


УТВЕРЖДЕНО:

Директор Общества
с ограниченной ответственностью
«ДЕПАРТАМЕНТ ОХРАНЫ»

Приложение №4 к приказу
№ 002-ПД от 01.10.2006г.



И.П.Какаулин

01.10.2006г.



ПОЛОЖЕНИЕ
«ОБ ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ
ПЕРСОНАЛЬНЫХ ДАННЫХ»

г. Томск, 2006 г.

СОДЕРЖАНИЕ

1. Термины и сокращения	3
2. Область применения	4
3. Общие положения	4
4. Организация работ по обеспечению безопасности персональных данных	4
5. Проведение работ по обеспечению безопасности персональных данных.....	6

1. ТЕРМИНЫ И СОКРАЩЕНИЯ

- **Персональные данные (ПД)** – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).
- **Оператор** – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.
- **Обработка персональных данных** – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.
- **Автоматизированная обработка персональных данных** - обработка персональных данных с помощью средств вычислительной техники.
- **Распространение персональных данных** – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.
- **Предоставление персональных данных** - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.
- **Блокирование персональных данных** – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).
- **Уничтожение персональных данных** – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.
- **Обезличивание персональных данных** – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.
- **Информационная система персональных данных (ИСПД)** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.
- **Трансграничная передача персональных данных** - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу. 2.1. Положение об обеспечении безопасности персональных данных (далее – Положение) разработано в целях выполнения требований законодательства Российской Федерации в области защиты персональных данных.
- **Средства защиты персональных данных (СЗПД)** - представляет собой совокупность организационных мер и технических средств защиты информации.

2. ОБЛАСТЬ ПРИМЕНЕНИЯ

2.2 Настоящее Положение определяет порядок и правила организации и проведения работ по обеспечению безопасности персональных данных в ООО «Департамент охраны» (далее – Оператор).

2.3 Настоящий документ учитывает положения основных нормативных правовых актов в области защиты персональных данных, перечисленных в Положении о комиссии по приведению в соответствие с требованиям законодательства в области персональных данных.

2.4 Настоящее Положение предназначено для всех работников Оператора, а также третьих лиц, получающих временный или постоянный доступ к обрабатываемым у него ПД на законном основании.

2.5 Настоящее Положение действует с момента его утверждения руководителем Оператора.

2.6 Актуализация настоящего Положения проводится не реже, чем два раза в год в соответствии с Регламентом по проведению контрольных мероприятий и реагированию на инциденты информационной безопасности в ООО «Департамент охраны».

2.7 Внесение изменений в настоящее Положение либо утверждение его новой редакции производится на основании соответствующего приказа руководителя Оператора.

3. ОБЩИЕ ПОЛОЖЕНИЯ

3.1 ПД, обрабатываемые у Оператора, цели, основание и сроки их обработки указаны в Перечне обрабатываемых персональных данных.

3.2 Обработка ПД осуществляется Оператором с использованием средств автоматизации и без их использования.

3.3 Сроки хранения ПД устанавливаются в письменном согласии субъекта ПД на обработку его персональных данных, а также требованиями законодательства Российской Федерации, устанавливающими сроки хранения документов.

4. ОРГАНИЗАЦИЯ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1 Под организацией работ по обеспечению безопасности ПД понимается формирование и всестороннее обеспечение реализации совокупности согласованных по цели, задачам, месту и времени организационных и технических мероприятий, направленных на минимизацию как непосредственного, так и опосредованного ущерба от реализации угроз безопасности ПД, и осуществляемых в целях:

4.2 Организация работ по обеспечению безопасности ПД у Оператора должна осуществляться в соответствии с действующими нормативными правовыми актами и разработанными для этих целей организационно-распорядительными документами по обеспечению безопасности ПД Оператором.

4.3 Задачи по приведению деятельности Оператора в соответствие с требованиями законодательства Российской Федерации в области ПД возлагаются на специально создаваемую для этих целей Комиссию и лиц, ответственных за организацию обработки и обеспечение безопасности ПД, которые могут быть включены в состав данной Комиссии.

4.4 В случаях, когда Оператор на основании договора поручает обработку ПД третьему лицу, Оператору необходимо заключить с данным лицом соглашение о соблюдении безопасности персональных данных, с возложением на третье лицо обязанности по обеспечению конфиденциальности и безопасности переданных Оператором ПД (либо включить данное обязательство в заключаемый/действующий договор).

4.5 Работы по приведению деятельности Оператора в соответствие с требованиями законодательства Российской Федерации ведутся по двум направлениям: обеспечение безопасности ПД, обрабатываемых без использования средств автоматизации, и обеспечение безопасности ПД в ИСПД Оператора.

4.6 Работы по обеспечению безопасности ПД, обрабатываемых без использования средств автоматизации, ведутся по следующим направлениям:

4.7 Организация и выполнение мероприятий по обеспечению безопасности ПД, обрабатываемых в ИСПД Оператора, осуществляются в рамках системы защиты персональных данных ИСПД (далее - СЗПД), развертываемой в ИСПД в процессе ее создания или модернизации.

- предотвращения возможных (потенциальных) угроз безопасности ПД;
- нейтрализации и/или парирования реализуемых угроз безопасности ПД;
- ликвидации последствий реализации угроз безопасности ПД.
- определение перечня лиц, допущенных к обработке ПД;
- определение помещений, в которых обрабатываются персональные данные;
- информирование работников Оператора об установленных правилах обработки ПД и требований по их защите, повышение осведомленности в вопросах обеспечения безопасности ПД;
- учет и защита носителей ПД;
- разграничение доступа к носителям ПД;
- уничтожение ПД.

4.8 СЗПД представляет собой совокупность организационных мер и технических средств защиты информации, а также используемых в ИСПД информационных технологий, функционирующих в соответствии с определенными целями и задачами обеспечения безопасности ПД.

4.9 СЗПД должна являться неотъемлемой составной частью каждой вновь создаваемой ИСПД Оператора.

4.10 Для существующих ИСПД, в которых в процессе их создания не были предусмотрены меры по обеспечению безопасности ПД должен быть проведен комплекс организационных и технических мероприятий по разработке и внедрению СЗПД.

4.11 Структура, состав и основные функции СЗПД определяются в соответствии с уровнем защищенности персональных данных, обрабатываемых в ИСПД и моделью угроз безопасности персональных данных при их обработке в ИСПД.

5. ПРОВЕДЕНИЕ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1 В целях оценки уровня защищенности обрабатываемых у Оператора ПД и своевременного устранения несоответствий требованиям законодательства РФ в области защиты ПД у Оператора раз в год должен проводиться анализ изменений процессов защиты ПД.

5.2 Анализ изменений проводится по следующим основным направлениям:

- перечень работников и третьих лиц, допущенных в обработку ПД, степень их участия в обработке ПД и характер взаимодействия между собой;
- перечень помещений, в которых обрабатываются персональные данные;
- перечень и объем обрабатываемых ПД;
- цели обработки ПД;
- процедуры сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления и уничтожения ПД;
- способы обработки ПД (автоматизированная, неавтоматизированная);
- перечень уполномоченных органов, в рамках отношений с которыми осуществляется обработка ПД;
- перечень программно-технических средств, используемых для обработки ПД;
- конфигурация и топология ИСПД в целом и ее отдельных компонент, физические, функциональные и технологические связи как внутри этих систем, так и с другими системами различного уровня и назначения;
- способы физического подключения и логического взаимодействия компонент ИСПД, способы подключения к сетям связи общего пользования и международного информационного обмена с определением пропускной способности линий связи;
- режимы обработки ПД в ИСПД в целом и в отдельных компонентах;
- состав используемого комплекса средств защиты ПД и механизмов идентификации, аутентификации и разграничения прав доступа пользователей ИСПД на уровне операционных систем, баз данных и прикладного программного обеспечения;
- перечень организационно-распорядительной документации, определяющей порядок обработки и защиты ПД у Оператора;
- физические меры защиты ПД, организация пропускного режима.

5.3. Результаты анализа изменений используются для оценки корректности требований по обеспечению безопасности ПД, обрабатываемых с использованием средств автоматизации и без использования таких средств и при необходимости их уточнения.

5.4 У Оператора должен вестись учет действий, совершаемых работниками Оператора при обработке ПД в ИСПД. Действия с ПД учитываются в log-файлах ИСПД и/или в отдельной базе данных ИСПД.

5.5 Доступ к ПД осуществляется в соответствии с Регламентом по допуску работников и третьих лиц к обработке персональных данных, утвержденным Оператором.

5.6 Лица, допущенные к обработке ПД, должны быть проинформированы:

- о допуске к обработке ПД путем ознакомления с Перечнем должностей и третьих лиц, имеющих доступ к персональным данным, обрабатываемым у Оператора;
- о категориях, обрабатываемых ПД путем ознакомления с утвержденным Перечнем обрабатываемых персональных данных;
- о правилах осуществления обработки ПД путем ознакомления под роспись с Положением об обработке персональных данных.

5.7. Неавтоматизированная обработка ПД должна осуществляться таким образом, чтобы в отношении каждой категории ПД можно было определить места хранения материальных носителей и установить перечень лиц, допущенных к обработке ПД. У Оператора должен вестись учет носителей ПД.

5.8 Фиксация ПД должна осуществляться на отдельных материальных носителях (отдельных документах). ПД должны отделяться от иной информации.

5.9 Фиксация на одном материальном носителе ПД, цели обработки которых заведомо несовместимы, не допускается. В случае если на одном материальном носителе все же зафиксированы ПД, цели обработки которых несовместимы, должны быть приняты меры по обеспечению отдельной обработки ПД, в частности:

- при необходимости использования или распространения определенных ПД осуществляется выборочное копирование ПД, подлежащих распространению или использованию, способом, исключающим одновременное копирование ПД, не подлежащих распространению и использованию, и используется (распространяется);
- при необходимости уничтожения или блокирования части ПД уничтожается или блокируется материальный носитель с предварительным выборочным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование ПД, подлежащих уничтожению или блокированию.

5.10. Правила учета, хранения и уничтожения ПД при неавтоматизированной обработке описаны в Регламенте по учёту, хранению и уничтожению носителей персональных данных, утвержденном Оператором.

5.11 Должен осуществляться мониторинг фактов несанкционированного доступа к персональным данным и приниматься соответствующие меры при их обнаружении. Мониторинг осуществляется Администратором безопасности ИСПД.

5.12 Администратором безопасности ИСПД должен осуществляться контроль за принимаемыми мерами по обеспечению безопасности персональных данных.

5.13 При обработке ПД Оператор должен иметь возможность и средства для восстановления ПД, в случае их модификации или уничтожении вследствие несанкционированного доступа к ним. Правила резервного копирования и восстановления ПД Оператором установлены в Регламенте по резервному копированию персональных данных, утвержденному Оператором.

5.14 Оператор определяет перечень помещений, используемых при обработке ПД. При этом организация режима безопасности, охрана этих помещений должны обеспечивать сохранность носителей ПД, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

5.15 Пользователи ИСПД должны обеспечивать сохранность съемных носителей, содержащих ПД. В случае утраты носителя пользователи должны немедленно сообщить об этом Администратору безопасности ИСПД.

5.16 Если при работе с ПД работнику Оператора необходимо покинуть рабочее место, материальные носители ПД должны быть защищены от неконтролируемого доступа к ним. Для этого материальные носители помещаются в отведенных для хранения места.

5.17 В случае достижения цели обработки ПД Оператор прекращает обработку ПД или обеспечивает ее прекращение (если обработка ПД осуществляется другим лицом, действующим по поручению Оператора) и уничтожает ПД или обеспечивает их уничтожение (если обработка ПД осуществляется другим лицом, действующим по поручению Оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки ПД, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПД. В случае

если ПД невозможно уничтожить, то они блокируются и уничтожаются в срок, не превышающий шести месяцев.

5.18 Проведение работ по созданию (модернизации) СЗПД включает следующие стадии:

5.19 На предпроектной стадии проводится определение уровня защищенности персональных данных, обрабатываемых в ИСПД, формируется Модель угроз безопасности ПД при их обработке в ИСПД, разрабатывается Техническое задание на СЗПД.

5.20 Определение уровня защищенности персональных данных, обрабатываемых в ИСПД, осуществляется в соответствии с Регламентом по определению уровня защищенности персональных данных, обрабатываемых в информационных системах персональных данных.

5.21 ИСПД Оператора указаны в Перечне информационных систем персональных данных.

5.22 Уровень защищенности персональных данных, обрабатываемых в ИСПД, оформляется соответствующим актом.

5.23 Модель угроз безопасности ПД при их обработке в ИСПД формируется на основании руководящих документов ФСТЭК России и ФСБ России.

5.24 Перечень актуальных угроз формируется для каждой ИСПД Оператора с учетом условий функционирования ИСПД и особенностей обработки ПД.

5.25 По итогам определения уровня защищенности персональных данных, обрабатываемых в ИСПД и результатам определения актуальных угроз безопасности ПД формируются требования по обеспечению безопасности ПД, обрабатываемых в ИСПД. Данные требования оформляются в виде технического задания на СЗПД.

5.26 Стадия проектирования СЗПД включает разработку СЗПД в составе ИСПД, а именно разработку разделов задания и проекта проведения по созданию (модернизации) СЗПД в соответствии с требованиями технического задания;

5.27 Стадия реализации СЗПД включает:

- предпроектная стадия;
- стадия проектирования;
- стадия реализации СЗПД;
- стадия ввода в действие СЗПД.
- закупку совокупности используемых в СЗПД сертифицированных технических, программных и программно-технических средств защиты информации и их установку;
- определение подразделений и назначение лиц, ответственных за эксплуатацию средств защиты информации с их обучением;
- разработку эксплуатационной документации на СЗПД и средства защиты информации.

5.28 На стадии ввода в действие СЗПД осуществляются:

- предварительные испытания средств защиты информации в комплексе с другими техническими и программными средствами;
- устранение несоответствий по итогам предварительных испытаний;
- опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПД;

- приемо-сдаточные испытания средств защиты информации по результатам опытной эксплуатации.

5.29 В процессе функционирования ИСПД может осуществляться модернизация СЗПД. В обязательном порядке модернизация проводится в случае, если:

- произошло изменение номенклатуры обрабатываемых ПД, влекущее за собой изменение уровня защищенности персональных данных, обрабатываемых в ИСПД;
 - произошло изменение номенклатуры и/или актуальности угроз безопасности ПД;
 - изменилась структура ИСПД или технические особенности ее построения (изменился состав или структура программного обеспечения, технических средств обработки ПД, топологии ИСПД и т.п.);
 - произошло изменение законодательства Российской Федерации в области ПД, затрагивающее вопросы обеспечения безопасности ПД при их обработке в ИСПД.
- 5.30. При возникновении условий, влияющих на безопасность ПД (компрометация паролей, нарушение целостности и доступности персональных данных и пр.) работник Оператора обязан незамедлительно проинформировать об этом Администратора безопасности ИСПД.

5.31 Лица, виновные в нарушении требований, предъявляемых законодательством РФ к защите ПД, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.