

УТВЕРЖДАЮ

Генеральный директор

АО «ГЦБиТ»

В.И. Горн

« 05 » октября 2016 г.

Приложение №2 к Приказу от 05.10.2016 № 25

**ПОЛОЖЕНИЕ
об обработке и защите персональных данных в информационной системе персональных данных
АО «ГЦБиТ»**

Москва, 2016

1. Обозначения и сокращения

Положение – Положение об обработке и защите персональных данных в информационной системе персональных данных АО «ГЦБиТ».

Общество – акционерное общество «Городской центр бронирования и туризма».

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

Субъект ПДн – физическое лицо, ПДн которого обрабатываются Обществом.

ИСПДн – информационная система персональных данных – совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств.

Ответственный за обработку ПДн – лицо, ответственное за организацию обработки ПДн, назначаемое приказом генерального директора Общества.

Ответственный за безопасность ПДн – лицо, ответственное за обеспечение безопасности ПДн, назначаемое приказом генерального директора Общества.

2. Общие положения

Целью Положения об обработке и защите персональных данных в информационной системе персональных данных АО «ГЦБиТ» (далее – Положение) является обеспечение защиты персональных данных (далее – ПДн) при обработке их ПДн в информационной системе персональных данных (далее – ИСПДн) акционерном обществе «Городской центр бронирования и туризма» (далее – Общество).

Обеспечение защиты ПДн, обрабатываемых в ИСПДн, достигается посредством внедрения технических и организационных мер.

Настоящее Положение разработано в соответствии с требованиями следующих нормативно-правовых актов:

- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – ФЗ «О персональных данных»);
- Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК России от 18 февраля 2013 г. N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

Настоящее Положение, а также все дополнения и изменения к нему утверждаются генеральным директором Общества и вступают в силу с момента утверждения.

3. Политика Общества в отношении обработки персональных данных

Общество обрабатывает ПДн, полученные непосредственно от самих субъектов ПДн или работодателей субъектов ПДн. Обработка ПДн осуществляется Обществом с согласия субъекта ПДн.

Состав ПДн, обрабатываемых в ИСПДн, определяется Перечнем защищаемых информационных ресурсов информационной системы персональных данных АО «ГЦБиТ», утверждаемым генеральным директором.

Целью обработки ПДн в ИСПДн являются осуществление коммерческой деятельности Общества – бронирование, оформление авиа и железнодорожных билетов, оказание услуг визовой поддержки, оказание услуг внутреннего, международного туризма (въездного / выездного), оказание услуг по организации мероприятий, организации проживания в гостиницах, предоставление услуг страхования.

4. Организационные меры обеспечения защиты персональных данных

Для обеспечения защиты ПДн, обрабатываемых в ИСПДн, принимаются следующие организационные меры:

- определение актуальных угроз безопасности ПДн
- назначение лиц, ответственных за обеспечение безопасности ПДн при их обработке в ИСПДн;

- учет лиц, допущенных к работе с ПДн;
- ограничение доступа пользователей в помещения, где размещены технические средства ИСПДн, позволяющие осуществлять обработку конфиденциальной информации;
- разграничение доступа пользователей ИСПДн к информационным ресурсам, программным средствам обработки (передачи) и защиты конфиденциальной информации;
- разработка и поддержание актуальности комплекта внутренних нормативных документов.

Разработку и поддержание в актуальном состоянии Модели угроз безопасности персональных данных при их обработке в информационной системе персональных данных АО «ГЦБиТ» (далее – Модель угроз) осуществляет Ответственный за безопасность ПДн. Модель угроз утверждается генеральным директором Общества.

Модель угроз должна отражать актуальные угрозы безопасности ПДн и актуальное состояние защищенности ИСПДн Общества.

5. Технические меры обеспечения защиты персональных данных

Для защиты ПДн, обрабатываемых в ИСПДн, в Обществе внедряются и поддерживаются в актуальном состоянии средства защиты информации (далее - СрЗИ).

Администратор безопасности ИСПДн обеспечивает функционирование СрЗИ в штатном режиме.

Применение СрЗИ ПДн, обрабатываемых в ИСПДн, осуществляется в соответствии с Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», 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», методическими документами ФСТЭК России, а также Моделью угроз.

Защита ПДн должна обеспечиваться на всех технологических этапах обработки ПДн в ИСПДн, в том числе при проведении ремонтных и регламентных работ. При этом применение СрЗИ не должно ухудшать основные функциональные характеристики ИСПДн.

СрЗИ в Обществе должны реализовывать следующие меры:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- защита машинных носителей персональных данных;
- регистрация событий безопасности;
- антивирусная защита;
- контроль (анализ) защищенности ПДн;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных;
- управление конфигурацией информационной системы и системы защиты ПДн.

СрЗИ должны функционировать в круглосуточном режиме.

В Обществе должно обеспечиваться резервирование элементов СрЗИ и восстановление при нарушениях работоспособности.

Технические и программные СрЗИ должны удовлетворять требованиям законодательства Российской Федерации.

Общество вправе поручить на основании договора деятельность по технической защите информации, в том числе внедрению СЗИ, компаниям, имеющим соответствующие лицензии ФСТЭК России.

6. Порядок допуска и доступа к персональным данным

Допуск сотрудников Общества к работе с ПДн, обрабатываемыми в ИСПДн, осуществляется с письменного согласия руководителей структурных подразделений.

Сотрудник, получивший допуск к работе с ПДн, должен подписать Обязательство о неразглашении ПДн.

Каждый сотрудник имеет индивидуальную учетную запись, которая определяет его права и полномочия в ИСПДн.

Прекращение прав работы с ПДн, обрабатываемыми в ИСПДн, осуществляется на основании приказа об увольнении работника, либо о переводе его на работу, не подразумевающую обработку ПДн.

Созданием, удалением и изменением учетных записей сотрудников, допущенных к работе с ПДн в ИСПДн, занимаются уполномоченные администраторы в соответствии с должностными обязанностями.

Доступ в помещения обработки ПДн контролируется при помощи пропускного и внутриобъектового режимов, в том числе системы контроля управления доступом, физической охраны и системы охранно-пожарной сигнализации.

Запрещается нахождение посторонних лиц в помещениях обработки ПДн без сопровождения сотрудников Общества и служебной необходимости.

7. Ответственность

Сотрудники, виновные в нарушении норм, регулирующих обработку и защиту ПДн, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

До начала самостоятельной работы с ПДн в Обществе сотрудники должны быть ознакомлены с настоящим Положением. Контроль ознакомления осуществляет лицо, ответственное за обработку ПДн в Обществе.