МФТИ it
УПРАВЛЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Инструкция о порядке обеспечения конфиденциальности при обработке информации, содержащей персональные данные

1. Общие положения

1.1. Настоящая Инструкция устанавливает применяемые в МФТИ способы обеспечения безопасности при обработке, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, защиту, распространение (в том числе передачу), обезличивание, блокирование, уничтожение, персональных данных с целью соблюдения конфиденциальности сведений, содержащих персональные данные работников и обучающихся в МФТИ.

1.2. Настоящая Инструкция разработана на основании Конституции Российской Федерации, Трудового кодекса Российской Федерации, Федерального закона РФ от 27.07.2006 № 152-ФЗ «О персональных данных», постановлений Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Требования к защите персональных данных при их обработке в информационных системах персональных данных» и от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» и иных нормативных правовых актов Российской Федерации, а также «Положения об обработке персональных данных» МФТИ.

1.3. В соответствии с законодательством РФ под персональными данными понимается любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, необходимая институту в связи с трудовыми отношениями и организацией образовательного процесса.

1.4. Требование обеспечения конфиденциальности при обработке персональных данных означает обязательное для соблюдения должностными лицами института, допущенными к обработке персональных данных, иными получившими доступ к персональным данным лицами, требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

1.5. В целях обеспечения требований безопасности при обработке персональных данных Институт предоставляет должностным лицам, работающим с персональными данными, необходимые условия для выполнения указанных требований:

- знакомит работника под роспись с требованиями «Положения об обработке персональных данных МФТИ», с настоящей Инструкцией, с должностной инструкцией и иными локальными нормативными актами института в сфере обеспечения безопасности персональных данных;
- предоставляет хранилища для документов, учетные записи для доступа к информационным системам с обработкой персональных данных;
- обучает правилам эксплуатации средств защиты информации;
- проводит иные необходимые мероприятия.

1.6. Должностные лица Института, работающие с персональными данными, обязаны использовать информацию о персональных данных исключительно для целей, связанных с выполнением своих трудовых обязанностей.

1.7. Должностным лицам Института, работающим с персональными данными, запрещается сообщать их устно или письменно кому бы то ни было, если это не вызвано служебной необходимостью.

1.8. В случае прекращения исполнения должностных обязанностей, связанных с обработкой персональных данных, все носители информации, содержащие персональные данные (оригиналы и копии документов, машинные и бумажные носители и пр.), которые находились в распоряжении должностного лица в связи с выполнением должностных обязанностей, данный работник должен передать своему непосредственному руководителю.

1.9. Передача персональных данных третьим лицам допускается только в случаях, установленных законодательством РФ, в соответствии с «Положением об обработке персональных данных МФТИ», в соответствии с действующим регламентом подразделения (должностной инструкцией) и на основании письменного заявления субъекта персональных данных.

1.10. Передача персональных данных осуществляется ответственным за обработку персональных данных должностным лицом на основании письменного или устного распоряжения руководителя структурного подразделения.

1.11. Передача сведений и документов, содержащих персональные данные, оформляется путем составления акта по установленной настоящей форме.

1.12. Должностное лицо, предоставившее персональные данные третьим лицам, направляет письменное уведомление субъекту персональных данных о факте передачи его данных третьим лицам.

1.13. Запрещается передача персональных данных по телефону, факсу, электронной почте за исключением случаев, установленных законодательством и действующими в институте локальными нормативными актами.

1.14. Ответы на запросы граждан и организаций даются в том объеме, который позволяет не разглашать в ответах персональные данные, за исключением данных, содержащихся в материалах заявителя или опубликованных в общедоступных источниках.

1.15. Должностные лица Института, работающие с персональными данными, обязаны немедленно сообщать своему непосредственному руководителю, администратору информационной безопасности и начальнику административного отдела обо всех ставших им известными фактах получения третьими лицами несанкционированного доступа либо попытки получения доступа к персональным данным, об утрате или недостаче носителей информации, содержащих персональные данные, удостоверений, пропусков, ключей от сейфов (хранилищ), личных печатей, электронных ключей и других фактах, которые могут привести к несанкционированному доступу к персональным данным, а также о причинах и условиях возможной утечки этих сведений.

1.16. Должностные лица, осуществляющие обработку персональных данных, за невыполнение требований защиты персональных данных несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством РФ.

1.15. Порядок обеспечения безопасности при обработке персональных данных, осуществляемой без использования средств автоматизации регламентируется «Инструкцией по обработке персональных данных без использования средств автоматизации».

2. Порядок обеспечения безопасности при обработке персональных данных, осуществляемой с использованием средств автоматизации

2.1. Обработка персональных данных с использованием средств автоматизации означает совершение действий (операций) с такими данными с помощью в Информационных системах с обработкой персональных данных (далее ИСПДн), функционирующих на объектах вычислительной техники в Корпоративной сети передачи данных института (далее - КСПД).

2.2. Безопасность персональных данных при их обработке в ИСПДн обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации, разрабатываемые в соответствии с перечнем «Мер противодействия актуальным угрозам информационной безопасности в МФТИ», в соответствии с которым вводятся необходимые ограничения на доступ и передачу данных через Интернет, запуск приложений, запрет доступа к незарегистрированным внешним носителям данных и другие необходимые ограничения.

2.3. Технические и программные средства защиты информации должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации. Средства защиты информации, применяемые в КСПД, в установленном порядке проходят процедуру оценки соответствия.
За разработку, внедрение и эксплуатацию системы защиты персональных данных несёт ответственность начальник ОЭАСПС.

2.4. Информация, содержащая персональные данные, вводится для дальнейшей автоматизированной обработки в ИСПДн МФТИ. В случае производственной необходимости, с разрешения руководителя подразделения и согласования с администратором информационной безопасности МФТИ, персональные данные могут содержаться в компьютерных файлах, размещаемых в сетевых папках ограниченного доступа соответствующих подразделений.

2.5. Без согласования с руководителем структурного подразделения и администратором информационной безопасности создание и хранение баз данных, файловых папок, архивов и др., содержащих персональные данные, запрещается.

2.6. Запись, хранение и передача в установленном порядке персональных данных на внешних носителях допускается только в случае определения такого регламента в соответствующих должностных инструкциях подразделений с обязательным применением специально подготовленных и учтенных внешних носителей данных.

2.7. Доступ к персональным компьютерам и сетевым папкам, в которых содержатся файлы с персональными данными осуществляется с обязательным применением персонального корпоративного аккаунта, выдача которого производится в соответствии с «Положением об информационно-технологическом пространстве МФТИ».

2.8. Допуск лиц в информационные системы с обработкой персональных данных осуществляется в соответствии с «Регламентом о выдаче прав доступа в информационные системы» на основании заявок установленной формы.

2.9. Работа с персональными данными, содержащимися в информационных системах, осуществляется в строгом соответствии с регламентом обработки персональных соответствии в подразделении и должностной инструкцией, с которыми работник, в должностные обязанности которого входит обработка персональных данных, знакомится под роспись.

2.10. Работа с персональными данными должна быть организована таким образом, чтобы обеспечивалась сохранность носителей персональных данных и средств защиты информации, а также исключалась возможность неконтролируемого пребывания в этих помещениях посторонних лиц.

2.11. Пересылка персональных данных без использования специальных средств защиты по общедоступным сетям связи, в том числе Интернет, запрещается.

2.12. При обработке персональных данных в информационных системах пользователями должно быть обеспечено:

a) использование только предназначенных для этого каталогов (локальных или сетевых папок) или съемных маркированных носителей;
b) недопущение физического воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
c) постоянное использование антивирусного обеспечения для обнаружения зараженных файлов и незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним в соответствии с положением об антивирусной защите МФТИ
d) недопущение несанкционированных выноса из помещений, установки, подключения оборудования, а также самостоятельного удаления, инсталляции или настройки программного обеспечения.

2.13. При обработке персональных данных в информационных системах разработчиками и администраторами информационных систем должны обеспечиваться:

a) обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;
b) учет лиц, допущенных к работе с персональными данными в информационных системах, их прав и ролей доступа;
c) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;
d) контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией.

3. Порядок учета, хранения и обращения со съемными носителями персональных данных, твердыми копиями и их утилизации

3.1. Все находящиеся на хранении и в обращении в институте съемные носители (диски, дискеты, USB флеш-накопители, пр.), содержащие персональные данные, подлежат учёту. Каждый съемный носитель с записанными на нем персональными данными должен иметь этикетку, на которой указывается его уникальный учетный номер.

3.2. Учет и выдачу съемных носителей персональных данных осуществляет администратор информационной безопасности (при его отсутствии - начальник ОЭАСПС).
Работники института получают учтенный съемный носитель для выполнения работ на конкретный срок.
При получении делаются соответствующие записи в журнале учета съемных носителей персональных данных (далее - журнал учета), который ведется в ОЭАСПС.
По окончании работ пользователь сдает съемный носитель для хранения администратору информационной безопасности, о чем делается соответствующая запись в журнале учета.

3.3. При работе со съемными носителями, содержащими персональные данные, запрещается:

- хранить съемные носители с персональными данными вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;
- выносить съемные носители с персональными данными из служебных помещений для работы с ними на дому, в гостиницах и т.д.

3.4. При отправке или передаче персональных данных адресатам на съемные носители записываются только предназначенные адресатам данные. Отправка персональных данных адресатам на съемных носителях осуществляется в порядке, установленном для документов для служебного пользования. Вынос съемных носителей персональных данных для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя структурного подразделения института.

3.5. О фактах утраты съемных носителей, содержащих персональные данные, либо разглашения содержащихся в них сведений должно быть немедленно сообщено руководителю структурного подразделения, начальнику административного отдела, администратору ИБ.
На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы учета.

4. Заключительные положения

4.1. С положениями настоящей Инструкции должны быть ознакомлены под роспись все работники структурных подразделений Института и лица, выполняющие работы по договорам, имеющие отношение к обработке персональных данных. Ответственные за инструктаж – Администраторы информационных систем, в которых обрабатываются персональные данные.