Учреждение Российской академии наук
Институт механики
Уфимского научного центра РАН
(ИМех УНЦ РАН)

«УТВЕРЖДАЮ»
Директор ИМех УНЦ РАН
_____ С.Ф. Урманчеев
«13» декабря 2011 г.

ПОЛОЖЕНИЕ
об обеспечении безопасности персональных данных
при их обработке в информационных системах
ИМех УНЦ РАН

I. Общие положения

1.1. Настоящее Положение разработано в соответствии с Положением об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденным Постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781 и устанавливает методы и способы защиты информации, применяемые для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (ИСПДн) Института.

В настоящем Положении не рассматриваются вопросы обеспечения безопасности персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.

1.2. Работа с базой персональных данных сотрудников Института происходит на нескольких компьютерах бухгалтерии и отдела кадров, располагающихся в одном здании и объединенных в локальную сеть (ЛИС). Система является многопользовательской с разграничением прав доступа.

В данной системе обрабатываются персональные данные сотрудников Института, объем не превышает 1000 записей о субъектах и относится к одной организации.

Категория обрабатываемых данных – 3.

ИСПДн типа ЛИС бухгалтерии и кадрового учета имеет класс К3 в соответствии с Актом классификации ИСПДн.

1.3. Методы и способы защиты информации в ИСПДн Института разработаны на основе Модели угроз и системы защиты ИСПДн ИМех УНЦ РАН.

К ним относятся:

– методы и способы защиты информации, обрабатываемой техническими средствами информационной системы, от несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий (далее - методы и способы защиты информации от несанкционированного доступа);

– методы и способы защиты речевой информации, от несанкционированного доступа к персональным данным, результатом которого

может стать копирование, распространение персональных данных, а также иных несанкционированных действий (далее - методы и способы защиты информации от утечки по техническим каналам).

1.4. Для реализации методов и способов защиты информации в информационной системе директором Института назначается должностное лицо (работник), ответственное за обеспечение безопасности персональных данных.

1.5. Выбор и реализация методов и способов защиты информации в информационной системе осуществляются на основе определяемых угроз безопасности персональных данных (модели угроз) и в зависимости от класса информационной системы, определенного в соответствии с Порядком проведения классификации информационных систем персональных данных, утвержденным Приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. № 55/86/20.

1.6. Лица, доступ которых к персональным данным, обрабатываемым в ИСПДн, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании списка, утвержденного директором Института.

1.7. Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

II. Методы и способы защиты информации от несанкционированного доступа

Для ИСПДн Института применяются следующие основные методы и способы защиты информации:

а) **управление доступом**:

– идентификация и проверка подлинности пользователя при входе в систему по паролю условно-постоянного действия;

– разграничения доступа пользователей и обслуживающего персонала к информационным ресурсам;

б) **обеспечение целостности** программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность программных средств проверяется при загрузке системы по контрольным суммам компонентов средств защиты информации, а целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации;

в) **антивирусная защита**;

г) **физическая охрана** информационной системы (устройств и носителей информации), предусматривающая контроль доступа в помещения информационной системы посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения информационной системы и хранилище носителей информации.

д) **размещение устройств вывода** информации средств вычислительной техники, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав информационной системы, в помещениях, в которых они установлены, осуществляется таким образом, чтобы была исключена возможность просмотра посторонними лицами текстовой и графической видовой информации, содержащей персональные данные.

Разработано в соответствии с приказом от 20.10.2011 г. № 19-1252.

Вед. специалист секретариата Л.С. Бушуева