

## 1. Термины и определения

1.1. В настоящем Положении по обеспечению безопасности персональных данных ИП Ракицкий Андрей Евгеньевич используются следующие термины и определения.

<b>«Автоматизированная обработка персональных данных»</b>	Обработка персональных данных с помощью средств вычислительной техники.
<b>«Блокирование персональных данных»</b>	Временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).
<b>«Закон»</b>	Федеральный закон №152-ФЗ от 27.07.2006 года «О персональных данных».
<b>«Информационная система персональных данных»</b>	Совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.
<b>«Обезличивание персональных данных»</b>	Действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.
<b>«Обработка персональных данных»</b>	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.
<b>«Оператор»</b>	Индивидуальный предприниматель Ракицкий Андрей Евгеньевич зарегистрированный по законодательству Российской Федерации, ОГРНИП 315673300022818, ИНН 672906475287.
<b>«Персональные данные»</b>	Любая информация, относящаяся к прямо или

	косвенно определенному или определяемому физическому лицу (субъекту персональных данных).
<b>«Положение»</b>	Настоящее положение по обеспечению безопасности персональных данных ИП Ракицкий Андрей Евгеньевич
<b>«Предоставление персональных данных»</b>	Действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.
<b>«Распространение персональных данных»</b>	Действия, направленные на раскрытие персональных данных неопределенному кругу лиц.
<b>«Трансграничная передача персональных данных»</b>	Передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.
<b>«Уничтожение персональных данных»</b>	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.

1.2. Иные термины, используемые в Положении, определяются в соответствии с Законом и действующим законодательством Российской Федерации.

## **2. Область применения**

2.1. Положение разработано в целях выполнения требований законодательства Российской Федерации в области защиты персональных данных.

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

2.3. В связи с тем, что Оператор осуществляет сбор персональных данных с использованием информационно-телекоммуникационных сетей, в частности, сети Интернет, Положение постоянно размещено в свободном доступе в сети Интернет по адресу [http://net-dietam.net/PD\\_Security\\_Statement.pdf](http://net-dietam.net/PD_Security_Statement.pdf).

2.4. Положение разработано с учетом требований основных нормативных правовых актов в области защиты персональных данных, а именно:

2.4.1. Закона;

- 2.4.2. Постановления Правительства Российской Федерации от 17.11.2007 № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в Информационных системах персональных данных»;
- 2.4.3. Постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- 2.4.4. Приказа ФСТЭК Российской Федерации № 55, ФСБ Российской Федерации № 86, Мининформсвязи Российской Федерации № 20 от 13.02.2008 «Об утверждении Порядка проведения классификации информационных систем персональных данных»;
- 2.4.5. Нормативных актов ФСТЭК Российской Федерации:
  - 2.4.5.1. «Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденной Заместителем директора ФСТЭК России 15 февраля 2008 г.;
  - 2.4.5.2. «Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденной Заместителем директора ФСТЭК России 14 февраля 2008 г.;
  - 2.4.5.3. «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 Российской Федерации 19.02.2010 N 16456);
- 2.4.6. Нормативных актов ФСБ России:
  - 2.4.6.1. «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;
  - 2.4.6.2. «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.
- 2.5. Положение предназначено для всех работников Оператора, а также лиц, получающих временный доступ к обрабатываемым Оператором Персональным данным 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.

- 2.6. Положение вступает в силу с момента его утверждения уполномоченным лицом Оператора и действует до замены его новым Положением.
- 2.7. Плановая актуализация настоящего Положения проводится не реже, чем два раза в год. Внеплановая актуализация проводится при возникновении одного из следующих условий:
  - 2.7.1. изменение целей и/или состава обрабатываемых Персональных данных;
  - 2.7.2. возникновение условий существенно влияющих на процессы обработки Персональных данных и не регламентированных настоящим документом;
  - 2.7.3. по результатам мероприятий и проверок уполномоченных органов исполнительной власти Российской Федерации, выявивших несоответствия требованиям по обеспечению безопасности Персональных данных;
  - 2.7.4. при появлении новых требований к обеспечению безопасности Персональных данных со стороны законодательства и уполномоченных органов исполнительной власти Российской Федерации.
- 2.8. Ответственным за пересмотр Положения и составление рекомендаций по его изменению является Администратор информационной безопасности.
- 2.9. Внесение изменений в Положение производится на основании соответствующего приказа уполномоченного лица Оператора.

### **3. Общие положения**

- 3.1. Оператор осуществляет обработку Персональных данных следующих категорий субъектов Персональных данных: работников Оператора, контрагентов по заключенным договорам (физических лиц и представителей юридических лиц), данные которых получены Оператором в процессе осуществления своей деятельности.
- 3.2. Обрабатываемые Персональные данные могут быть отнесены к общедоступным Персональным данным на основании федеральных законов Российской Федерации, которые не распространяют на них требования по соблюдению конфиденциальности, или с согласия субъекта Персональных данных. Кроме того, при совершении субъектом Персональных данных определенных действий, включая, но, не ограничиваясь, внесением Персональных данных в форму заказа, а равно и внесением Персональных данных на сайт Оператора в сети Интернет, субъект Персональных данных самостоятельно делает свои Персональные данные общедоступными.

- 3.3. Персональные данные, обрабатываемые Оператором, цели и сроки их обработки указаны в Перечне персональных данных, обрабатываемых в ИП Ракицкий Андрей Евгеньевич
- 3.4. Оператор осуществляет обработку Персональных данных с использованием средств автоматизации и без использования таких средств.
- 3.5. Сроки хранения Персональных данных определяются в соответствии со сроком действия договора с субъектом 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 Персональных данных 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 Персональных данных, и осуществляемых в целях:
  - 4.1.1. предотвращения возможных (потенциальных) угроз безопасности Персональных данных;
  - 4.1.2. нейтрализации и/или парирования реализуемых угроз безопасности Персональных данных;
  - 4.1.3. ликвидации последствий реализации угроз безопасности Персональных данных.
- 4.2. Организация работ по обеспечению безопасности Персональных данных Оператора должна осуществляться в соответствии с действующими нормативными правовыми актами и разработанными для этих целей организационно-распорядительными документами по защите Персональных данных Оператора.
- 4.3. Задачи по приведению деятельности и внутренних документов Оператора в соответствие с требованиями законодательства Российской Федерации в области защиты Персональных данных возлагаются на специально создаваемую для этих целей комиссию.
- 4.4. В случаях, когда Оператор на основании договора поручает обработку Персональных данных другому лицу/сторонней организации, необходимо выполнить одно из следующих условий:
  - 4.4.1. в тексте договора в требованиях к контрагенту прописать обязанность обеспечения контрагентом безопасности и конфиденциальности Персональных данных;
  - 4.4.2. 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 Персональных данных при их обработке.

- 4.5. Работы по приведению деятельности и внутренних документов Оператора в соответствие с требованиями законодательства Российской Федерации ведутся по двум направлениям: обеспечение безопасности Персональных данных, обрабатываемых без использования средств автоматизации, и обеспечение безопасности Персональных данных в информационных системах Персональных данных Оператора.
- 4.6. Работы по обеспечению безопасности Персональных данных, обрабатываемых без использования средств автоматизации, ведутся по следующим направлениям:
  - 4.6.1. определение перечня лиц, осуществляющих неавтоматизированную обработку Персональных данных;
  - 4.6.2. информирование работников Оператора об установленных правилах обработки Персональных данных и требований по их защите, повышение осведомленности в вопросах обеспечения безопасности Персональных данных;
  - 4.6.3. учет и защита носителей Персональных данных;
  - 4.6.4. разграничение доступа к носителям Персональных данных;
  - 4.6.5. уничтожение Персональных данных.
- 4.7. Организация и выполнение мероприятий по обеспечению безопасности Персональных данных, обрабатываемых в информационных системах Персональных данных, осуществляются в рамках системы защиты персональных данных информационной системы, развертываемой в информационной системе в процессе ее создания или модернизации.
- 4.8. Система защиты Персональных данных представляет собой совокупность организационных мер и технических средств защиты информации, а также используемых в информационных системах Персональных данных информационных технологий, функционирующих в соответствии с определенными целями и задачами обеспечения безопасности Персональных данных.
- 4.9. Система защиты Персональных данных должна являться неотъемлемой составной частью каждой вновь создаваемой информационной системы Персональных данных.
- 4.10. Для существующих Информационных систем Персональных данных, в которых в процессе их создания не были предусмотрены меры по обеспечению безопасности Персональных данных должен быть проведен комплекс организационных и технических мероприятий по разработке и внедрению соответствующей системы защиты.
- 4.11. Структура, состав и основные функции системы защиты Персональных данных определяются в соответствии с классом Информационной системы Персональных данных и моделью угроз безопасности персональных данных при их обработке в Информационной системе Персональных данных.

## 5. Проведение работ по обеспечению безопасности Персональных данных

- 5.1. Для оценки уровня защищенности обрабатываемых Оператором Персональных данных и своевременного устранения несоответствий требованиям законодательства Российской Федерации в области защиты Персональных данных Оператором не реже чем один раз в год должен проводиться анализ изменений процессов защиты Персональных данных.
- 5.2. Анализ изменений проводится по следующим основным направлениям:
  - 5.2.1. перечень лиц (подразделений), участвующих в обработке Персональных данных, степень их участия в обработке Персональных данных и характер взаимодействия между собой;
  - 5.2.2. перечень и объем обрабатываемых Персональных данных;
  - 5.2.3. цели обработки Персональных данных;
  - 5.2.4. процедуры сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления и уничтожения Персональных данных;
  - 5.2.5. способы обработки Персональных данных (автоматизированная, неавтоматизированная);
  - 5.2.6. перечень сторонних организаций, в том числе государственных регулирующих органов, в рамках отношений с которыми осуществляется передача Персональных данных;
  - 5.2.7. перечень программно-технических средств, используемых для обработки Персональных данных;
  - 5.2.8. конфигурация и топология Информационной системы Персональных данных в целом и ее отдельных компонент, физические, функциональные и технологические связи как внутри этой системы, так и с другими системами различного уровня и назначения;
  - 5.2.9. способы физического подключения и логического взаимодействия компонент Информационной системы Персональных данных, способы подключения к сетям связи общего пользования и международного информационного обмена с определением пропускной способности линий связи;
  - 5.2.10. режимы обработки Персональных данных в Информационной системе Персональных данных в целом и в отдельных компонентах;
  - 5.2.11. состав используемого комплекса средств защиты Персональных данных и механизмов идентификации, аутентификации и разграничения прав доступа пользователей Информационной системе Персональных данных на уровне операционных систем, баз данных и прикладного программного обеспечения;

- 5.2.12. перечень организационно-распорядительной документации Оператора, определяющей порядок обработки и защиты Персональных данных;
- 5.2.13. физические меры защиты Персональных данных, организация пропускного режима.
- 5.3. Результаты анализа изменений используются для оценки корректности требований по обеспечению безопасности Персональных данных, обрабатываемых с использованием средств автоматизации и без использования таких средств и при необходимости их уточнения.
- 5.4. Оператором должен вестись учет действий, совершаемых с персональными данными в Информационной системе Персональных данных работниками Оператора.
- 5.5. Доступ к Персональным данным регламентируется Регламентом по допуску лиц к обработке персональных данных.
- 5.6. Лица, участвующие в обработке Персональных данных, должны быть проинформированы:
  - 5.6.1. о факте обработки ими Персональных данных – реализуется путем ознакомления лиц, обрабатывающих Персональные данные с Перечнем должностей и третьих лиц, имеющих доступ к персональным данным, обрабатываемым ИП Ракицкий Андрей Евгеньевич
  - 5.6.2. о категориях обрабатываемых Персональных данных – реализуется путем ознакомления с утвержденным Перечнем персональных данных, обрабатываемых в ИП Ракицкий Андрей Евгеньевич
  - 5.6.3. о правилах осуществления обработки Персональных данных – реализуется путем ознакомления под роспись с организационно-распорядительной документацией Оператора, регламентирующей процессы обработки Персональных данных, в Журнале ознакомления с организационно-распорядительной документацией и требованиями законодательства Российской Федерации в области персональных данных.
- 5.7. Неавтоматизированная обработка Персональных данных должна осуществляться таким образом, чтобы в отношении каждой категории Персональных данных можно было определить места хранения материальных носителей и установить перечень лиц, осуществляющих обработку Персональных данных либо имеющих к ним доступ. Оператор должен вести учет носителей Персональных данных.
- 5.8. Фиксация Персональных данных должна осуществляться на отдельных материальных носителях (отдельных документах). Персональные данные должны отделяться от иной информации.
- 5.9. Фиксация на одном материальном носителе Персональных данных, цели обработки которых заведомо несовместимы, не допускается. В случае если на одном материальном носителе все же зафиксированы Персональные данные, цели обработки которых несовместимы, должны быть приняты меры по обеспечению отдельной обработки Персональных данных, в частности:



- 5.9.1. при необходимости использования или распространения определенных Персональных данных осуществляется копирование Персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование Персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия Персональных данных – например, копирование части страницы, содержащей Персональные данные, которые необходимо использовать, предварительно закрыв остальную часть страницы чистым листом бумаги, либо копирование только необходимых страниц сшитого документа;
- 5.9.2. при необходимости уничтожения или блокирования части Персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование Персональных данных, подлежащих уничтожению или блокированию – например, копирование только необходимой части страницы, закрыв оставшуюся часть чистым листом бумаги.
- 5.10. Оператором должен осуществляться мониторинг фактов несанкционированного доступа к персональным данным и приниматься соответствующие меры при их обнаружении. Мониторинг осуществляется Администратором информационной безопасности.
- 5.11. Администратором информационной безопасности должен осуществляться контроль за принимаемыми мерами по обеспечению безопасности персональных данных.
- 5.12. При обработке Персональных данных, Оператор должен иметь возможность и средства для восстановления Персональных данных, при их модификации или уничтожении вследствие несанкционированного доступа к ним.
- 5.13. Должен быть определен перечень помещений, используемых для обработки Персональных данных. При этом организация режима безопасности, охрана этих помещений должны обеспечивать сохранность носителей Персональных данных, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.
- 5.14. Пользователи Информационной системы Персональных данных должны обеспечивать сохранность съемных носителей, содержащих Персональные данные. В случае утраты носителя, пользователи должны немедленно сообщить об этом Администратору информационной безопасности.
- 5.15. Если при работе с Персональными данными работнику Оператора необходимо покинуть рабочее место, материальные носители Персональных данных 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 Персональных данных Оператор прекращает обработку Персональных данных или обеспечивает ее прекращение (если обработка

Персональных данных осуществляется другим лицом, действующим по поручению Оператора) и уничтожает Персональные данные или обеспечивает их уничтожение (если обработка Персональных данных осуществляется другим лицом, действующим по поручению Оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки Персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект Персональных данных.

- 5.17. Проведение работ по созданию (модернизации) системы защиты Персональных данных Оператора включает следующие стадии:
  - 5.17.1. предпроектная стадия;
  - 5.17.2. стадия проектирования;
  - 5.17.3. стадия реализации системы защиты Персональных данных;
  - 5.17.4. стадия ввода в действие системы защиты Персональных данных.
- 5.18. На предпроектной стадии проводится классификация Информационной системы Персональных данных, формируется модель угроз безопасности Персональных данных при их обработке в Информационной системе Персональных данных, разрабатывается техническое задание на систему защиты Персональных данных.
- 5.19. Классификация Информационной системы Персональных данных 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 Информационной системе Персональных данных Оператора помимо обеспечения конфиденциальности обрабатываемых Персональных данных требуется обеспечить целостность и доступность Персональных данных, Информационная система Персональных данных Оператора является специальной информационной системой. Информационная система Персональных данных Оператора указана в Перечне информационных систем персональных данных ИП Ракицкий Андрей Евгеньевич.
- 5.21. Класс Информационной системы Персональных данных оформляется соответствующим актом.
- 5.22. Модель угроз безопасности Персональных данных при их обработке в Информационной системе Персональных данных формируется на основании соответствующих документов ФСТЭК России и ФСБ России.
- 5.23. Перечень актуальных угроз формируется для каждой Информационной системы Персональных данных Оператора с учетом условий функционирования Информационной системы Персональных данных и особенностей обработки Персональных данных.
- 5.24. По итогам классификации Информационной системы Персональных данных и результатам определения актуальных угроз безопасности Персональных данных формируются требования по обеспечению безопасности Персональных данных,

обрабатываемых в Информационной системе Персональных данных. Данные требования оформляются в виде технического задания на систему защиты Персональных данных.

- 5.25. Стадия проектирования системы защиты Персональных данных включает разработку системы защиты Персональных данных в составе Информационной системы Персональных данных, а именно разработку разделов задания и проекта проведения по созданию (модернизации) системы защиты Персональных данных в соответствии с требованиями технического задания;
- 5.26. Стадия реализации системы защиты Персональных данных включает:
  - 5.26.1. закупку совокупности используемых в системе защиты Персональных данных сертифицированных технических, программных и программно-технических средств защиты информации и их установку;
  - 5.26.2. определение подразделений и назначение лиц, ответственных за эксплуатацию средств защиты информации с их обучением;
  - 5.26.3. разработку эксплуатационной документации на систему защиты Персональных данных и средства защиты информации.
- 5.27. На стадии ввода в действие системы защиты Персональных данных осуществляются:
  - 5.27.1. предварительные испытания средств защиты информации в комплексе с другими техническими и программными средствами;
  - 5.27.2. устранение несоответствий по итогам предварительных испытаний;
  - 5.27.3. опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе Информационной системы;
  - 5.27.4. приемо-сдаточные испытания средств защиты информации по результатам опытной эксплуатации.
- 5.28. В процессе функционирования Информационной системы Персональных данных может осуществляться модернизация система защиты Персональных данных. В обязательном порядке модернизация проводится в случае, если:
  - 5.28.1. произошло изменение номенклатуры обрабатываемых Персональных данных, влекущее за собой изменение класса Информационной системы Персональных данных;
  - 5.28.2. произошло изменение номенклатуры и/или актуальности угроз безопасности Персональных данных;
  - 5.28.3. изменилась структура Информационной системы Персональных данных или технические особенности ее построения (изменился состав или структура программного обеспечения, технических средств обработки Персональных данных, топологии Информационной системы Персональных данных и т.п.).

- 5.29. Задачи по приведению Информационной системы Персональных данных ИП Ушанов Азамат Мирасович в соответствии с требованиями законодательства Российской Федерации в области защиты Персональных данных возлагаются на Администратора информационной безопасности.
- 5.30. При возникновении условий влияющих на безопасность Персональных данных (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 Российской Федерации к защите Персональных данных, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.