Приложение № 7
к пользовательскому соглашению

Положение по обеспечению безопасности персональных данных

1. ТЕРМИНЫ И СОКРАЩЕНИЯ

- Персональные данные (ПДн) – 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 (ИСПДн) – 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. ОБЛАСТЬ ПРИМЕНЕНИЯ

2.1 Положение об обеспечении безопасности персональных данных (далее – Положение) разработано в целях выполнения требований законодательства Российской Федерации в области защиты персональных данных.

2.2 Настоящее Положение определяет порядок и правила организации и проведения работ по обеспечению безопасности персональных данных.

2.3 Настоящий документ учитывает положения основных нормативных правовых актов в области защиты персональных данных, а именно:

- 5 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Постановления Правительства РФ от 17.11.2007 № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Постановления Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Приказа ФСТЭК РФ № 55, ФСБ РФ № 86, Мининформсвязи РФ № 20 от 13.02.2008 «Об утверждении Порядка проведения классификации информационных систем персональных данных»;
- Нормативных актов ФСТЭК России: «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденной Заместителем директора ФСТЭК России 15 февраля 2008 г.;
- «Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденной Заместителем директора ФСТЭК России 14 февраля 2008 г.;
- «Положения о методах и способах защиты информации в информационных системах персональных данных», утверждено приказом ФСТЭК России от 5 февраля 2010 г. № 58 (зарегистрированного в Минюсте РФ 19.02.2010 N 16456);

- Нормативных актов ФСБ России: «Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденных руководством 8 Центра ФСБ России 21 февраля 2008 г. № 1.49/6/6-622;
- «Методических рекомендаций по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», утвержденных руководством 8 Центра ФСБ России 21 февраля 2008 г. № 149/54-144.

2.4 Настоящее Положение предназначено для всех сотрудников сайта "Дом Мастера", а также лиц, получающих временный доступ к обрабатываемым в Компании ПДн на законном основании.
2.5 Настоящее Положение вступает в силу с момента его публикации на сайте "Дом Мастера" и действует до его замены новым Положением постоянно размещенным в публичном доступе на Сайте..

3. ОБЩИЕ ПОЛОЖЕНИЯ
3.1. Сайт "Дом Мастера" является оператором ПДн.
3.2. ПДн, обрабатываемые в Компании, цели и сроки их обработки указаны в Перечне персональных данных, обрабатываемых на Сайте.
3.3. В Компании обработка ПДн осуществляется с использованием средств автоматизации и без использования таких средств.
3.4. Сроки хранения ПДн определяются в соответствие со сроком действия договора с субъектом ПДн, 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 ПДн 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 ПДн, и осуществляемых в целях: предотвращения возможных (потенциальных) угроз безопасности ПДн; нейтрализации и/или парирования реализуемых угроз безопасности ПДн; ликвидации последствий реализации угроз безопасности ПДн.
4.2. В случаях, когда Дом Мастера на основании договора поручает обработку ПДн другому лицу/сторонней организации, необходимо выполнить одно из следующих условий: в тексте договора в требованиях к контрагенту прописать обязанность обеспечения контрагентом безопасности и конфиденциальности ПДн. В случае невозможности или

нецелесообразности изменения текста договора оформить дополнительное соглашение к договору или соглашение о конфиденциальности, в которых прописать обязанность обеспечения контрагентом конфиденциальности персональных данных и безопасности ПДн при их обработке.
4.3. СЗПДн представляет собой совокупность организационных мер и технических средств защиты информации, а также используемых в ИСПДн информационных технологий, функционирующих в соответствии с определенными целями и задачами обеспечения безопасности ПДн.
4.4. Система защиты ПДн должна являться неотъемлемой составной частью каждой вновь создаваемой ИСПДн.
4.5. Для существующих ИСПДн, в которых в процессе их создания не были предусмотрены меры по обеспечению безопасности ПДн должен быть проведен комплекс организационных и технических мероприятий по разработке и внедрению СЗПДн.
4.6. Структура, состав и основные функции СЗПДн определяются в соответствии с классом ИСПДн и моделью угроз безопасности персональных данных при их обработке в ИСПДн.

5. ПРОВЕДЕНИЕ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1 В целях оценки уровня защищенности обрабатываемых в ПДн и своевременного устранения несоответствий требованиям законодательства РФ в области защиты ПДн в Компании раз в год должен проводиться анализ изменений процессов защиты ПДн.
5.2 Анализ изменений проводится по следующим основным направлениям:

- перечень лиц (подразделений), участвующих в обработке ПДн, степень их участия в обработке ПДн и характер взаимодействия между собой;
- перечень и объем обрабатываемых ПДн; цели обработки ПДн;
- процедуры сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления и уничтожение ПДн;
- способы обработки ПДн (автоматизированная, неавтоматизированная);
- перечень сторонних организаций, в том числе государственных регулирующих органов, в рамках отношений с которыми осуществляется передача ПДн;
- перечень программно-технических средств, используемых для обработки ПДн;
- конфигурация и топология ИСПДн 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 ИСПДн, способы подключения к сетям связи общего

пользования и международного информационного обмена с определением пропускной способности линий связи;
- ❏ режимы обработки ПДн в ИСПДн в целом и в отдельных компонентах;
- ❏ состав используемого комплекса средств защиты ПДн и механизмов идентификации, аутентификации и разграничения прав доступа пользователей ИСПДн на уровне операционных систем, баз данных и прикладного программного обеспечения;
- ❏ перечень организационно-распорядительной документации, определяющей порядок обработки и защиты ПДн в Компании;
- ❏ физические меры защиты ПДн, организация пропускного режима.

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

5.4. На предпроектной стадии проводится классификация ИСПДн, формируется модель угроз безопасности ПДн при их обработке в ИСПДн, разрабатывается техническое задание на СЗПДн.

5.5. Классификация ИСПДн осуществляется в соответствии с положениями Приказа ФСТЭК РФ № 55, ФСБ РФ № 86, Мининформсвязи РФ № 20 от 13.02.2008 «Об утверждении Порядка проведения классификации информационных систем персональных данных».

5.6. В связи с тем, что в ИСПДн Компании помимо обеспечения конфиденциальности обрабатываемых ПДн требуется обеспечить целостность и доступность ПДн, ИСПДн являются специальными информационными системами.

5.7. Модель угроз безопасности ПДн при их обработке в ИСПДн формируется на основании руководящих документов ФСТЭК России и ФСБ России.

5.8. В процессе функционирования ИСПДн может осуществляться модернизация СЗПДн. В обязательном порядке модернизация проводится в случае, если:
- ❏ произошло изменение номенклатуры обрабатываемых ПДн, влекущее за собой изменение класса ИСПДн;
- ❏ произошло изменение номенклатуры и/или актуальности угроз безопасности ПДн;
- ❏ изменилась структура ИСПДн или технические особенности ее построения (изменился состав или структура программного обеспечения, технических средств обработки ПДн, топологии ИСПДн и т.п.).

5.9. При возникновении условий влияющих на безопасность ПДн (компрометация паролей, нарушение целостности и доступности персональных данных и пр.) необходимо незамедлительно принять необходимые действия по сохранности персональных данных.

5.10. Лица, виновные в нарушении требований, предъявляемых законодательством РФ к защите ПДн, несут гражданскую, уголовную,

административную, дисциплинарную и иную предусмотренную законодательством РФ ответственность.

Индивидуальный предприниматель
Лазарева Юлия Сергеевна