

ИСПДн – информационная система персональных данных.

комитет – комитет жилищно-коммунального хозяйства города Барнаула

2. Общие положения

* 1. Настоящее Положение разработано в соответствии с Конституцией Российской Федерации, Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных», постановлениями Правительства Российской Федерации от 15.09.2008 №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и другими нормативными документами.
  2. Разрешительная система допуска к ИСПДн комитета представляет собой совокупность процедур оформления права субъектов на доступ к информационным ресурсам (объекты доступа) организации, содержащим персональные данные, и ответственных лиц, осуществляющих реализацию этих процедур.
  3. Объектами доступа являются:

документированная информация на бумажных носителях в виде отдельных документов или дел;

информационные ресурсы в информационной системе в виде баз данных, библиотек, архивов и их копий на машинных носителях.

Субъектами доступа являются:

работники комитета;

юридические и физические лица.

* 1. Субъекты доступа несут персональную ответственность за соблюдение ими установленного в комитете порядка обеспечения защиты информационных ресурсов.
  2. Ответственными лицами комитета, осуществляющими реализацию процедур оформления прав субъектов на доступ к информационным ресурсам, являются:

председатель;

заместители председателя;

начальники отделов;

администратор ИСПДн, ИБ;

ответственный за обработку персональных данных;

ответственный за обеспечение безопасности персональных данных (администратор безопасности).

3. Порядок формирования информационных ресурсов организации

* 1. Формирование информационных ресурсов на бумажных носителях осуществляется в структурных подразделениях и регламентируется внутренними документами комитета.
  2. Информационные ресурсы, формируемые в ИС подразделяются на:

сетевые ресурсы с доступом одной группы пользователей (ресурсы отдела);

сетевые ресурсы с доступом нескольких групп пользователей (базы данных и т.п.);

ресурсы общего пользования (справочно-информационные системы, библиотеки, каталоги и т.п.);

сетевой ресурс почтового обмена;

сетевые принтеры;

ресурсы пользователя (сетевые или локальные).

* 1. Информационные ресурсы, содержащие персональные данные, указываются в «Перечне защищаемых информационных ресурсов».
  2. Решение о формировании новых информационных ресурсов принимает начальник отдела, инициирующего это решение. В заявке на формирование обосновывается необходимость создания новых информационных ресурсов и указывается, в интересах каких групп пользователей они создаются.
  3. Непосредственное формирование нового сетевого информационного ресурса осуществляется администратором ИСПДн. На исполненной заявке администратор ИСПДн, проставляет отметку о создании и местонахождении ресурса.
  4. На основании исполненной заявки вносятся изменения и дополнения в «Матрицу разграничения доступа» и «Перечень защищаемых информационных ресурсов».

4. Допуск к информационным ресурсам работников организации

* 1. Допуск работников к информации, содержащей персональные данные, осуществляется в соответствии с занимаемой должностью и в объеме, необходимом для выполнения ими должностных обязанностей.
  2. Допуск к персональным данным разрешается руководителем, только уполномоченным лицам с соблюдением требований «Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».
  3. Допуск работника к информационным ресурсам ИСПДн, оформляется заявкой администратору ИСПДн, которая предоставляется начальником соответствующего отдела после согласования с председателем. В заявке указывается, к каким ресурсам и с какими правами (полномочиями) допустить конкретного работника.
  4. Заявку подписывает председатель комитета, подтверждающий, что указанный сотрудник действительно принят в штат комитета.

Заявка согласуется с АИБом и передается в комитет.

Комитет рассматривает представленную заявку и совершает необходимые операции по созданию учетной записи пользователя, присвоению ему начального значения пароля и прав доступа к ресурсам комитета в соответствии с «Матрицей доступа».

По окончании регистрации учетной записи пользователя в заявке делается отметка о выполнении задания за подписями исполнителей.

Минимальные права в ИС комитета, определенные выше, а также присвоение начального пароля производится АИБом, при согласовании заявки на предоставление (изменение) прав доступа пользователя к ИР.

Процедура предоставления (или изменения) прав доступа пользователя к ресурсам комитета инициируется заявкой руководителя структурного подразделения сотрудника.

Заявка согласуется с АИБом и передается комитету.

По окончании внесения изменений в заявке делается отметка о выполнении задания за подписями исполнителей.

* 1. При наступлении момента прекращения срока действия полномочий пользователя (окончание договорных отношений, увольнение сотрудника) учетная запись должна немедленно блокироваться.

Допускается регистрация постоянных учетных записей при отсутствии механизмов автоматической блокировки. В этом случае отдел, ответственный за кадровое обеспечение обязан своевременно подавать заявки на блокирование учетной записи сотрудника не позднее, чем за сутки до момента прекращения срока действия полномочий пользователя.

Заявку подписывает председатель комитета, утверждая тем самым факт прекращения срока действия полномочий пользователя.

АИБ рассматривает представленную заявку и передает заявку на исполнение комитету.

По окончании внесения изменений в заявке делается отметка о выполнении задания за подписями исполнителей.

* 1. Исполненные заявки передаются АИБу, и хранятся в архиве в течение 5 лет с момента окончания предоставления доступа к ИС комитета.

Копии исполненных заявок хранятся у системного администратора.

В случае невозможности исполнения заявки инициатору заявки направляется мотивированный отказ с приложением заявки.

* 1. Администратором безопасности (или ответственным лицом) проверяется соответствие требуемых прав доступа с реально необходимыми для выполнения должностных (функциональных) обязанностей данного работника.
  2. Согласованная заявка является разрешением на допуск и основанием для регистрации пользователя в сети администратором ИСПДн.

5. Допуск к информационным ресурсам сторонних организаций, деятельность которых не связана с исполнением функций организации

* 1. К организациям, деятельность которых не связана с исполнением функций организации, могут относиться:

правоохранительные органы;

судебные органы;

органы статистики;

органы исполнительной и законодательной власти субъектов Российской Федерации;

средства массовой информации и пр.

* 1. Допуск к информационным ресурсам сторонних организаций, деятельность которых не связана с исполнением функций организации, регламентируется законодательством Российской Федерации, договорами и соглашениями об информационном обмене и другими нормативными актами.

6. Допуск к информационным ресурсам организации сторонних организаций, выполняющих работы в организации на договорной основе

* 1. 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 технических средств ИСПДн, сопровождение программно-прикладного обеспечения;

организации, оказывающие услуги в области защиты информации (проведение специальных проверок и 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 (мебели, канцтоваров, оргтехники, расходных материалов и т.п.);

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

* 1. Порядок допуска определяется в договоре на выполнение работ (оказание услуг), в соответствии с «Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».
  2. Решением о допуске является подписанный в установленном порядке договор на выполнение работ или оказание услуг.
  3. В договор на оказание услуг включается условие о неразглашении сведений, составляющих персональные данные, а также служебной информации, ставшей известной в ходе выполнения работ, если для их выполнения предусмотрено использование таких сведений. Со всех работников сторонней организации, участвующих в выполнении работ, в этом случае берется подписка о неразглашении таких сведений.

7. Доступ к информационным ресурсам организации

* 1. Правила и процедуры доступа к информационным ресурсам комитета определяются «Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» и «Положением о разрешительной системе допуска».
  2. Администрирование прав доступа к информации в ИСПДн, производится администратором ИСПДн.
  3. После регистрации пользователя в ИСПДн, администратор безопасности вносит изменения в «Матрицу разграничения доступа» для последующего контроля прав и полномочий пользователя.

1. Контроль функционирования разрешительной системы допуска

к информационным ресурсам организации

* 1. 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;

приказами руководителя.

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

Председатель комитета Д.А. Ращепкин