Приложение
К приказу № 23/4
От 30.08.2023г

Модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных

1. Общие положения

В настоящей модели угроз безопасности персональных данных при их обработке в информационной системе персональных данных МКОУ «Танрыкуловская СОШ» (далее – Модель угроз) в соответствии с пунктом 1 части 2 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» определены актуальные угрозы безопасности персональных данных при их обработке в информационной системе персональных данных МКОУ «Танрыкуловская СОШ» (далее – ИСПДн МКОУ «Танрыкуловская СОШ»).

Под угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в ИСПДн МКОУ «Танрыкуловская СОШ» (нарушение конфиденциальности, целостности и доступности обрабатываемых персональных данных). Для ИСПДн целью защиты информации является обеспечение конфиденциальности, целостности и доступности обрабатываемых персональных данных.

В качестве источников угроз безопасности персональных данных могут выступать субъекты (физические лица, организации) или явления (техногенные аварии, стихийные бедствия, иные природные явления). При этом источники угроз могут быть следующих типов:

антропогенные источники (антропогенные угрозы);

техногенные источники (техногенные угрозы);

стихийные источники (угрозы стихийных бедствий, иных природных явлений).

Источниками антропогенных угроз безопасности персональных данных могут выступать:

лица, осуществляющие преднамеренные действия с целью доступа к персональным данным (воздействия на персональные данные), содержащимся в ИСПДн или нарушения функционирования ИСПДн или обслуживающей ее инфраструктуры (преднамеренные угрозы безопасности персональных данных);

лица, имеющие доступ к ИСПДн, не преднамеренные действия которых могут привести к нарушению безопасности персональных данных (непреднамеренные угрозы безопасности персональных данных).

Преднамеренные угрозы безопасности персональных данных могут быть реализованы за счет утечки персональных данных по техническим каналам (технические каналы утечки информации, обрабатываемой в технических средствах ИСПДн, технические каналы перехвата информации при ее передаче по каналам (линиям) связи, технические каналы утечки акустической (речевой) информации) либо за счет несанкционированного доступа.

Настоящая Модель угроз содержит перечень угроз безопасности персональных данных, актуальных при обработке персональных данных в ИСПДн, которые могут быть реализованы в ИСПДн, а также содержит совокупность предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак для ИСПДн.

Настоящая Модель угроз разработана с использованием следующих документов:

Федерального закона Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 15.02.2008;

Угрозы безопасности персональных данных, актуальные при обработке персональных данных в ИСПДн, определяются по результатам оценки возможностей (потенциала) внешних и внутренних нарушителей, оценки уровня исходной защищенности ИСПДн, анализа возможных способов реализации угроз безопасности персональных данных и последствий от нарушения свойств безопасности персональных данных (конфиденциальности, целостности, доступности).

Источником данных об угрозах безопасности информации, на основе которых определяются угрозы безопасности персональных данных, актуальные при обработке персональных данных в ИСПДн, являются Базовые угрозы. При этом Базовые угрозы подлежат адаптации, которая направлена на уточнение (уменьшение) перечня угроз безопасности персональных данных, актуальных при обработке персональных данных в ИСПДн, и осуществляется с учетом структурно-функциональных характеристик ИСПДн, применяемых информационных технологий и особенностей функционирования (в том числе исключение угроз, которые непосредственно связаны с информационными технологиями, не используемыми в ИСПДн, или структурно-функциональными характеристиками, не свойственными ИСПДн).

Угрозы безопасности персональных данных, актуальные при обработке персональных данных в ИСПДн подлежат пересмотру (переоценке):

при внесении изменений в Базовые угрозы для типа информационных систем персональных данных, к которому относится ИСПДн;

при изменении структурно-функциональных характеристик или особенностей функционирования ИСПДн, вследствие чего изменился тип, к которому относится ИСПДн;

при применении в ИСПДн информационных технологий, посредством которых могут формироваться новые угрозы безопасности персональных данных, исключенные из базового (предварительного) перечня угроз безопасности персональных данных для ИСПДн в соответствии с положениями раздела 4 настоящей Модели угроз;

при повышении возможности реализации существующих угроз безопасности персональных данных.

1. Описание информационной системы персональных данных и особенностей ее функционирования

ИСПДн эксплуатируется в целях *осуществления государственных (муниципальных) функций (указать каких) и (или) иных функций (указать каких), или в целях оказания государственных (муниципальных) услуг (указать каких).*

ИСПДн представляет собой[1]:

автоматизированное рабочее место (далее – АРМ), не имеющее подключение (незащищенное, защищенное) к каким-либо сетям связи, в том числе к беспроводным сетям связи (исключение составляют беспроводные технологии, предназначенные для функционирования периферийных устройств (клавиатура, манипулятор «мышь» и другие), входящих в состав АРМ) (тип 1 в соответствии с пунктом 2.5 Базовых угроз);

автоматизированное рабочее место, имеющее подключение к сетям связи, включая сети связи общего пользования и (или) сети международного информационного обмена, в том числе сеть «Интернет» (тип 2 в соответствии с пунктом 2.5 Базовых угроз)[2]*;*

В ИСПДн применяются *технологии виртуализации, клиент (файл)-серверные технологии, удаленный доступ, мобильные устройства*. При этом в ИСПДн не применяются технологии автоматизации управления технологическим процессом, облачные технологии, технологии больших данных, суперкомпьютеры и грид-вычисления, посредством которых могут формироваться дополнительные угрозы безопасности персональных данных.

Все технические средства ИСПДн находятся в пределах Российской Федерации в *здании МКОУ «Танрыкуловская СОШ» по адресу с. Танрыкулово ул. Советская,12.*

При входе в здание организована контрольно-пропускная система, дежурство обслуживающего персонала. В ночное время организовано дежурство сторожей.

Помещения, в которых ведется обработка персональных данных в ИСПДн (далее – Помещения), оснащены входными дверьми с замками. Установлен порядок доступа в Помещения, препятствующий возможности неконтролируемого проникновения или пребывания в этих Помещениях лиц, не имеющих права доступа в них. В рабочее время, в случае ухода лиц, имеющих право самостоятельного доступа в Помещение, а также в нерабочее время двери Помещения закрываются на ключ. Доступ посторонних лиц в Помещения допускается только в присутствии лиц, имеющих право самостоятельного доступа в данные Помещения на время, ограниченное служебной необходимостью. При этом предпринимаются меры, исключающие возможность доступа посторонних лиц к обрабатываемым персональным данным, в том числе через устройства ввода (вывода)

информации, а также к носителям персональных данных.

Устройства ввода (вывода) информации из состава ИСПДн участвующие в обработке персональных данных, располагаются в Помещениях таким образом, чтобы исключить случайный просмотр обрабатываемой информации посторонними лицами, вошедшими в Помещение, а также через двери и окна Помещения.

Ввод (вывод) персональных данных в ИСПДн осуществляется с использованием бумажных и машинных носителей информации, *в том числе съемных машинных носителей информации (флеш-накопители)* (далее – Машинные носители персональных данных).

Режим обработки информации в ИСПДн *однопользовательский/многопользовательский* с разграничением прав доступа (набора действий, разрешенных для выполнения) пользователей. Управление (администрирование) ИСПДн а также обслуживание технических и программных средств ИСПДн средств защиты информации включая настройку, конфигурирование и распределение носителей ключевой информации между пользователями ИСПДн, осуществляется сотрудниками *имеющими доступ к персональным данным*.

Сотрудники, участвующие в управлении (администрировании) ИСПДн и ее системой защиты информации, а также обслуживающие технические и программных средств ИСПДн являются привилегированными пользователями. *(ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных)*, которые назначаются из числа доверенных лиц.

В целях обеспечения целостности обрабатываемых в ИСПДн персональных данных осуществляется их резервирование в соответствии с установленным в *ОУ* порядком с использованием Машинных носителей персональных данных.

Помещения с техническими средствами ИСПДн оснащены средствами пожарной сигнализации.

К объектам защиты в ИСПДн относятся:

обрабатываемые персональные данные;

технические средства (Машинные носители персональных данных, технические средства обработки буквенно-цифровой, графической информации);

средства защиты информации;

документы, в которых отражена информация о мерах и средствах защиты ИСПДн;

Помещения.

ИСПДн с учетом структурно-функциональных характеристик и условий эксплуатации, а также применяемых информационных технологий и предпринятых мер обеспечения безопасности персональных данных, приведенных в настоящем разделе, имеет средний уровень исходной защищенности.