Приложение 3

УТВЕРЖДЕНО
приказом ГАОУ ВО МИОО
от 25.10.2017 № 406/ОД

ПОРЯДОК КОНТРОЛЯ ПРОЦЕССОВ ОБРАБОТКИ И ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ГОСУДАРСТВЕННОМ АВТОНОМНОМ ОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ ВЫСШЕГО ОБРАЗОВАНИЯ ГОРОДА МОСКВЫ «МОСКОВСКИЙ ИНСТИТУТ ОТКРЫТОГО ОБРАЗОВАНИЯ»

Москва, 2017 г.

СОДЕРЖАНИЕ

1. ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

ИСПДн – информационная система персональных данных.

Институт – Государственное автономное образовательное учреждение высшего образования города Москвы «Московский институт открытого образования».

ПДн – персональные данные.

СЗИ – средства защиты информации.

2. НАЗНАЧЕНИЕ И ОБЛАСТЬ ПРИМЕНЕНИЯ

2.1. Настоящий Порядок контроля процессов обработки и обеспечения безопасности персональных данных в Государственном автономном образовательном учреждении высшего образования города Москвы «Московский институт открытого образования» (далее – Порядок) определяет порядок проведения проверочных мероприятий по контролю за принимаемыми мерами по обеспечению безопасности ПДн и поддержанию необходимого уровня защищённости ИСПДн.

2.2. Действие Порядка распространяется на все подразделения Института, включая его обособленные и внутренние структурные подразделения.

3. 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).

Оператор – Государственное автономное образовательное учреждение высшего образования города Москвы «Московский институт открытого образования», самостоятельно или совместно с другими лицами организующий и (или) осуществляющий обработку персональных данных, а также определяющие 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.

Ответственный за организацию обработки ПДн – работник Института, назначенный приказом ректора Института ответственным за организацию обработки персональных данных в Институте (в обязанности входят организация и проведение мероприятий по обеспечению соответствия процессов обработки ПДн законодательным требованиям, обработке обращений субъектов ПДн и запросов уполномоченного органа по защите прав субъектов ПДн).

Офицер ИБ – работник Института, назначенный приказом ректора Института на роль ответственного за обеспечение информационной безопасности в Института, в том числе безопасности персональных данных.

4. ПОРЯДОК КОНТРОЛЯ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. В целях поддержания необходимого уровня защищённости ПДн, предотвращения возможных неправомерных действий с ПДн и своевременного реагирования на нарушения установленного порядка обработки ПДн в Институте на регулярной основе должны проводиться контрольные мероприятия (проверки).

4.2. Контрольные мероприятия (проверки) проводятся на плановой основе, а также при необходимости - внепланово.

4.3. Решение о необходимости проведения внеплановых контрольных мероприятий принимает обеспечение безопасности ПДн в Институте. Данное решение может быть обосновано возросшими рисками информационной безопасности для обрабатываемых ПДн или же существенными изменениями в среде обработки ПДн.

4.4. Контрольные мероприятия (проверки) организуются офицером ИБ.

4.5. Плановые проверки включают в себя следующие типы проверок:

– оценка соответствия процессов обработки и обеспечения безопасности ПДн в Институте требованиям, установленным законодательством и подзаконными актами РФ, а также локальными нормативными актами Института, регламентирующими обработку ПДн;

– проверку деятельности сотрудников Института, допущенных к работе с ПДн в ИСПДн, на соответствие порядку обработки и обеспечения безопасности ПДн, установленному Положением об обработке персональных данных и другими нормативными документами;

– проверку правильности приема и обработки обращений и запросов субъектов ПДн или их представителей;

– проверку работоспособности и эффективности технических средств ИСПДн и средств защиты ПДн;

– проверку работоспособности средств восстановления технических средств ИСПДн и средств защиты ПДн и резервных копий;

– проверку соответствия предоставленных прав доступа пользователей к ПДн утвержденной матрице доступа;

– проверку настроек парольной политики;

– проверку отсутствия на АРМ пользователей средств разработки;

– проверку отсутствия на АРМ пользователей нештатного ПО;

– оценку знаний сотрудников в части правил обработки ПДн.

4.6. Ответственный за обеспечение безопасности ПДн составляет план контрольных мероприятий на год, в котором определяет состав и периодичность проведения проверок на данный период времени (Приложение 1).

4.7. План контрольных мероприятий утверждает ректор Института.

4.8. Результаты проверок оформляются актами (Приложение 2).

4.9. Выявленные в ходе проверок нарушения, а также отметки об их устранении фиксируются в журнале учета выявленных нарушений в порядке обработки и обеспечения безопасности персональных данных (Приложение 3).

4.10. Выявленные нарушения расследуются в соответствии с Инструкцией о порядке проведения разбирательств по фактам нарушений порядка обработки и защиты персональных данных, приводящих к снижению уровня защищенности персональных данных.

Приложение 1
к Порядку контроля процессов
обработки и обеспечения
безопасности персональных данных

ПЛАН КОНТРОЛЬНЫХ МЕРОПРИЯТИЙ

УТВЕРЖДАЮ
Ректор ГАОУ ВО МИОО
_____ *И. О. Фамилия*
«__» _____20___г.

№ п/п	Тип мероприятия	Объекты и деятельность, подвергающиеся контролю	Периодичность проведения мероприятия/дата проведения мероприятия	Сроки проведения мероприятия	Перечень документов, на основании которых проводится проверка	Отчётные материалы
1.						

Приложение 2
к Порядку контроля процессов
обработки и обеспечения
безопасности персональных данных

АКТ №_____
о результатах проведения проверки

_____
(область проверки)

в

_____
(название структурного подразделения)

Государственного автономного образовательного учреждения высшего образования города Москвы «Московский институт открытого образования».

В ходе проведения проверки было установлено, что _____
_____
_____
_____

Выявлены следующие нарушения:
_____
_____
_____

Ответственным за устранение нарушений назначен:
_____

Ответственный за организацию обработки ПДн _____
(подпись, ФИО)

_____
(дата)

Приложение 3
к Порядку контроля процессов
обработки и обеспечения
безопасности персональных данных

ЖУРНАЛ
учета выявленных нарушений в порядке обработки
и обеспечения безопасности персональных данных

Журнал начат «____» _____201__ г.
Должность_____
_____ / *И. О. Фамилия* /

Журнал завершен «____» _____201__ г.
Должность_____
_____ / *И. О. Фамилия* /

На _____ листах

№ п/п	Сведения о проведении проверки, в ходе которой выявлено нарушение	Описание нарушения	Ответственный за устранение нарушения	Отметка об устранении нарушения	Дата	Подпись ответственного лица	Примечание