Приложение 4

к приказу комитета

от 27.03.2015 №42р

Описание технологического процесса обработки информации в информационных системах.

1. ‍Перечень используемых определений, обозначений и сокращений

* АИБ – администратор информационной безопасности.
* АРМ – автоматизированное рабочее место.
* ИС – информационная система.
* ИСПДн – информационная система персональных данных.

1. ‍Общие положения
   1. ‍Настоящее Положение разработано в соответствии с Конституцией Российской Федерации, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», .
   2. ‍Разрешительная система допуска к ИСПДн Комитета по земельным ресурсам и землеустройству города Барнаула (далее – Комитет по земельным ресурсам и землеустройству города Барнаула) представляет собой совокупность процедур оформления права субъектов на доступ к информационным ресурсам (объекты доступа) организации, содержащим ПДн, и ответственных лиц, осуществляющих реализацию этих процедур.
   3. ‍Объектами доступа являются:
      1. ‍документированная информация на бумажных носителях в виде отдельных документов или дел;
      2. ‍информационные ресурсы в ИС в виде баз данных, библиотек, архивов и их копий на машинных носителях.
   4. ‍Субъектами доступа являются:
      1. ‍работники Комитета;
      2. ‍юридические и физические лица.
   5. ‍Субъекты доступа несут персональную ответственность за соблюдение ими установленного в Комитете порядка обеспечения защиты информационных ресурсов.
   6. ‍Ответственными лицами Комитета, осуществляющими реализацию процедур оформления прав субъектов на доступ к информационным ресурсам, являются:
      1. ‍руководитель;
      2. ‍заместители руководителя;
      3. ‍начальники отделов;
      4. ‍администратор ИС, АИБ;
      5. ‍ответственный за обработку персональных данных.
2. ‍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:
      1. ‍сетевые ресурсы с доступом одной группы пользователей (ресурсы отдела);
      2. ‍сетевые ресурсы с доступом нескольких групп пользователей (базы данных и т. п.);
      3. ‍ресурсы общего пользования (справочно-информационные системы, библиотеки, каталоги и т. п.);
      4. ‍сетевой ресурс почтового обмена;
      5. ‍сетевые принтеры;
      6. ‍ресурсы пользователя (сетевые или локальные).
   3. ‍Информационные ресурсы, содержащие персональные данные, указываются в «Перечне защищаемых информационных ресурсов».
   4. ‍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.
   5. ‍Непосредственное формирование нового сетевого информационного ресурса осуществляется администратором ИСПДн. На исполненной заявке администратор ИСПДн, проставляет отметку о создании и местонахождении ресурса.
   6. ‍На основании исполненной заявки вносятся изменения и дополнения в «Матрицу разграничения доступа» и «Перечень защищаемых информационных ресурсов».
3. ‍Допуск к информационным ресурсам работников организации
   1. ‍Допуск работников к информации, содержащей ПДн, осуществляется в соответствии с занимаемой должностью и в объеме, необходимом для выполнения ими должностных обязанностей.
   2. ‍Допуск к ПДн, разрешается руководителем, только уполномоченным лицам с соблюдением требований «Положения об обеспечении безопасности ПДн, при их обработке в информационных системах персональных данных».
   3. ‍Допуск работника к информационным ресурсам ИСПДн, оформляется заявкой администратору ИС, которая предоставляется начальником соответствующего отдела после согласования с руководителем. В заявке указывается, к каким ресурсам и с какими правами (полномочиями) допустить конкретного работника.
   * Заявку подписывает Ведущий специалист по кадровым вопросам Бухгалтерии, Бухгалтерии подтверждающий, что указанный сотрудник действительно принят в штат Комитета.
   * Заявка согласуется с АИБом и передается Отделу АСУ.
   * Отдел АСУ, Отдел АСУ 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.
   1. ‍Процедура предоставления (или изменения) прав доступа пользователя к ресурсам Комитета инициируется заявкой руководителя структурного подразделения сотрудника.
   * Заявка согласуется с АИБом и передается Отделу АСУ на исполнение.
   * 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 Ведущий специалист по кадровым вопросам Бухгалтерии, Бухгалтерии обязан своевременно подавать заявки на блокирование учетной записи сотрудника не позднее, чем за сутки до момента прекращения срока действия полномочий пользователя.
   * Заявку подписывает Ведущий специалист по кадровым вопросам Бухгалтерии, Бухгалтерии, утверждая тем самым факт прекращения срока действия полномочий пользователя.
   * АИБ рассматривает представленную заявку и передает заявку на исполнение Отделу АСУ.
   * По окончании внесения изменений в заявке делается отметка о выполнении задания за подписями исполнителей.
   * В случае необходимости сохранения персональных документов (профайла пользователя) на АРМ сотрудника, после прекращения срока действия его полномочий, сотрудник (или его непосредственный руководитель) должен своевременно (не позднее, чем за 3 суток до момента прекращения срока действия своих полномочий) подать заявку на блокирование учетной записи пользователя с указанием срока хранения указанной информации. Заявка должна подаваться даже в случае применения механизмов автоматической блокировки учетных записей уволенных сотрудников.
   * Такая заявка должна быть предварительно согласована с АИБом, и после выполнения действий по блокированию учетной записи передается Отделу АСУ для исполнения требования по сохранению данных.
   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 инициатору заявки направляется мотивированный отказ с приложением Заявки.
   1. ‍АИБом 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 ИС.
4. ‍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:
      1. ‍правоохранительные органы;
      2. ‍судебные органы;
      3. ‍органы статистики;
      4. ‍органы исполнительной и законодательной власти субъектов Российской Федерации;
      5. ‍средства массовой информации и пр.
   2. ‍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.
5. ‍Допуск к информационным ресурсам организации сторонних организаций, выполняющих работы в организации на договорной основе
   1. ‍К организациям, выполняющим работы на договорной основе, могут относиться:
      1. ‍организации, выполняющие строительные работы и осуществляющие ремонт зданий, систем инженерно-технического обеспечения (отопления, освещения, водоснабжения, канализации, электропитания, кондиционирования и т. п.);
      2. ‍организации, осуществляющие монтаж и настройку технических средств ИСПДн, сопровождение программно-прикладного обеспечения;
      3. ‍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.);
      4. ‍организации, осуществляющие поставку товаров для обеспечения повседневной деятельности (мебели, канцтоваров, оргтехники, расходных материалов и т. п.);
      5. ‍организации и частные лица, оказывающие юридические услуги, услуги по информационно-техническому обеспечению, осуществляющие преподавательскую деятельность и т. п.
   2. ‍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».
   3. ‍Решением о допуске является подписанный в установленном порядке договор на выполнение работ или оказание услуг.
   4. ‍В договор на оказание услуг включается условие о неразглашении сведений, составляющих персональные данные, сведений составляющих врачебную тайну, 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.
6. ‍Доступ к информационным ресурсам организации
   1. ‍Правила и процедуры доступа к информационным ресурсам 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 ИС.
   3. ‍После регистрации пользователя в ИСПДн, АИБ вносит изменения в «Матрицу разграничения доступа» для последующего контроля прав и полномочий пользователя.
7. ‍Контроль функционирования разрешительной системы допуска к информационным ресурсам организации
   1. ‍Контроль функционирования разрешительной системы допуска к информационным ресурсам организуется в соответствии с:
      1. ‍планом основных мероприятий по защите информации на текущий год;
      2. ‍функциональными обязанностями должностных лиц;
      3. ‍приказами руководителя.
   2. ‍Контроль функционирования разрешительной системы допуска к информационным ресурсам осуществляется ответственными лицами. Организация контроля возлагается на АИБа.