Утверждено

Приказом Владимирского УФАС России

от 30.11.2016 № 329/2/16

ПОЛИТИ**КА**

управления Федеральной антимонопольной службы по Владимирской области 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 ПДн определенному лицу или определенному кругу лиц.

Блокирование ПДн - временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения 11Ди).

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 па территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

**2.** Назначение и правовая основа документа.

Политика Владимирского УФАС России (далее Управление) 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 Управление 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, Уголовный и Трудовой кодексы, Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных», Федеральный закон РФ от 27.07.2004 № 79-ФЗ «О государственной гражданской службе». Федеральный закон РФ от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан РФ», Федеральный закон РФ от 10.01.2002 № 7-ФЗ «Об охране окружающей среды», законы, указы, постановления, другие нормативные документы действующего законодательства Российской Федерации, документы ФСТЭК и ФСБ России.

Использование данной Политики в качестве основы для построения комплексной системы информационной безопасности ПДн Управления 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 защиту информации.

З. Основными объектами системы безопасности ПДн в Управлении являются:

* информационные ресурсы с ограниченным доступом, содержащие ПДн;
* процессы обработки ПДн в ИСПДн Управления, 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 ПДп, файлы cookies и метаданные.

4. Интересы затрагиваемых субъектов информационных отношений.

Субъектами информационных отношений при обеспечении безопасности ПДн Управления являются:

- Управление, как собственник информационных ресурсов;

- руководство и сотрудники Управления, в соответствии с возложенными на них функциями;

- физические лица, не являющиеся сотрудниками Управления, но имеющими с ней отношения;

Перечисленные субъекты информационных отношений заинтересованы в обеспечении:

- своевременного доступа к необходимым им 11Дн (их доступности);

* достоверности (полноты, точности, адекватности, целостности) ПДн;
* конфиденциальности (сохранения в тайне) 11Дн;

защиты от навязывания им ложных (недостоверных, искаженных) 11Дп; разграничения ответственности за нарушения их нрав (интересов) и установленных правил обращения с 11Дн;

возможности осуществления непрерывного контроля и управления процессами обработки и передачи ПДн;

* защиты ПДн от незаконного распространения.

1. Цели защиты.

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

Указанная цель достигается посредством обеспечения и постоянного поддержания следующих свойств ПДн:

* доступности для легальных пользователей (устойчивого функционирования информационных систем Управления, при котором пользователи имеют возможность получения необходимых ПДн и результатов решения задач за приемлемое для них время);
* целостности и аутентичности (подтверждение авторства) ПДн, хранимых и обрабатываемых в информационных системах Управления и передаваемой по каналам связи;
* конфиденциальности - сохранения в тайне определенной части ПДн, хранимых, обрабатываемых и передаваемых по каналам связи.

Необходимый уровень доступности, целостности и конфиденциальности Г1Дп обеспечивается соответствующими множеству значимых угроз методами и средствами.

1. Основные задачи системы обеспечения безопасности ПДн.

Для достижения основной цели защиты и обеспечения указанных свойств ПДн система обеспечения информационной безопасности Управления 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 Управления;

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 Управления (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей), то есть 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 Управления 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.

1. Основные пути решения задач системы защиты.

Поставленные основные цели защиты и решение перечисленных выше задач достигаются:

* строгим учетом всех подлежащих защите ресурсов информационных систем Управления (информации, задач, документов, каналов связи, серверов, автоматизированных рабочих мест);
* журналированием действий персонала, осуществляющего обслуживание и модификацию программных и технических средств информационных систем
* полнотой, реальной выполнимостью и непротиворечивостью требований организационно-распорядительных документов Управления по вопросам обеспечения безопасности информации;
* подготовкой должностных лиц (сотрудников), ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности 11Дн и процессов их обработки;
* наделением каждого сотрудника (пользователя) минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к информационным ресурсам Управления;
* четким знанием и строгим соблюдением всеми пользователями информационных систем Управления требований организационно-распорядительных документов по вопросам обеспечения безопасности и информации;
* персональной ответственностью за свои действия каждого сотрудника, в рамках своих функциональных обязанностей имеющего доступ к информационным ресурсам Управления;
* 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 Управления 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.

5. Построение системы, обеспечения безопасности ПДн Управления, и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

1. Законность.

Предполагает осуществление защитных мероприятий и разработку системы безопасности ПДн Управления 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 случаях.

Все пользователи ИСПДн должны иметь представление об ответственности за правонарушения в области обработки 11Дн.

1. Системность.

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

При создании системы защиты должны учитываться все слабые и наиболее уязвимые места ИСПДн, а также характер, возможные объекты и направления атак на нее со стороны нарушителей (особенно высококвалифицированных злоумышленников).

Система защиты должна строиться с учетом не только всех известных каналов проникновения и несанкционированного доступа к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

1. Комплексность.

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

1. Непрерывность защиты.

Обеспечение безопасности ПДн - процесс, осуществляемый руководством Управления, 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 Управления и каждый сотрудник должен принимать участие в этом процессе. Деятельность по обеспечению информационной безопасности является составной частью повседневной деятельности Управления. И ее эффективность зависит от участия руководства Управления в обеспечении информационной безопасности ПДн.

Кроме того, большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных "закладок" и других средств преодоления защиты.

1. Своевременность.

Предполагает упреждающий характер мер обеспечения безопасности ПДн, то есть постановку задач по комплексной защите ПДн и реализацию мер обеспечения безопасности ПДн на ранних стадиях разработки информационных систем в целом и их систем защиты, в частности.

Разработка системы защиты должна вестись параллельно с разработкой и развитием самих защищаемых информационных систем. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) системы, обладающие достаточным уровнем защищенности.

1. Преемственность и совершенствование.

Предполагает постоянное совершенствование мер и средств защиты ПДи па основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационных систем Управления и системы их защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований но защите, достигнутого отечественного и зарубежного опыта в этой области.

1. Разумная достаточность (экономическая целесообразность).

Предполагает соответствие уровня затрат на обеспечение безопасности ПДн

ценности информационных ресурсов и величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения. Используемые меры и средства обеспечения безопасности информационных ресурсов не должны заметно ухудшать эргономические показатели работы компонентов ИСПДн Управления. Излишние меры безопасности, помимо экономической неэффективности, приводя т к утомлению и раздражению персонала.

Создать абсолютно непреодолимую систему защиты принципиально невозможно. Пока ПДн находятся в обращении, принимаемые меры могут только снизить вероятность негативных воздействий или ущерб от них, но не исключи ть их полностью. При достаточном количестве времени и средств возможно преодолеть любую защиту. Поэтому имеет смысл рассматривать некоторый приемлемый уровень обеспечения безопасности. Высокоэффективная система защиты стоит дорого, использует при работе существенную часть ресурсов и может создавать ощутимые дополнительные неудобства пользователям. Важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми.

1. 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.

1. 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.

1. Исключение конфликта интересов (разделение функций).

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 независимым контролем. Реализация данного принципа предполагает, что не один сотрудник не должен иметь полномочий, позволяющих ему единолично осуществлять выполнение критичных операций. Наделение сотрудников полномочиями, порождающими конфликт интересов, дает ему возможность подтасовывать информацию в корыстных целях или с тем, чтобы скрыть проблемы или понесенные убытки. Для снижения риска манипулирования ПДн и риска хищения, такие полномочия должны в максимально возможной степени быть разделены между различными сотрудниками или подразделениями Управления. Необходимо проводить периодические проверки обязанностей, функций и деятельности сотрудников, выполняющих ключевые функции, с тем, чтобы они не имели возможности скрывать совершение неправомерных действий. Кроме того, необходимо принимать специальные меры по недопущению сговора между сотрудниками.

1. Взаимодействие и сотрудничество.

Предполагает создание благоприятной атмосферы в коллективе Управления. В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие деятельности ответственного за обработку ПДн.

Важным элементом эффективной системы обеспечения безопасности ПДн в Управлении является высокая культура работы с информацией. Руководство Управления несет ответственность за строгое соблюдение этических норм и стандартов профессиональной деятельности, подчеркивающей и демонстрирующей персоналу на всех уровнях важность обеспечения информационной безопасности Управления. Все сотрудники Управления должны понимать свою роль в процессе обеспечения информационной безопасности и принимать участие в этом процессе. Несмотря на то, что высокая культура обеспечения информационной безопасности не гарантирует автоматического достижения целей, ее отсутствие создает больше возможностей для нарушения безопасности или не обнаружения фактов ее нарушения.

1. Гибкость системы защиты.

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

изменения организационной и штатной структуры Управления;

изменение существующих или внедрение принципиально новых информационных систем;

- новые технические средства.

Свойство гибкости системы обеспечения информационной безопасности избавляет в таких ситуациях от необходимости принятия кардинальных мер до полной замене средств и методов защиты на новые, что снижает ее общую стоимость.

1. Открытость алгоритмов и механизмов защиты.

Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже авторам). Это, однако, не означает, что информация об используемых системах и механизмах защиты должна быть общедоступна.

1. Простота применении средств защиты.

Механизмы и методы защиты должны быть интуитивно понятны и просты в использовании. Применение средств и методов защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций.

1. Обоснованность и технический 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.

1. Специализация и профессионализм.

Предполагает привлечение к разработке средств и реализации мер защиты ПДн специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности информационных ресурсов, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными специалистами Управления (ответственных за организацию обработки 11Дн).

1. 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 направленные на уменьшение возможности совершения сотрудниками ошибок и нарушений в рамках предоставленных им прав и полномочий.

1. Организационные (административные) меры защиты.

Организационные (административные) меры зашиты - это меры организационного характера, регламентирующие процессы функционирования системы обработки ГЩн, 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.

1. Формирование политики безопасности.

Главная цель административных мер, предпринимаемых па 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.

С практической точки зрения политику в области обеспечения безопасности ПДн в Управлении целесообразно разбить на два уровня. К верхнему уровню относятся решения руководства, затрагивающие деятельность Управления в целом. Политика верхнего уровня должна четко очертить сферу влияния и ограничения при определении целей безопасности ПДн, определить какими ресурсами (материальные, структурные, организационные) они будут достигнуты, и найти разумный компромисс между приемлемым уровнем безопасности и функциональностью.

Политика нижнего уровня, определяет процедуры, и правила достижения целей и решения задач безопасности ПДн и детализирует (регламентирует) эти правила:

* каковы роли и обязанности должностных лиц, отвечающие за проведение политики безопасности ПДн;
* кто имеет права доступа к ПДн, кто и при каких условиях может читать и модифицировать ПДн и т.д.

Политика нижнего уровня должна:

* предусматривать регламент информационных отношений, исключающих возможность произвольных, монопольных или несанкционированных действий в отношении информационных ресурсов;
* определять коалиционные и иерархические принципы и методы разделения секретов и разграничения доступа к 11Дн;
* выбирать программно-технические (аппаратные) средства противодействия ПСД, аутентификации, авторизации, идентификации и других защитных механизмов, обеспечивающих гарантии реализации прав и ответственности субъектов информационных отношений.

1. Регламентации доступа в помещении.

Компоненты информационных систем Управления должны размещаться в помещениях, находящихся под охраной или наблюдением, исключающим

возможность бесконтрольного проникновения в помещения посторонних лиц.