УТВЕРЖДАЮ
Директор ООО «МИКО»

_____ Г.Т. Климова
« 01 » марта 2021г.

ПОЛИТИКА
Общества с ограниченной ответственностью «МИКО» (ООО «МИКО») в отношении обработки персональных данных

1. Термины и определения

Персональные данные (ПДн) - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн). Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн.

Обработка ПДн - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн.

Автоматизированная обработка ПДн - обработка ПДн с помощью средств вычислительной техники.

Распространение ПДн - действия, направленные на раскрытие ПДн неопределенному кругу лиц.

Предоставление ПДн - действия, направленные на раскрытие ПДнопределенному лицу или определенному кругу лиц.

Блокирование ПДн - временное прекращение обработки ПДн (за исключениемслучаев, если обработка необходима для уточнения ПДн).

Уничтожение ПДн - действия, в результате которых становится невозможным восстановить содержание ПДн в ИСПДн и (или) в результате которых уничтожаются материальные носители ПДн.

Обезличивание ПДн - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность ПДн конкретному субъекту ПДн.

Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств.

Трансграничная передача ПДн - передача ПДн на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

2. Назначение и правовая основа документа

Политика ООО «МИКО» (далее по тексту – Организация) определяет систему взглядов на проблему обеспечения безопасности ПДн и представляет собой систематизированное изложение целей и задач защиты, как одно или несколько правил, процедур, практических приемов и руководящих принципов в области информационной безопасности, которыми руководствуется Организация в своей деятельности, а также основных принципов построения, организационных, технологических и процедурных аспектов обеспечения безопасности ПДн.

Законодательной основой настоящей Политики являются Конституция Российской Федерации, Гражданский кодекс РФ, Уголовный кодекс РФ, Трудовой кодекс РФ, Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных», Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 №149-ФЗ, Федеральный закон от 17.07.1999 №178-ФЗ «О государственной социальной помощи», законы, указы, постановления, другие нормативные документы действующего законодательства Российской Федерации в области предоставления населению социальной помощи, а так же документы ФСТЭК и ФСБ России.

Использование данной Политики в качестве основы для построения комплексной системы информационной безопасности ПДн Организации позволит оптимизировать затраты на ее построение.

При разработке Политики учитывались основные принципы создания комплексных систем

обеспечения безопасности информации, характеристики и возможности организационно-технических методов и современных аппаратно-программных средств защиты и противодействия угрозам безопасности информации.

Основные положения Политики базируются на качественном осмыслении вопросов безопасности информации и не затрагивают вопросов экономического (количественного) анализа рисков и обоснования необходимых затрат на защитуинформации.

3. Основными объектами системы безопасности ПДн в Организации являются:

-информационные ресурсы с ограниченным доступом, содержащие ПДн;

-процессы обработки ПДн в ИСПДн Организации, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, персонал разработчиков и пользователей системы и ее обслуживающий персонал;

-информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых расположены технические средства обработки ПДн. Интересы затрагиваемых субъектов информационных отношений

Субъектами информационных отношений при обеспечении безопасности ПДн Организации являются:

- Организация, как собственник информационных ресурсов;
- руководство и сотрудники Организации, в соответствии с возложенными наних функциями;
- физические лица, получающие социальные услуги в Организации.

Перечисленные субъекты информационных отношений заинтересованы вобеспечении:

-своевременного доступа к необходимым им ПДн (их доступности);

-достоверности (полноты, точности, адекватности, целостности) ПДн;

-конфиденциальности (сохранения в тайне) ПДн;

-защиты от навязывания им ложных (недостоверных, искаженных) ПДн;

-разграничения ответственности за нарушения их прав (интересов) и установленных правил обращения с ПДн;

-возможности осуществления непрерывного контроля за процессами обработки и передачи ПДн;

-защиты ПДн от незаконного распространения.

3.1. Цель защиты

Основной целью, на достижение которой направлены все положения настоящей Политики, является защита субъектов информационных отношений Организации от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на ПДн, их носители, процессы обработки и передачи.

3.2. Основные задачи системы обеспечения безопасности ПДн

Для достижения основной цели защиты и обеспечения указанных свойств ПДн система обеспечения информационной безопасности Организации должна обеспечивать эффективное решение следующих задач:

-своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений, нарушению нормального функционирования информационных систем Организации;

-создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;

-создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации;

-защиту от вмешательства в процесс функционирования информационных систем посторонних лиц (доступ к информационным ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);

-разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам Организации (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей), тоесть защиту от несанкционированного доступа;

-обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);

-защиту от несанкционированной модификации используемых в информационных системах Организации программных средств, а также защиту системы от внедрения несанкционированных программ, включая компьютерные вирусы;

-защиту информации ограниченного пользования от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

3.3. Основные пути решения задач системы защиты

Поставленные основные цели защиты и решение перечисленных выше задач достигаются:

-строгим учетом всех подлежащих защите ресурсов информационных систем Организации (информации, задач, документов, каналов связи, серверов, автоматизированных рабочих мест);

-учетом действий персонала, осуществляющего обслуживание и модификацию программных и технических средств информационных систем;

-полнотой, реальной выполнимостью требований организационно-распорядительных документов Организации по вопросам обеспечения безопасности информации;

-подготовкой должностных лиц (сотрудников), ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности ПДн и процессов их обработки;

-наделением каждого сотрудника (пользователя) минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к информационным ресурсам Организации;

-четким знанием и строгим соблюдением всеми пользователями информационных систем Организации требований организационно-распорядительных документов по вопросам обеспечения безопасности информации;

-персональной ответственностью за свои действия каждого сотрудника, в рамках своих функциональных обязанностей имеющего доступ к информационным ресурсам Организации;

-непрерывным поддержанием необходимого уровня защищенности элементов информационной среды;

-применением физических и технических (программно-аппаратных) средств защиты ресурсов системы и непрерывной административной поддержкой их использования;

-эффективным контролем над соблюдением пользователями информационных ресурсов требований по обеспечению безопасности информации;

-юридической защитой интересов Организации при взаимодействии с внешними организациями (связанном с обменом ПДн) от противоправных действий, как со стороны этих организаций, так и от несанкционированных действий обслуживающего персонала и третьих лиц.

4. Принципы обеспечения безопасности ПДн Организации:

4.1. Законность

Предполагает осуществление защитных мероприятий и разработку системы безопасности ПДн Организации в соответствии с действующим законодательством в области защиты ПДн, а также других законодательных актов по безопасности информации РФ, с применением всех дозволенных методов обнаружения и пресечения правонарушений при работе с ПДн. Принятые меры безопасности ПДн не должны препятствовать доступу правоохранительных органов в предусмотренных законодательством РФ случаях.

4.2. Системность

Системный подход к построению системы защиты информации в Организации предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности ПДн.

4.3. Комплексность

Комплексное использование методов и средств защиты компьютерных систем предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами.

4.4. Непрерывность защиты

Обеспечение безопасности ПДн - процесс, осуществляемый руководством Организации, ответственными за организацию обработки ПДн и сотрудниками всех уровней. Это не только и не столько процедура или политика, которая осуществляется в определенный отрезок времени или совокупность средств защиты, сколько процесс, который должен постоянно идти на всех уровнях

внутри Организации и каждый сотрудник должен принимать участие в этом процессе.

4.5. Своевременность

Мероприятия предупредительного характера направленные на обеспечение безопасности ПДн включают постановку задач по комплексной защите ПДн и реализацию мер обеспечения безопасности ПДн на стадии разработки информационных систем в целом и их систем защиты. Разработка системы защиты должна вестись параллельно с разработкой и развитием защищаемых информационных систем.

4.6. Разумная достаточность

Предполагает соответствие уровня затрат на обеспечение безопасности ПДн ценности информационных ресурсов и величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения.

4.7. Персональная ответственность

Предполагает возложение ответственности за обеспечение безопасности ПДн и системы их обработки на каждого сотрудника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

4.8. Минимизация полномочий

Означает предоставление пользователям минимальных прав доступа в соответствии со служебной необходимостью. Доступ к ПДн должен предоставляться только в том случае и объеме, если это необходимо сотруднику для выполнения его должностных обязанностей.

4.9. Исключение конфликта интересов

Эффективная система обеспечения информационной безопасности предполагает четкое разделение обязанностей сотрудников и исключение ситуаций, когда сфера ответственности сотрудников допускает конфликт интересов. Сферы потенциальных конфликтов должны выявляться, минимизироваться, и находится под строгим контролем генерального директора Организации. Реализация данного принципа предполагает, что не один сотрудник не должен иметь полномочий, позволяющих ему единолично осуществлять выполнение критичных операций.

4.10. Взаимодействие и сотрудничество

Предполагает создание благоприятной атмосферы в коллективе Организации. В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие деятельности ответственного за обработку ПДн. Генеральный директор Организации несет ответственность за строгое соблюдение этических норм и стандартов профессиональной деятельности, подчеркивающей идемонстрирующей персоналу на всех уровнях важность обеспечения информационной безопасности Организации.

4.11. Гибкость системы защиты

Система обеспечения информационной безопасности должна быть способна реагировать на изменения внешней среды и условий осуществления Организацией своей деятельности. В число таких изменений входят:

-изменения организационной и штатной структуры Организации;

-изменение существующих или внедрение принципиально новых информационных систем;

-новые технические средства.

4.12. Простота применения средств защиты

Механизмы и методы защиты должны быть интуитивно понятны и просты в использовании.

4.13. Обоснованность и техническая реализуемость

Информационные технологии, технические и программные средства, средства и меры защиты ПДн должны быть реализованы на современном уровне развития науки и техники, обоснованы с точки зрения достижения заданного уровня безопасности информации и экономической целесообразности, а также должны соответствовать установленным нормам и требованиям по безопасности ПДн.

4.14. Специализация и профессионализм

Предполагает возможность привлечения к разработке средств и реализации мер защиты ПДн специализированных организаций имеющих опыт практической работы и лицензию на право оказания

услуг в этой области.

4.15. Обязательность контроля

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил, обеспечения безопасности ПДн, на основе используемых систем и средств защиты ПДн, при совершенствовании критериев и методов оценки эффективности этих систем и средств. Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

5. Меры обеспечения информационной безопасности

Все меры обеспечения безопасности ИСПДн Организации подразделяются на:

5.1. Правовые меры защиты

К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с ПДн, закрепляющие права и обязанности участников информационных отношений в процессе их обработки и использования, а также устанавливающие ответственность за нарушения этих правил. Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом ИСПДн Организации.

5.2. Морально-этические меры защиты

К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения информационных технологий в обществе. Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективе.

5.3. Организационные меры защиты

Организационные меры защиты - это меры организационного характера, регламентирующие процессы функционирования системы обработки ПДн, использование ее ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

5.4. Формирование политики безопасности

Главная цель административных мер, предпринимаемых на высшем управленческом уровне - сформировать политику в области обеспечения безопасности ПДн (отражающую подходы к защите ПДн) и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

5.5. Регламентация доступа в помещения

Компоненты информационных систем Организации должны размещаться в помещениях, находящихся под охраной или наблюдением, исключающим возможность бесконтрольного проникновения в помещения посторонних лиц и обеспечивающим физическую сохранность находящихся в помещении защищаемых ресурсов (документов, АРМ и т.п.). Уборка таких помещений должна производиться в присутствии ответственного сотрудника, за которым закреплены данные компоненты, с соблюдением мер, исключающих доступ посторонних лиц к защищаемым информационным ресурсам.

Все посторонние лица допускаются в помещения с компонентами информационной системы только в присутствии сотрудников Организации.

5.6. Регламентация допуска сотрудников к использованию информационных ресурсов

В рамках разрешительной системы доступа устанавливается: кто, кому, какую информацию и для какого вида доступа может предоставить и при каких условиях.

Допуск пользователей к работе с информационными системами Организации и доступ к их ресурсам должен быть строго регламентирован. Любые изменениясостава и полномочий пользователей подсистем должны производиться установленным порядком.

5.7. Регламентация процессов обслуживания и осуществления модификации аппаратных и программных ресурсов

В целях поддержания режима информационной безопасности аппаратно- программная

конфигурация автоматизированных рабочих мест сотрудников Учреждения, с которых возможен доступ к ресурсам информационной системы, должна соответствовать кругу возложенных на данных пользователей функциональных обязанностей.

В компонентах информационной системы и на рабочих местах пользователей должны устанавливаться и использоваться лицензионные программные средства.

5.8. Обеспечение и контроль физической целостности аппаратных ресурсов

Оборудование информационных систем, используемое для доступа и хранения ПДн, к которому доступ обслуживающего персонала в процессе эксплуатации не требуется, после наладочных, ремонтных и иных работ, связанных с доступом к его компонентам должно закрываться.

5.9. Подбор и подготовка персонала, обучение пользователей

Пользователи ИСПДн Организации, а также руководящий и обслуживающий персонал должны быть ознакомлены со своим уровнем полномочий, а также организационно-распорядительной, нормативной, технической и эксплуатационной документацией, определяющей требования и порядок обработки ПДн в Организации.

5.10. Средства обеспечения безопасности ПДн

Для обеспечения информационной безопасности Организации используются следующие средства защиты:

- Физические меры защиты основанные на применении разного рода механических, электронных или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемым ПДн, а также технических средств визуального наблюдения, связи и охранной сигнализации.

- Технические меры защиты основанные на использовании различных электронных устройств и специальных программ и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, и т.д.).

- Средства идентификации и аутентификации пользователей

В целях предотвращения работы с ресурсами ИСПДн Организации посторонних лиц необходимо обеспечить возможность распознавания каждого легального пользователя (или групп пользователей). Для идентификации могут применяться различного рода устройства: магнитные карточки, ключи, ключевые вставки, дискеты и т.п.

Аутентификация (подтверждение подлинности) пользователей также может осуществляться:

-путем проверки наличия у пользователей каких-либо специальных устройств (магнитных карточек, ключей, ключевых вставок и т.д.);

-путем проверки знания ими паролей;

-путем проверки уникальных физических характеристик и параметров самих пользователей при помощи специальных биометрических устройств.

5.11. Контроль эффективности системы защиты

Контроль эффективности защиты ПДн осуществляется с целью своевременного выявления и предотвращения утечки ПДн за счет несанкционированного доступа, а также предупреждения возможных специальных воздействий, направленных на уничтожение ПДн, разрушение средств информатизации. Контроль может проводиться привлекаемыми для этой цели организациями, имеющими лицензию на этот вид деятельности. Оценка эффективности мер защиты ПДн проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.