МОСКОВСКИЙ ИНСТИТУТ ТЕХНОЛОГИЙ И УПРАВЛЕНИЯ

MOSCOW INSTITUTE OF TECHNOLOGY AND MANAGEMENT

ПРИКАЗ

г. Москва

«28» октября 2022 г. № 3-ПД

Об утверждении Плана мероприятий по обеспечению Безопасности персональных данных, Перечня мероприятий по защите персональных данных – утверждении Положения о порядке реагирования на инциденты информационной безопасности в информационных системах персональных данных, О назначении Администратора информационной безопасности в Образовательной автономной некоммерческой организации высшего образования «Московский институт технологий и управления» (далее- ОАНО ВО «МИТУ»)

В целях исполнения требований Федерального закона от 27 июля 2006 года № 152-ФЗ "О персональных данных", Постановления Правительства Российской Федерации от 21 марта 2012 года № 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных", **приказываю:**

1. Утвердить Перечень мероприятий по защите персональных данных в ОАНО ВО «МИТУ».
2. Утвердить Положение о порядке реагирования на инциденты информационной безопасности в информационных системах персональных данных.
3. Назначить Администратором информационной безопасности в ОАНО ВО «МИТУ»– Румянцева Льва Александровича.
4. Возложить на Румянцева Льва Александровича следующие обязанности:

- создание условий для осуществления своевременного обнаружения и оперативного реагирования на Инциденты информационной безопасности, в том числе их закрытия;
- предотвращение и (или) снижение негативного влияния Инцидентов информационной безопасности на осуществление технологических процессов ОАНО ВО «МИТУ»; оперативное совершенствование системы обеспечения информационной безопасности ОАНО ВО «МИТУ».

5. Администратору информационной безопасности обеспечить размещение настоящего приказа и утвержденных Положений на сайте ОАНО ВО «МИТУ».
6. Контроль исполнения Приказа возложить на Ректора – Бородину М.И.

Приложение:

1. Перечень мероприятий по защите персональных данных в ОАНО ВО МИТУ.
2. Положение о порядке реагирования на инциденты информационной безопасности в информационных системах персональных данных.

Ректор
ОАНО ВО «МИТУ» Бородина М.И.

Приложение 1
к приказу ОАНО ВО «МИТУ»
от 28 октября 2022 г. № 3-ПД

План
Мероприятий по обеспечению безопасности персональных данных

1. Общие положения

План мероприятий по обеспечению защиты персональных данных (далее - План мероприятий) содержит необходимый перечень мероприятий для обеспечения защиты персональных данных в ОАНО ВО «МИТУ».

План мероприятий составлен на основании списка мер, методов и средств защиты, определенных в Политике в отношении обработки персональных данных.

Выбор конкретных мероприятий осуществляется на основании анализа Отчета о результатах обследования ИСПДн и Модели угроз безопасности.

В План мероприятий включены следующие категории мероприятий:

- организационные (административные);
- физические;
- технические (аппаратные и программные);
- контролирующие.

В План мероприятий включена следующая информация:

- название мероприятия;
- исполнитель мероприятия/ответственный за исполнение;
- итог выполнения мероприятия.

Меры (мероприятия) по защите персональных данных

Любое юридическое лицо в силу требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» обязано принимать меры по защите персональных данных, при этом перечень таких мер оно вправе определять самостоятельно.

Мероприятия по защите персональных данных можно разделить на две большие подгруппы: по внутренней и внешней защите персональных данных.

К мерам по внутренней защите персональных данных относятся следующие действия:

- ограничение числа работников (с регламентацией их должностей), которым открыт доступ к персональным данным. Кого может включать этот перечень? Абсолютно всех, кто имеет доступ к личным делам, т.е. сотрудников отделов кадров или ответственных за кадровое делопроизводство, работников бухгалтерии, секретарей-делопроизводителей, специалистов, которые заключают договоры с физическими лицами, а также инженеров, программистов, юристов;
- назначение ответственного лица, обеспечивающего исполнение организацией законодательства в рассматриваемой сфере;
- утверждение перечня документов, содержащих персональные данные;
- издание внутренних документов по защите персональных данных, осуществление контроля за их соблюдением;
- ознакомление работников действующими нормативами в области защиты персональных данных и локальными актами; проведение систематических проверок соответствующих знаний работников, обрабатывающих персональные данные, и соблюдения ими требований нормативных документов по защите конфиденциальных сведений. Следует иметь в виду, что все сотрудники, которые имеют доступ к персональным данным других людей, должны быть ознакомлены с особенностями законодательства в области защиты персональных данных;
- рациональное размещение рабочих мест для исключения несанкционированного использования защищаемой информации;

- утверждение списка лиц, имеющих право доступа в помещения, в которых хранятся персональные данные;

- утверждение порядка уничтожения информации;

- выявление и устранение нарушений требований по защите персональных данных;

- проведение профилактической работы с сотрудниками по предупреждению разглашения ими персональных данных.

Меры (мероприятия) по внешней защите персональных данных:

- введение пропускного режима, порядка приема и учета посетителей;

- внедрение технических средств охраны, программных средств защиты информации на электронных носителях и др.

Несмотря на то, что законом не установлены конкретные требования к количеству и содержанию локальных актов, принимаемых в организации по вопросам обработки и защиты персональных данных, практика реализации данного нормативного акта сформировала необходимый минимум документов, которые должны быть разработаны в учреждении:

- общий документ, определяющий политику организации в отношении обработки персональных данных, например Политика обработки в отношении персональных данных;

- список лиц, обрабатывающих персональные данные;

- приказ о назначении сотрудника, ответственного за организацию обработки персональных данных. Указанное лицо должно осуществлять внутренний контроль за соблюдением организацией и ее работниками законодательства о персональных данных, в том числе требований к их защите, доводить до сведения персонала положения законодательства о персональных данных, локальных актов по вопросам их обработки, а также требования к защите таких данных, организовывать прием и обработку обращений и запросов субъектов персональных данных и (или) контролировать прием и обработку таких обращений и запросов;

- положение о правовых, организационных и технических мерах защиты персональных данных от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении персональных данных. В данном положении прописаны конкретные меры по защите персональных данных (введение пропускного режима, применение программных средств защиты информации - паролей, антивирусных программ, хранение персональных данных обособленно от других сведений, на отдельных материальных носителях и в специально оборудованных помещениях с ограниченным доступом и т. д.);

- локальный акт, устанавливающий процедуры, направленные на предотвращение и выявление нарушений законодательства в сфере защиты персональных данных, устранение последствий таких нарушений. Так, в компании могут быть разработаны план мероприятий по внутреннему контролю безопасности персональных данных, инструкция о порядке проведения служебного расследования по фактам нарушений законодательства в сфере защиты персональных данных, вестись журнал антивирусных проверок и контроля работы с персональными данными, журнал обучения, инструктажа и аттестации по вопросам защиты персональных данных.

2. План мероприятий по обеспечению безопасности ПДн (организационные меры)

№ п/п	Мероприятие	Исполнитель	Итог выполнения мероприятия
1	Утвердить и ознакомить под роспись работников с разработанными организационно-распорядительными документами.	Ответственный за организацию Обработки персональных данных	Выполнение требований ФЗ-152, Постановление Правительства РФ от 15 сентября 2008 г. № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации", требований Постановление Правительства РФ № 1119
2	Добавить пункт о соблюдении конфиденциальности в трудовые договора. Заключить дополнительные соглашения с физическими лицами, в части соблюдения конфиденциальности и обеспечения безопасности персональных данных по приведенному в документах примеру.		Приведение договоров с третьими лицами в соответствие с требования ФЗ
3	При необходимости, заключить дополнительные соглашения с организациями, имеющие доступ к БД ИСПДн - в части соблюдения конфиденциальности и обеспечения безопасности персональных данных по приведенному в документах примеру		Приведение договоров с третьими лицами в соответствие с требования ФЗ-152
4	Получить согласия на, обработку персональных данных сотрудников. Добавить пункт о согласии на обработку ПДн для сбора данных через сайт (Отдельные документы)		Выполнение требований ФЗ-152
5	Оформить с работниками, осуществляющими обработку персональных данных по форме Приложения Приказа «Об организации мероприятий по защите		Выполнение требований ФЗ-152

	персональных данных» обязательствам неразглашении персональных данных		
6	Копию «Политики в отношении обработки персональных» разместить на официальном сайте, в приемной в общедоступном месте.		Выполнение требований ФЗ-152
7	Организовать рассмотрение запросов субъектов ПДн и их законных представителей в соответствие с Приложением Приказа «Об организации мероприятий по защите персональных данных»		Выполнение требований ФЗ-152
8	По номенклатуре дел определить документы, у которых истек срок хранения, уничтожить их составив Акт об уничтожении - Приложение Типовая форма акта об уничтожении ПДн Приказа «Об организации мероприятий по защите персональных данных»		Приведение в соответствие с требования ФЗ-152 Акты уничтожение носителей ПДн Выполнение требований Постановление Правительства РФ № 687
9	Создать комиссию и утвердить «Акт определения уровня защищенности персональных данных при их обработке в информационной системе»	Оператор ПДн	Выполнение требований 1111 РФ № 1119; Акты определения уровня защищенности персональных данных при их обработке в информационной системе
10	Подписать и направить нарочно или почтовым отправлением Уведомление (изменение в уведомление) об обработке персональных данных в территориальный орган Роскомнадзора	Ответственный за организацию обработки персональных данных	Выполнение требований ФЗ-152
11	При заключении договоров с третьими лицами, оказание услуг которыми подразумевает передачу персональных данных работников, необходимо перед заключением договора получить согласие на передачу персональных данных от сотрудников	Ответственный за организацию обработки персональных данных	Выполнение требований ФЗ-152
12	При заключении договоров с третьими лицами, оказание услуг которыми подразумевает передачу	Ответственный за организацию обработки	Выполнение требований ФЗ-152

	персональных данных работников или доступ третьих лиц к информационной. системе персональных данных необходимо в договор включить соответствующий пункт	персональных данных	
13	Приобретение средств защиты информации (СЗИ) в соответствии с разработанной документацией, технических средств обеспечения ограничения доступа к ИСПДн и местам хранения ПДн	Ответственный за организацию обработки персональных данных	Выполнение требований 1111 РФ № 1119, Приказов ФСТЭК России № 17,21; Отметки в журнале учета СЗИ, СКЗИ
14	Внедрение СЗИ в соответствии с требованиями нормативных актов	Лицензиат ФСТЭК и ФСБ	Выполнение требований 1111 РФ № 1119, Приказа ФСТЭК России № 17,21; Акт установки и ввода в эксплуатацию СЗИ; Эксплуатационная документация на применяемые средства защиты информации