Приложение 10

УТВЕРЖДЕНО
приказом ГАОУ ВО МИОО
от 25.10.2017 № 406/ОД

ПОЛОЖЕНИЕ
ПО ОРГАНИЗАЦИИ И ПРОВЕДЕНИЮ РАБОТ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ГОСУДАРСТВЕННОМ АВТОНОМНОМ ОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ ВЫСШЕГО ОБРАЗОВАНИЯ ГОРОДА МОСКВЫ «МОСКОВСКИЙ ИНСТИТУТ ОТКРЫТОГО ОБРАЗОВАНИЯ»

Москва, 2017 г

СОДЕРЖАНИЕ

1. НАЗНАЧЕНИЕ И ОБЛАСТЬ ДЕЙСТВИЯ

1.1. Настоящее Положение предназначено для организации в Государственном автономном образовательном учреждении высшего образования города Москвы «Московский институт открытого образования» (далее – Институт) процесса обеспечения безопасности ПДн согласно требованиям действующего федерального законодательства.

1.2. Действие настоящего Положения распространяется на все процессы Института по сбору, записи, систематизации, накоплению, хранению, уточнению, извлечению, использованию, передаче (распространению, предоставлению, доступу), обезличиванию, блокированию, удалению, уничтожению ПДн, осуществляемые с использованием средств автоматизации и без их использования.

1.3. Положение обязательно для ознакомления и исполнения всеми работниками Института.

1.4. Основными нормативно-правовыми и методическими документами, на которых базируется настоящее Положение, являются:

– Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», устанавливающий основные принципы и условия обработки ПДн, права, обязанности и ответственность участников отношений, связанных с обработкой ПДн;

– «Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденные Постановлением Правительства РФ от 01.11.2011 № 1119;

– «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденные приказом ФСТЭК России от 18.02.2013 № 21.

1.5. Настоящий документ является локальным нормативным Института и не подлежит представлению другим сторонам без согласования с руководством Института.

2. ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И СОКРАЩЕНИЯ

В настоящем документе использованы следующие термины и определения:

Персональные данные (ПДн) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Субъект персональных данных – физическое лицо.

Оператор – лицо, самостоятельно или совместно с другими лицами организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели обработки персональных данных; состав персональных данных, подлежащих обработке; действия (операции), совершаемые с персональными данными.

Обработка персональных данных – 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.

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

Уничтожение персональных данных – 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.

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

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

Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе.

Ответственный за организацию обработки ПДн – работник Института, назначенный приказом руководителя Института ответственным за организацию обработки персональных данных в Институте (в обязанности входят организация и проведение мероприятий по обеспечению соответствия процессов обработки ПДн законодательным требованиям, обработки обращений субъектов ПДн и запросов уполномоченного органа по защите прав субъектов ПДн). Кроме того, в обязанности этого работника входит организация и проведение контрольных мероприятий порядка обработки и защиты ПДн.

ФСТЭК – Федеральная служба по техническому и экспортному контролю.

ФСБ – Федеральная служба безопасности.

3. ОБЯЗАТЕЛЬНЫЕ МЕРОПРИЯТИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИСПДН

3.1. Общие требования

3.1.1. В Институте до начала проведения работ по обеспечению безопасности ПДн должна быть проведена инвентаризация ИСПДн путем опроса владельцев автоматизированных систем на предмет наличия обработки в них ПДн.

3.1.2. Для каждой ИСПДн разрабатывается Модель угроз в соответствии с:

– нормативно-методическими документами ФСТЭК России «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» и «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», если в ИСПДн не используются криптографические средства защиты;

– нормативно-методическим документом ФСБ России «Методические рекомендации по обеспечению с помощью криптографических средств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», если в ИСПДн используются криптографические средства защиты.

3.1.3. Для всех эксплуатируемых ИСПДн должен быть определен уровень защищенности ПДн в соответствии с Постановлением Правительства РФ от 01.11.2011 № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных». Определение уровня защищенности ИСПДн проводится в следующей последовательности:

– приказом руководителя Института создается Комиссия по определению уровней защищенности ПДн (далее - комиссия), которые необходимо обеспечить при обработке в ИСПДн;

– комиссия в определенный приказом срок устанавливает категории и объем обрабатываемых ПДн в ИСПДн, тип угроз безопасности ПДн, характерных для ИСПДн (на основании разработанных Моделей угроз);

– комиссия формирует акты определения уровня защищенности для каждой ИСПДн.

3.1.4. Выбор методов и способов защиты информации в ИСПДн осуществляются на основе Модели угроз и в зависимости от уровней защищенности ПДн, которые необходимо обеспечить при обработке в ИСПДн.

3.1.5. Выбранные методы и способы защиты ПДн в ИСПДн должны обеспечивать нейтрализацию актуальных угроз безопасности ПДн при их обработке в ИСПДн в составе создаваемой системы защиты ПДн.

3.1.6. В соответствии с выбранными методами и способами защиты ПДн проектируется и внедряется система защиты ПДн.

3.1.7. Для проведения работ по выбору и реализации методов и способов защиты ПДн (включая техническое проектирование системы защиты ПДн, внедрение средств защиты ПДн, сопровождение средств защиты ПДн и т. д.) могут привлекаться подрядные организации, имеющие лицензию на осуществление деятельности по технической защите конфиденциальной информации.

3.2. Требования к разрабатываемым и вводимым в эксплуатацию ИСПДн

3.2.1. Разработка ИСПДн должна включать следующие стадии:

– предпроектная стадия (включает предварительный анализ целей и условий функционирования ИСПДн, а также обрабатываемых в ней ПДн; на основании этого анализа определяется предварительный уровень защищенности ПДн, степень участия должностных лиц, актуализируются угрозы безопасности);

– стадия проектирования системы защиты ПДн для ИСПДн;

– стадия ввода в эксплуатацию ИСПДн.

3.2.2. По результатам проведенного анализа и с учетом действующих требований федерального законодательства и регуляторов должны быть разработаны:

– Модель угроз безопасности персональных данных при их обработке в ИСПДн;

– Модель нарушителя безопасности персональных данных при их обработке в ИСПДн (если планируется использование средств криптографической защиты);

– Требования к защите персональных данных при их обработке в ИСПДн;

– Акт определения уровня защищенности ПДн при их обработке в ИСПДн.

3.2.3. Проектирование системы защиты ПДн для вводимой в эксплуатацию ИСПДн должно производиться с учетом уже построенной в Институте системы защиты ПДн, включающей комплекс организационных и технических мер.

3.2.4. На стадии ввода в эксплуатацию ИСПДн должны быть проведены, как минимум, следующие мероприятия:

– установка пакета прикладных программ ИСПДн совместно со средствами защиты информации (встроенными и наложенными);

– опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПДн;

– приемо-сдаточные испытания средств защиты информации по результатам опытной эксплуатации.

3.2.5. Перед вводом новой ИСПДн в опытную эксплуатацию должен быть составлен Акт определения уровня защищенности ИСПДн (Приложение 1).

3.2.6. После вывода ИСПДн из эксплуатации должна быть переведена в архивный фонд Института (в соответствии с ч. 2 ст. 13 ФЗ «Об архивном деле»), при этом должны быть выполнены следующие требования:

– доступ к архивной ИСПДн и хранимым в ней документам должен обеспечиваться на основании соответствующей заявки (Приложение 2), согласованной с непосредственным руководителем лица, запрашивающего доступ и утверждаемой ответственным за организацию обработки персональных данных;

– ПДн, содержащиеся в архивных ИСПДн, могут быть использованы и переданы третьим лицам только в целях исполнения законодательства Российской Федерации;

– должны быть обеспечены финансовые, материально-технические и иные условия, необходимые для комплектования, хранения, учета и использования ИСПДн, включая специальное помещение, отвечающее нормативным условиям труда работников архива;

– доступ в помещения, где предполагается хранение технических и программных средств выводимой из эксплуатации ИСПДн, должен быть ограничен;

– все персональные данные, содержащиеся на отчуждаемых носителях, должны уничтожаться при извлечении носителей из состава ИСПДн;

– должен быть регламентирован перечень лиц, допущенных к работе с ИСПДн, переданных в архив;

– все внешние запоминающие устройства (ленты с резервными копиями, дискеты, CD-диски, флеш-накопители и т. п.), относящиеся к архивной ИСПДн, должны храниться в сейфах.

3.2.7. При передаче технических средств ИСПДн на ремонт или гарантийное обслуживание все данные, содержащиеся на машинных носителях информации, должны быть уничтожены способом, обеспечивающим гарантированное уничтожение информации.

4. ОБЕСПЕЧЕНИЕ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ПДН

4.1. Общие требования

4.1.1. Обеспечение безопасности ПДн при их обработке в ИСПДн должно осуществляться на всех стадиях жизненного цикла ИСПДн и состоять из согласованных мероприятий, направленных на предотвращение (нейтрализацию) и устранение угроз безопасности ПДн в ИСПДн, минимизацию возможного ущерба, а также на восстановление данных и нормальное функционирование ИСПДн в случае реализации этих угроз.

4.1.2. В целях защиты ПДн от несанкционированного доступа и иных неправомерных действий мероприятия по организации и обеспечению технической защиты ПДн для каждой ИСПДн должны включать:

– выявление актуальных угроз безопасности ПДн на основе анализа ИСПДн и актуализации Модели угроз безопасности ПДн;

– определение уровня защищенности ПДн при их обработке в ИСПДн на основании установленных критериев в соответствии с Постановлением Правительства РФ от 01.11.2011 № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– выбор и реализацию методов и способов защиты информации в информационной системе на основе Моделей угроз и нарушителей безопасности ПДн и в зависимости от уровня защищенности ПДн, который необходимо обеспечить при их обработке в ИСПДн;

– внедрение соответствующих программных, аппаратных и программно-аппаратных средств защиты информации.

4.1.3. Защита ПДн, обрабатываемых в ИСПДн, от несанкционированного доступа и иных неправомерных действий должна осуществляться в Институте следующими методами и способами:

– реализация разрешительной системы допуска пользователей (обслуживающего персонала) к информационным ресурсам ИСПДн и связанным с ее использованием работам, документам;

– ограничение доступа в помещения, где размещены технические средства, ИСПДн, а также носители информации, содержащие ПДн;

– разграничение доступа пользователей (обслуживающего персонала) к информационным ресурсам (включая ПДн), программным средствам обработки и защиты ПДн;

– регистрация действий пользователей (обслуживающего персонала) ИСПДн, мониторинг попыток несанкционированного доступа;

– учет и хранение носителей информации содержащих ПДн, их обращение, исключающее хищение, подмену и уничтожение;

– резервирование технических средств, дублирование массивов и носителей содержащих ПДн;

– использование защищенных каналов связи для передачи ПДн;

– размещение технических средств ИСПДн, позволяющее осуществлять обработку ПДн в пределах контролируемой территории;

– периодический анализ защищенности ИСПДн, предполагающий применение специализированных программных средств (сканеров безопасности);

– предотвращение внедрения в ИСПДн вредоносных программ (программ-вирусов) и программных закладок;

– регистрация событий и мониторинг процессов обработки ПДн;

– использование средств антивирусной защиты;

– централизованное управление системой защиты ПДн.

4.1.4. При организации взаимодействия ИСПДн с информационно-телекоммуникационными сетями международного информационного обмена (Интернет) наряду с указанными методами и способами должны применяться следующие дополнительные методы и способы защиты ПДн от несанкционированного доступа:

– межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры ИСПДн;

– защита ПДн при их передаче по каналам связи.

4.1.5. В Институте также могут разрабатываться и применяться другие методы защиты информации от несанкционированного доступа, обеспечивающие нейтрализацию угроз безопасности ПДн.

4.1.6. Конкретные методы и средства защиты ПДн в ИСПДн должны определяться на основании нормативно-методических документов ФСТЭК России и ФСБ России, исходя из уровня защищенности ИСПДн и актуальных угроз безопасности ПДн.

4.1.7. Должен осуществляться учет технических средств защиты информации, ответственность возлагается на ответственного за обеспечение безопасности ПДн. Приложение 3 содержит форму журнала учета технических средств защиты информации.

5. ПРОВЕДЕНИЕ КОНТРОЛЬНЫХ МЕРОПРИЯТИЙ

5.1. Ответственный за организацию обработки ПДн на периодической основе организуют проведение внутреннего контроля соблюдения порядка обработки и обеспечения безопасности ПДн.

5.2. Контрольные мероприятия по обеспечению безопасности ПДн должны включать:

– проверку деятельности работников Института, допущенных к работе с ПДн, на соответствие порядку обработки и обеспечения безопасности ПДн, установленному настоящим Положением, Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» и другими нормативными правовыми актами;

– проверку состояния защищенности ПДн, обрабатываемых в ИСПДн, включая выполнение требований по защите каждой конкретной ИСПДн, корректности работы системы защиты ПДн, контроль состава технических средств, программного обеспечения и средств защиты информации ИСПДн и т. д.

5.3. По результатам проведенных проверок формируется отчет, предоставляемый для анализа руководителю Института.

5.4. При необходимости должны быть предложены меры по минимизации последствий выявленных угроз ИБ.

6. ОБЕСПЕЧЕНИЕ ФИЗИЧЕСКОЙ ЗАЩИТЫ ПДН

6.1. Для минимизации риска несанкционированного доступа к ПДн, а также нарушения их конфиденциальности и целостности применяются методы контроля физического доступа и защиты от воздействия окружающей среды.

6.2. Доступ в помещения, в которых размещены компоненты информационной инфраструктуры, обрабатывающие, хранящие и передающие ПДн, должен быть ограничен. Доступ в данные помещения может быть предоставлен сотрудникам Института и представителям третьих сторон только для выполнения должностных или договорных обязанностей.

6.3. В Институте должен быть установлен пропускной режим, обеспечивающий контроль доступа сотрудников и посетителей на территорию Института.

6.4. Все устройства, хранящие, передающие и обрабатывающие ПДн, должны быть размещены в охраняемых помещениях.

6.5. Устройства вывода (отображения) информации должны быть установлены способом, исключающим несанкционированный просмотр информации.

Приложение 1
к Положению по организации и
проведению работ по обеспечению
безопасности ПДн при их обработке

А К Т
определения уровня защищенности ПДн при их обработке в ИСПДн «_____»

В соответствии с Постановлением Правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» от 01.11.2012 №1119 и приказом по ГАОУ ВО МИОО от «____» _____ 201_ г., Комиссия в составе:
председателя _____
и членов:

1) _____;
2) _____;
3) _____;

произвела определение уровня защищенности ПДн, обрабатываемых в информационной системе персональных данных «_____».

Выявлены следующие характеристики системы:

Категория обрабатываемых персональных данных	
Объем обрабатываемых персональных данных	
Структура информационной системы	
Наличие подключений информационной системы к сетям общего пользования и (или) сетям международного информационного обмена	
Режим обработки персональных данных	
Режим разграничения прав доступа пользователей	
Местонахождение технических средств информационной системы	
Тип актуальных угроз безопасности персональных данных	

По результатам анализа исходных данных и Модели угроз необходимо обеспечить __-й уровень защищенности персональных данных при их обработке в информационной системе «_____».

Председатель комиссии:
Члены комиссии:

Приложение 2
к Положению по организации и
проведению работ по обеспечению
безопасности ПДн при их обработке

СОГЛАСОВАНО
_____
(должность)
_____ *(И.О. Фамилия)*
«____»_____2016 г.

УТВЕРЖДАЮ
_____
(должность)
_____ *(И.О. Фамилия)*
«____»_____2016 г.

Заявка
на предоставление доступа к архивной ИСПДн
и хранимым в ней документам

Прошу предоставить
_____
(должность, наименование структурного подразделения, фамилия, имя, отчество)
_____

доступ к архивной ИСПДн «_____» и хранимым в ней данным.

Необходимость предоставления доступа обусловлена следующими задачами:
_____
_____
_____

«____» _____ 201_ г.

_____/_____
(подпись) *(инициалы, фамилия)*

Приложение 3
к Положению по организации и
проведению работ по обеспечению
безопасности ПДн при их обработке

ЖУРНАЛ
учета технических средств защиты информации

№ п/п	Тип СЗИ	Наименование СЗИ	Индекс или условное наименование* (для сертифицированных СЗИ)	Регистрационный номер* (для сертифицированных СЗИ)	ИСПДн, в которой(ых) применяется СЗИ	Наличие и место хранения документации
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						

* Перечень индексов, условных наименований и регистрационных номеров определяется ФСТЭК России и ФСБ России в пределах их полномочий.