Приложение №1
к приказу № 100 от 30.04.2014г.

Положение о защите персональных данных при их обработке в информационных системах ОАО "Автопарк №6 "Спецтранс"

Настоящий документ устанавливает требования к защите персональных данных при их обработке в информационных системах персональных данных (далее - информационные системы) и уровни защищенности таких данных, на основании: Федерального закона №152-ФЗ от 27.07.2006 (ред. от 23.07.2013) "О персональных данных", постановления Правительства РФ от 1 ноября 2012 г. №1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных").

Безопасность персональных данных при их обработке в информационной системе обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы, определенные в Федеральном законе "О персональных данных".

Система защиты персональных данных включает в себя организационные и технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах. Выбор средств защиты информации для системы защиты персональных данных осуществляется соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю.

Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного доступа к персональным данным при их обработке и хранении в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных.

Положение является основой для:

- принятия управленческих решений и разработки практических мер по воплощению политики безопасности информации и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз безопасности информации;
- координации деятельности структурных подразделений организации при проведении работ по созданию, развитию и эксплуатации информационных систем с соблюдением требований обеспечения безопасности информации;
- разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности информации ОАО Автопарк №6 "Спецтранс"
- создания приказа о назначении ответственных сотрудников по направлениям.

Положение учитывает современное состояние технических средств и ближайшие перспективы развития ОАО Автопарк №6 "Спецтранс", цели, задачи и правовые основы ее создания и эксплуатации, режимы функционирования данной системы, а также результаты анализа угроз безопасности на основании проведенного аудита ООО"ИТБ" в ноябре-декабре 2013года.

Актуализация угроз и уровня защищенности персональных данных в ОАО Автопарк №6 "Спецтранс"

Согласно классификации угроз и уровня защищенности на предприятии возможны

угрозы 2-го типа - связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе. При этом возникает необходимость обеспечения 3-го уровня защищенности персональных данных при их обработке в информационной системе.

В соответствии с той же классификацией в этом случае для обеспечения 3-го уровня защищенности персональных данных необходимо выполнять следующие требования:

а) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) обеспечение сохранности носителей персональных данных;

в) утверждение документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;

г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности

д) назначение должностное лицо (лиц), ответственных за обеспечение безопасности персональных данных в информационных системах.

Необходимо принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, определить перечень и состав мероприятий:

1) издание, документов, определяющих политику работодателя в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

2) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных

3) осуществление внутреннего контроля и аудита соответствия обработки персональных данных, требованиям к защите персональных данных, в отношении обработки персональных данных;

4) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения закона, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей;

5) ознакомление работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и обучение указанных работников.

6) принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

Виды информации, подпадающие под настоящее Положение и относящиеся к персональным данным:

-фамилия, имя, отчество;

-пол, возраст;

-образование, квалификация, профессиональная подготовка и сведения о повышении квалификации;

-место жительства;

-семейное положение, наличие детей, родственные связи;

-факты биографии и предыдущая трудовая деятельность (место работы, размер заработка, судимость, служба в армии, работа на выборных должностях, на государственной службе и др.);

-финансовые (доходы, долги, номера банковских карт, владение недвижимым имуществом, денежные вклады и др.);

-деловые и иные личные качества, которые носят оценочный характер;

-прочие сведения, которые могут идентифицировать человека.

Из указанного списка работодатель вправе получать и использовать только те сведения, которые характеризуют гражданина как сторону трудового договора.

Персональные сведения могут содержаться в следующих документах:

- анкета, автобиография, личный листок по учету кадров, которые заполняются работником при приеме на работу. В этих документах содержатся анкетные и биографические данные работника;

- копия документа, удостоверяющего личность работника. Здесь указываются фамилия, имя, отчество, дата рождения, адрес регистрации, семейное положение, состав семьи работника, а также реквизиты этого документа;

- личная карточка N Т-2. В ней указываются фамилия, имя, отчество работника, место его рождения, состав семьи, образование, а также данные документа, удостоверяющего личность, и пр.;

- трудовая книжка или ее копия. Содержит сведения о трудовом стаже, предыдущих местах работы;

- копии свидетельств о заключении брака, рождении детей. Такие документы содержат сведения о составе семьи, которые могут понадобиться работодателю для предоставления работнику определенных льгот, предусмотренных трудовым и налоговым законодательством;

- документы воинского учета. Содержат информацию об отношении работника к воинской обязанности и необходимы работодателю для осуществления в организации воинского учета работников;

- справка о доходах с предыдущего места работы. Нужна работодателю для предоставления работнику определенных льгот и компенсаций в соответствии с налоговым законодательством;

- документы об образовании. Подтверждают квалификацию работника, обосновывают занятие определенной должности;

- документы обязательного пенсионного страхования. Нужны работодателю для уплаты за работника соответствующих взносов;

- трудовой договор. В нем содержатся сведения о должности работника, заработной плате, месте работы, рабочем месте, а также иные персональные данные работника;

- подлинники и копии приказов по личному составу. В них содержится информация о приеме, переводе, увольнении и иных событиях, относящихся к трудовой деятельности работника;

- при необходимости - иные документы, содержащие персональные данные работников.

Открытая информация:

буклеты, общедоступная информация на web-сайте www.sp6.ru, учредительные документы, устав, типовая стоимость услуг, контактные данные менеджеров кампании.

Запрещено требовать с работников и вносить в информационные системы:

1. Специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни,

2. Сведений, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных

3. Обработка персональных данных в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи, а также в целях политической агитации допускается только при условии предварительного согласия субъекта персональных данных.

Меры по формированию режима информационной безопасности в Автопарке №6 «Спецтранс» делятся на три уровня:

1.Программно-технический - комплекс конкретных мероприятий, по хранению и обработке данных в информационных системах,

2. Организационный (административный) - действия общего характера, предпринимаемые руководством организации;

3.Процедурный - конкретные меры безопасности, имеющие дело с людьми, организация обработки (ввода) данных;

Программно-техническое обеспечение безопасности персональных данных в информационных системах

1) Определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

2) Применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

3) Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4) Назначение администраторов серверов, системных программистов, специалистов по обслуживанию технических средств вычислительной техники;

5) Оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

6) Обнаружение фактов несанкционированного доступа к персональным данным и принятием мер;

7) Восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

8) Разработка системы авторизации пользователей для доступа к информации, правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

9) Контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

10) Определение периодичности и способа проведения внешнего аудита информационных систем Автопарка в составе: сбор информации, анализ данных аудита, выработку рекомендаций, подготовку аудиторского отчета. Рекомендации аудитора должны быть конкретными и применимыми к данной ИС, экономически обоснованными, аргументированными (подкрепленными результатами анализа) и отсортированными по степени важности. При этом мероприятия по обеспечению защиты организационного уровня имеют приоритет над конкретными программно—техническими методами защиты.

Организационные (административные) мероприятия:

1) Организация режима обеспечения безопасности помещений, в которых размещены модули информационной системы, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в них;
2) Оценка эффективности принимаемых мер по обеспечению безопасности;
3) Обнаружение фактов несанкционированного физического доступа посторонних лиц к вычислительным ресурсам на территории Автопарка и принятие мер;
4) Контроль за сотрудниками по хранению логинов/паролей от информационных систем.
5) Анализ эффективности системы контроля управлением доступом на территорию Автопарка, соблюдение правил пропускного режима.
6) Еженедельное проведение контроля режима работы систем видеонаблюдения в административном здании и на удаленных объектах (МПК, АЗС, территория Автопарка)
7) Регулярное проведение инструктажа с руководителями подразделения пользующихся и допущенных к информационным носителям с целью недопущения утечки информации (с записью в соответствующем журнале).

Процедурные мероприятия, организация обработки (ввода) данных.

1) Осуществление внутреннего контроля за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
2) Назначение ответственных за ведение баз данных (ввод, корректировка, удаление данных в БД);
3) Доведение до сведения работников (операторов) положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
3) Организовать прием и обработку обращений и запросов субъектов персональных данных или их представителей и осуществлять контроль за приемом и обработкой таких обращений и запросов.

Обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью. Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:
1) Фамилию, имя, отчество, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
2) Цель обработки персональных данных;
3) Перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
4) наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных
5) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
6) срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;
7) подпись субъекта персональных данных.

Оператор обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные.

СОГЛАСИЕ
НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

Я, _____,
(ФИО)

паспорт _____ выдан _____,
(серия, номер) (когда и кем выдан)

_____

адрес регистрации: _____,

_____

даю свое согласие на обработку в ___**АО «Автопарк №6 «Спецтранс»**_____
(наименование организации)

моих персональных данных, относящихся исключительно к перечисленным ниже категориям персональных данных:

- фамилия, имя, отчество; дата рождения; место рождения; пол; гражданство; знание иностранного языка; образование и повышение квалификации или наличие специальных знаний; профессия (специальность);

- общий трудовой стаж, сведения о приемах, перемещениях и увольнениях по предыдущим местам работы, размер заработной платы; состояние в браке, состав семьи, место работы или учебы членов семьи и ближайших родственников;

- паспортные данные, адрес места жительства, дата регистрации по месту жительства; номер телефона; идентификационный номер; номер страхового свидетельства государственного пенсионного страхования; сведения, включенные в трудовую книжку; сведения о воинском учете; фотография;

- сведения о состоянии здоровья, которые относятся к вопросу о возможности выполнения работником трудовой функции.

Я проинформирован (–а), что ____**АО «Автопарк №6 «Спецтранс»**_____
(наименование организации)

гарантирует обработку моих персональных данных в соответствии с действующим законодательством Российской Федерации как неавтоматизированным, так и автоматизированным способами.

Данное согласие действует до достижения целей обработки персональных данных или в течение срока хранения информации.

Данное согласие может быть отозвано в любой момент по моему письменному заявлению.

Я подтверждаю, что, давая такое согласие, я действую по собственной воле и в своих интересах.

"__" _____ 201_ г. _____/_____/
Подпись Расшифровка подписи