УТВЕРЖДЕНА
приказом НИЯУ МИФИ
от 16 03 2015 г. № 75/3

ПОЛИТИКА

в отношении обработки персональных данных
в НИЯУ МИФИ

Документ не подлежит передаче третьим лицам без письменного разрешения ректора

Москва
2015

Содержание

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Политика в отношении обработки персональных данных (далее – Политика) в федеральном государственном автономном образовательном учреждении высшего профессионального образования «Национальный исследовательский ядерный университет «МИФИ» (далее – НИЯУ МИФИ) определяет основные подходы к обработке и защите персональных данных (далее – ПДн) в НИЯУ МИФИ и содержит сведения о реализуемых требованиях к защите ПДн. Политика представляет собой систематизированное изложение целей, задач, принципов и условий обработки ПДн и действует в отношении любой информации о субъекте ПДн (физическом лице), которую НИЯУ МИФИ вправе обрабатывать.

1.2. Настоящая Политика разработана в соответствии с Конституцией Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» и иными нормативно-правовыми актами, регулирующими отношения, связанные с обработкой и защитой ПДн, а также Уставом НИЯУ МИФИ.

1.3. Политика является методологической основой для:

– принятия управленческих решений и разработки практических мер по воплощению политики в отношении обработки ПДн и их защиты и выработки комплекса согласованных правовых, организационных, технических и иных мер, направленных на выявление угроз в отношении ПДн и их ликвидацию (уменьшение) в НИЯУ МИФИ;

– координации деятельности структурных подразделений НИЯУ МИФИ при проведении работ по созданию, развитию и эксплуатации информационных технологий с соблюдением требований по обеспечению безопасности информации, которые применяются при обработке ПДн;

– разработки предложений по совершенствованию правовых, организационных, технических и иных мер по обработке и защите ПДн в НИЯУ МИФИ;

– построения комплексной системы обработки и защиты ПДн, в том числе при их обработке в информационных системах персональных данных (далее – ИСПДн) НИЯУ МИФИ и должна способствовать оптимизации затрат на ее построение.

1.4. Действие настоящей Политики распространяется на ПДн всех категорий субъектов ПДн, обработка которых осуществляется в НИЯУ МИФИ, а именно:

– работников, состоящих в трудовых отношениях с НИЯУ МИФИ;

– абитуриентов, участвующих в конкурсе на зачисление в НИЯУ МИФИ;

– слушателей, студентов, аспирантов, докторантов, соискателей (далее – обучающихся);

– членов диссертационных советов, членов ГЭК и ГАК;

– авторов охраняемых результатов интеллектуальной деятельности и средств индивидуализации;

– исполнителей по гражданско-правовым договорам, авторским договорам;

– посетителей НИЯУ МИФИ;

– физических лиц, пользующихся услугами НИЯУ МИФИ;

– физических лиц, вступающих в расчетно-финансовые отношения с НИЯУ МИФИ;

– иных физических лиц, которые обращаются с запросами в НИЯУ МИФИ.

2. ЦЕЛИ И ЗАДАЧИ ПОЛИТИКИ. ПРИНЦИПЫ ОБРАБОТКИ ПДН В НИЯУ МИФИ

2.1. Основные цели Политики:

– повышение доверия к НИЯУ МИФИ со стороны абитуриентов, обучающихся, работников НИЯУ МИФИ и иных лиц;

– обеспечение режима конфиденциальности ПДн, защиты от несанкционированного распространения;

– повышение стабильности функционирования НИЯУ МИФИ, а также обеспечение реализации уставных целей и осуществления направлений деятельности, указанных в Уставе НИЯУ МИФИ;

– содействие субъектам ПДн в осуществлении учебной, научной, трудовой и иной деятельности, обеспечение защиты прав и свобод субъектов ПДн НИЯУ МИФИ при обработке их ПДн, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну;

– регулирование отношений, связанных с обработкой ПДн субъектов ПДн, осуществляемой НИЯУ МИФИ;

– определение задач, принципов, условий и порядка обработки ПДн субъектов ПДн в НИЯУ МИФИ;

– обеспечение защиты прав и свобод субъектов ПДн при обработке их ПДн от несанкционированного доступа к ним;

– установление ответственности должностных лиц НИЯУ МИФИ за невыполнение требований норм, регулирующих обработку и защиту ПДн.

2.2. Основные задачи Политики:

– определение направлений деятельности НИЯУ МИФИ по обработке и защите ПДн абитуриентов, обучающихся, работников НИЯУ МИФИ и иных лиц;

– установление оптимальных требований по обеспечению защиты ПДн при их обработке с использованием средств автоматизации и без использования средств автоматизации;

– повышение эффективности мероприятий обработки и защиты ПДн.

2.3. Принципы обработки ПДн в НИЯУ МИФИ:

– обработка ПДн в НИЯУ МИФИ должна осуществляться в соответствии с действующим законодательством в сфере защиты ПДн, Уставом НИЯУ МИФИ, настоящей Политикой и иными локальными нормативными актами НИЯУ МИФИ;

– обработка ПДн должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка ПДн, несовместимая с целями сбора ПДн;

– не допускается объединение баз данных, содержащих ПДн, обработка которых осуществляется в целях, несовместимых между собой;

– обработке подлежат только ПДн, которые отвечают целям их обработки;

– содержание и объем обрабатываемых ПДн должны соответствовать заявленным целям обработки. Обрабатываемые ПДн не должны быть избыточными по отношению к заявленным целям их обработки;

– при обработке ПДн должны быть обеспечены точность ПДн, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки ПДн;

– НИЯУ МИФИ должно принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных;

– хранение ПДн должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом и (или) договором, стороной которого либо выгодоприобретателем по которому является субъект ПДн;

– обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

3. УСЛОВИЯ И ПОРЯДОК ОБРАБОТКИ ПДН В НИЯУ МИФИ

3.1. Обработка ПДн в НИЯУ МИФИ осуществляется с соблюдением принципов, определенных п. 2.3 настоящей Политики.

3.2. Обработка ПДн допускается в следующих случаях:

– обработка ПДн осуществляется с согласия субъекта ПДн на обработку его ПДн, за исключением случаев, определенных федеральными законами;

– обработка ПДн необходима для осуществления и выполнения функций, полномочий и обязанностей, возложенных на НИЯУ МИФИ законодательством Российской Федерации, Уставом НИЯУ МИФИ и (или) договором;

– обработка ПДн необходима для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица, подлежащих исполнению в соответствии с законодательством Российской Федерации об исполнительном производстве;

– обработка ПДн необходима для исполнения договора, стороной которого либо выгодоприобретателем по которому является субъект ПДн, а также для

заключения договора по инициативе субъекта ПДн или договора, по которому субъект ПДн будет являться выгодоприобретателем;

– обработка ПДн необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта ПДн, если получение согласия субъекта ПДн невозможно;

– обработка ПДн необходима для осуществления прав и законных интересов НИЯУ МИФИ или третьих лиц, либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта ПДн;

– обработка ПДн осуществляется в статистических или иных исследовательских целях, за исключением целей, указанных в статье 15 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», при условии обязательного обезличивания ПДн;

– осуществляется обработка ПДн, доступ неограниченного круга лиц к которым предоставлен субъектом ПДн, либо по его просьбе;

– осуществляется обработка ПДн, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральными законами.

3.3. Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни в НИЯУ МИФИ не производится.

3.4. Обработка персональных данных о судимости в НИЯУ МИФИ осуществляется в соответствии с законодательством Российской Федерации.

3.5. Обработка биометрических ПДн в НИЯУ МИФИ осуществляется с учетом требований, установленных статьей 10 и 11 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

3.6. НИЯУ МИФИ вправе поручить обработку ПДн другому лицу с согласия субъекта ПДн, если иное не предусмотрено федеральным законом, на основании заключенного с этим лицом договора.

3.7. НИЯУ МИФИ осуществляет обработку ПДн с использованием средств автоматизации и без использования средств автоматизации.

4. ОСНОВНЫЕ ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМЫ БЕЗОПАСНОСТИ ПДН

4.1. Законность. Предполагает осуществление защитных мероприятий и разработку системы безопасности ПДн НИЯУ МИФИ в соответствии с действующим законодательством в области защиты ПДн, а также других законодательных актов по безопасности информации Российской Федерации, 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 НИЯУ

МИФИ должны иметь представление об ответственности за правонарушения в области обработки ПДн.

4.2. Системность. 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 НИЯУ МИФИ, 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.

4.3. 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.

4.4. Непрерывность защиты. Для эффективного выполнения функций физических и технических средств защиты 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.

4.5. 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 ИСПДн в целом и их систем защиты, в частности. Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой ИСПДн. 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.

4.6. Преемственность и совершенствование. Предполагает постоянное совершенствование мер и средств защиты ПДн на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования ИСПДн НИЯУ МИФИ и системы ее защиты с учетом изменений в методах и средствах перехвата информации, нормативных

требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

4.7. 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. Используемые меры и средства обеспечения безопасности информационных ресурсов не должны заметно ухудшать эргономические показатели работы компонентов ИСПДн НИЯУ МИФИ. Излишние меры безопасности не должны приводить к экономической неэффективности, снижению эффективности работы персонала.

4.8. Персональная ответственность. Предполагает возложение ответственности за обеспечение безопасности ПДн и системы их обработки на каждого сотрудника в пределах его должностных обязанностей. 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.

4.9. Минимизация полномочий. Предполагает 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.

4.10. Исключение конфликта интересов. Предполагает четкое разделение обязанностей сотрудников и исключение ситуаций, когда сфера ответственности сотрудников допускает конфликт интересов. Сферы потенциальных конфликтов должны выявляться, минимизироваться и находиться под строгим независимым контролем.

4.11. **Гибкость системы защиты.** Система обеспечения информационной безопасности должна быть способна реагировать на изменения внешней среды и условий осуществления НИЯУ МИФИ своей деятельности. В число таких изменений входят:

– изменения организационной и штатной структуры НИЯУ МИФИ;

– изменение существующих или внедрение принципиально новых ИСПДн;

– новые технические средства и технологии.

4.12. Открытость алгоритмов и механизмов защиты. 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 разработчикам). Это, однако, не означает, что информация об используемых системах и механизмах защиты должна быть общедоступна.

4.13. Простота применения 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.

4.14. 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.

4.15. Специализация и профессионализм. Реализация административных мер и эксплуатация средств защиты должны осуществляться профессионально подготовленными специалистами НИЯУ МИФИ (ответственными за организацию обработки и защиты ПДн).

4.16. **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 И МЕТОДЫ ОБЕСПЕЧЕНИЯ ТРЕБУЕМОГО УРОВНЯ ЗАЩИТЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ

5.1. При обработке ПДн НИЯУ МИФИ должны приниматься необходимые правовые, организационные и технические меры для их защиты от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении них.

5.2. Обеспечение безопасности ПДн, обрабатываемых в НИЯУ МИФИ, должно достигаться:

– назначением ответственных лиц за организацию обработки и обеспечение безопасности ПДн в каждом подразделении НИЯУ МИФИ;

– полнотой, реальной выполнимостью и непротиворечивостью требований организационно-распорядительных документов НИЯУ МИФИ по вопросам обеспечения безопасности информации;

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

– персональной ответственностью за свои действия каждого сотрудника, в

рамках своих должностных обязанностей, имеющего доступ к информационным ресурсам НИЯУ МИФИ;

– осуществлением внутреннего контроля и/или аудита соответствия обработки ПДн в НИЯУ МИФИ Федеральному закону от 27 июля 2006 года № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите ПДн, локальным актам НИЯУ МИФИ не реже 1 раза в три года;

– ознакомлением абитуриентов, обучающихся, работников НИЯУ МИФИ, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе с требованиями к защите ПДн, локальными актами НИЯУ МИФИ в отношении обработки ПДн и/или обучением указанных сотрудников;

– оценкой эффективности принимаемых мер по обеспечению безопасности ПДн в НИЯУ МИФИ;

– выявлением фактов несанкционированного доступа к персональным данным и принятием соответствующих мер по их защите;

– восстановлением ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

5.3. При обработке ПДн в ИСПДн необходимый уровень защиты должен достигаться:

– строгим учетом всех подлежащих защите ресурсов ИСПДн НИЯУ МИФИ (информации, задач, документов, каналов связи, серверов, АРМ);

– наделением каждого сотрудника (пользователя) минимально необходимыми для выполнения им своих должностных обязанностей полномочиями по доступу к информационным ресурсам НИЯУ МИФИ;

– четким знанием и строгим соблюдением всеми пользователями ИСПДн НИЯУ МИФИ требований организационно-распорядительных документов по вопросам обеспечения безопасности информации;

– определением угроз безопасности ПДн при их обработке в ИСПДн;

– непрерывным поддержанием необходимого уровня защищенности элементов информационной среды НИЯУ МИФИ;

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

6. СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПДН

6.1. На технические средства защиты возлагается решение следующих основных задач:

– идентификация и аутентификация пользователей при помощи имен или специальных аппаратных средств;

– регламентация и управление доступом пользователей в помещения, к физическим и логическим устройствам;

– защита от проникновения компьютерных вирусов и разрушительного воздействия вредоносных программ;

– регистрация всех действий пользователя в защищенном журнале, наличие нескольких уровней регистрации;

– защита данных системы защиты на файловом сервере от доступа пользователей, в чьи должностные обязанности не входит работа с информацией, находящейся на нем.

6.2. В состав системы защиты должны быть включены следующие технические средства защиты:

– средства разграничения доступа к данным;

– средства регистрации доступа к компонентам ИСПДн и контроля за использованием информации;

– средства реагирования на нарушения режима информационной безопасности.

6.3. Технические средства разграничения доступа должны по возможности быть составной частью единой системы контроля доступа на контролируемую территорию, в отдельные помещения, к компонентам информационной среды НИЯУ МИФИ и элементам системы защиты ПДн (физический доступ), к информационным ресурсам (документам, носителям информации, файлам, наборам данных, архивам, справкам и т.д.), к активным ресурсам (прикладным программам, задачам и т.п.), к операционной системе, системным программам и программам защиты.

6.4. Средства обеспечения целостности должны включать средства резервного копирования, программы антивирусной защиты, программы восстановления целостности операционной среды и баз данных.

6.5. Средства оперативного контроля должны обеспечивать обнаружение и регистрацию всех событий (действий пользователей, попыток несанкционированного доступа и т.п.), которые могут повлечь за собой нарушение безопасности и привести к возникновению кризисных ситуаций.

6.6. Для своевременного выявления и предотвращения утечки ПДн за счет несанкционированного доступа, а также предупреждения возможных специальных воздействий, направленных на уничтожение ПДн, разрушение средств информатизации должен осуществляется контроль эффективности защиты ПДн, а также оценка эффективности мер защиты ПДн с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.

7. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЯ В ОБЛАСТИ ОБРАБОТКИ И ЗАЩИТЫ ПДН

7.1. Обязанности работников НИЯУ МИФИ, осуществляющих обработку и защиту ПДн, а также их ответственность, определяются должностными инструкциями и положениями о структурных подразделениях НИЯУ МИФИ

(для руководителей структурных подразделений), а также иными локальными нормативными актами НИЯУ МИФИ.

8. УТВЕРЖДЕНИЕ, ВВЕДЕНИЕ В ДЕЙСТВИЕ И ИЗМЕНЕНИЕ ПОЛИТИКИ

8.1. Настоящая Политика утверждается приказом ректора НИЯУ МИФИ.

8.2. НИЯУ МИФИ имеет право вносить изменения в настоящую Политику:

– по мере принятия новых нормативных правовых актов в сфере ПДн или внесения в них изменений;

– по мере принятия локальных нормативных актов НИЯУ МИФИ, регламентирующие организацию обработки и обеспечение безопасности ПДн.

8.3. Политика вступает в силу с момента ее утверждения приказом ректора и подлежит размещению на сайте НИЯУ МИФИ для обеспечения доступа к ней всех заинтересованных лиц.