

ООО «Ваан»

125040, Москва, улица Нижняя, дом 14, корпус 1

ИНН 7805399430/ КПП 771401001

Телефон: +7 495 646-81-29

УТВЕРЖДАЮ

Генеральный директор ООО «Ваан»

Тарханов В.О.

«26» марта 2013 г.



**ПОЛОЖЕНИЕ
ОБ ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ
В ООО «ВААН»**

Москва 2013 г.

СОДЕРЖАНИЕ

1. Термины и сокращения.....	3
2. Область применения.....	4
3. Общие положения.....	7
4. Организация работ по обеспечению безопасности персональных данных.....	8
5. Проведение работ по обеспечению безопасности персональных данных	10

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 в ООО «Ваан» (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 в ООО «Ваан» (далее – Компания).

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

- 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»;

2.3.1 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);

2.3.2 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. № 149/6/6-622;
- «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 работников ООО «Ваан», а также лиц, получающих временный доступ к обрабатываемым в Компании ПДн на законном основании. Ознакомление с Положением осуществляется под роспись в Журнале ознакомления с организационно-распорядительной документацией и требованиями законодательства Российской Федерации в области персональных данных.

2.5 Настоящее Положение вступает в силу с момента его утверждения Генеральным директором ООО «Ваан» и действует до замены его новым Положением.

2.6 Плановая актуализация настоящего Положения проводится не реже, чем два раза в год. Внеплановая актуализация проводится при возникновении одного из следующих условий:

- 1) изменение целей и/или состава обрабатываемых персональных данных;

- 2) возникновение условий существенно влияющих на процессы обработки персональных данных и не регламентированных настоящим документом;
- 3) по результатам контрольных мероприятий и проверок контролирующих органов исполнительной власти Российской Федерации, выявивших несоответствия требованиям по обеспечению безопасности ПДн;
- 4) при появлении новых требований к обеспечению безопасности ПДн со стороны российского законодательства и контролирующих органов исполнительной власти Российской Федерации.

2.7 Ответственным за пересмотр настоящее Положение и составление рекомендаций по изменению является Администратор информационной безопасности.

2.8 Внесение изменений в настоящее Положение производится на основании соответствующего приказа Генерального директора ООО «Ваан».

3. ОБЩИЕ ПОЛОЖЕНИЯ

3.1 ООО «Ваан» является оператором ПДн.

3.2 В Компании осуществляется обработка ПДн следующих категорий субъектов ПДн: работников Компании, клиентов (физических лиц и представителей юридических лиц), данные которых получены ООО «Ваан» в процессе осуществления своей деятельности.

3.3 ПДн, обрабатываемые в Компании, цели и сроки их обработки указаны в Перечне персональных данных, обрабатываемых в ООО «Ваан».

3.4 В Компании обработка ПДн осуществляется с использованием средств автоматизации и без использования таких средств.

3.5 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 Организация работ по обеспечению безопасности ПДн ООО «Ваан» должна осуществляться в соответствии с действующими нормативными правовыми актами и разработанными для этих целей организационно-распорядительными документами по защите ПДн в Компании.

4.3 Задачи по приведению ООО «Ваан» в соответствие с требованиями законодательства Российской Федерации в области защиты ПДн возлагаются на специально создаваемую для этих целей комиссию.

4.5 В случаях, когда ООО «Ваан» 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.

4.6 Работы по приведению ООО «Ваан» в соответствие с требованиями законодательства Российской Федерации ведутся по двум направлениям: обеспечение безопасности ПДн, обрабатываемых без использования средств автоматизации, и обеспечение безопасности ПДн в ИСПДн Компании.

4.7 Работы по обеспечению безопасности ПДн, обрабатываемых без использования средств автоматизации, ведутся по следующим направлениям:

- определение перечня лиц, осуществляющих неавтоматизированную обработку ПДн в ООО «Ваан»;
- информирование работников Компании об установленных правилах обработки ПДн и требований по их защите, повышение осведомленности в вопросах обеспечения безопасности ПДн;
- учет и защита носителей ПДн;
- разграничение доступа к носителям ПДн;
- уничтожение ПДн.

4.8 Организация и выполнение мероприятий по обеспечению безопасности ПДн, обрабатываемых в ИСПДн Компании, осуществляются в рамках системы защиты персональных данных ИСПДн (далее - СЗПДн), развертываемой в ИСПДн в процессе ее создания или модернизации.

4.9 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.

4.10 Система защиты ПДн должна являться неотъемлемой составной частью каждой вновь создаваемой ИСПДн ООО «Ваан».

4.11 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.

4.12 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 ООО «Ваан» 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 В Компании должен вестись учет действий, совершаемых с персональными данными в ИСПДн сотрудниками Компании.

5.5 Доступ к ПДн регламентируется Регламентом по допуску лиц к обработке персональных данных.

5.6 Лица, участвующие в обработке ПДн, должны быть проинформированы:

- о факте обработки ими ПДн – реализуется путем ознакомления лиц, обрабатывающих ПДн с Перечнем должностей и третьих лиц, имеющих доступ к персональным данным, обрабатываемым в ООО «Ваан»;
- о категориях обрабатываемых ПДн – реализуется путем ознакомления с утвержденным Перечнем персональных данных, обрабатываемых в ООО «Ваан»;
- о правилах осуществления обработки ПДн – реализуется путем ознакомления под роспись с организационно-распорядительной документацией ООО «Ваан», регламентирующей процессы обработки ПДн, в Журнале ознакомления с организационно-распорядительной документацией и требованиями законодательства Российской Федерации в области персональных данных

5.7 Неавтоматизированная обработка ПДн должна осуществляться таким образом, чтобы в отношении каждой категории ПДн можно было определить места хранения материальных носителей и установить перечень лиц, осуществляющих обработку ПДн либо имеющих к ним доступ. В Компании должен вестись учет носителей ПДн.

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

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

- при необходимости использования или распространения определенных ПДн осуществляется копирование ПДн, подлежащих распространению или использованию, способом, исключающим одновременное копирование ПДн, не подлежащих распространению и использованию, и используется (распространяется) копия ПДн – например, копирование части страницы, содержащей ПДн, которые необходимо использовать, предварительно закрыв остальную часть страницы чистым листом бумаги, либо копирование только необходимых страниц сшитого документа;
- при необходимости уничтожения или блокирования части ПДн уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование ПДн, подлежащих уничтожению или блокированию – например, копирование только необходимой части страницы, закрыв оставшуюся часть чистым листом бумаги.

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

5.11 В Компании Администратором информационной безопасности должен осуществляться контроль за принимаемыми мерами по обеспечению безопасности персональных данных.

5.12 При обработке ПДн, Компания, должна иметь возможность и средства для восстановления ПДн, при их модификации или уничтожении вследствие несанкционированного доступа к ним.

5.13 Должен быть определен перечень помещений, используемых для обработки ПДн. При этом организация режима безопасности, охрана этих помещений должны обеспечивать сохранность носителей ПДн, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

5.14 Пользователи ИСПДн должны обеспечивать сохранность съемных носителей, содержащих ПДн. В случае утраты носителя, пользователи должны немедленно сообщить об этом Администратору информационной безопасности.

5.15 Если при работе с ПДн работнику ООО «Ваан» необходимо покинуть рабочее место, материальные носители ПДн должны быть защищены от неконтролируемого доступа к ним. Для этого материальные носители запираются в отведенных для этого шкафах или сейфах.

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

5.17 Проведение работ по созданию (модернизации) СЗПДн Компании включает следующие стадии:

- предпроектная стадия;
- стадия проектирования;
- стадия реализации СЗПДн;
- стадия ввода в действие СЗПДн.

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

5.19 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».

5.20 В связи с тем, что в ИСПДн Компании помимо обеспечения конфиденциальности обрабатываемых ПДн требуется обеспечить целостность и доступность ПДн, ИСПДн ООО «Ваан» являются специальными информационными системами. ИСПДн ООО «Ваан» указаны в Перечне информационных систем персональных данных ООО «Ваан».

5.21 Класс ИСПДн оформляется соответствующим актом.

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

5.23 Перечень актуальных угроз формируется для каждой ИСПДн Компании с учетом условий функционирования ИСПДн и особенностей обработки ПДн.

5.24 По итогам классификации ИСПДн и результатам определения актуальных угроз безопасности ПДн формируются требования по обеспечению безопасности ПДн, обрабатываемых в ИСПДн. Данные требования оформляются в виде технического задания на СЗПДн.

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

5.26 Стадия реализации СЗПДн включает:

- закупку совокупности используемых в СЗПДн 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 СЗПДн и средства защиты информации.

5.27 На стадии ввода в действие СЗПДн 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.

5.28 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.).

5.29 Задачи по приведению ИСПДн ООО «Ваан» в соответствие с требованиями законодательства РФ в области защиты ПДн возлагаются на Администратора информационной безопасности.

5.30 При возникновении условий влияющих на безопасность ПДн (компрометация паролей, нарушение целостности и доступности персональных данных и пр.) необходимо незамедлительно проинформировать об этом Администратора информационной безопасности.

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