УТВЕРЖДАЮ
Директор МБОУ СОШ № 28
_____/ М.М.Кривчук
Приказ № «_____»
от «_____» _____ 20_____ г.

Положение
о комиссии по классификации информационных систем персональных данных МБОУ СОШ № 28

1. Проведение обследования

На этапе обследования информационных систем ПДн выполняются следующие работы:

- формируется перечень ПДн, информационных систем и технических средств, используемых для их обработки;
- определяются подразделения и сотрудники, обрабатывающие ПДн;
- определяются категории ПДн;
- разрабатывается описание объекта защиты, включая состав и характеристики средств обработки данных
- проводится предварительная классификация информационных систем ПДн;
- в соответствии с рекомендациями ФСТЭК России и (или) ФСБ России определяются и уточняются типовые модели угроз и соответствующие им типовые требования к системам защиты ПДн;
- осуществляется оценка необходимых мероприятий и затрат по приведению информационных систем ПДн в соответствие с предъявляемыми требованиями.

Результатами работ на этапе обследования являются:

- перечень и категории ПДн,
- перечни информационных систем и технических средств используемых для обработки ПДн и анализ их состояния,
- состав имеющихся в наличии мер и средств защиты ПДн;
- подразделения и сотрудники, обрабатывающие ПДн;
- предварительная классификация информационных систем, обрабатывающих ПДн на типовые (1 - 4 классов) и специальные;
- описание объектов защиты
- уточненные типовые модели угроз и требования к системам защиты ПДн;
- оценка необходимых мероприятий и затрат по приведению информационных систем ПДн в соответствие с предъявляемыми требованиями.

Если затраты времени и средств на приведение информационных систем персональных данных (ИСПДн) в соответствие с предъявляемыми требованиями окажутся слишком высокими, то следует оценить возможность обезличивания или понижения классов информационных систем и провести необходимые работы повторно.

Наиболее эффективным способом приведению ИСПДн в соответствие с предъявляемыми требованиями является их обезличивание. Оно позволяет классифицировать ИСПДн по низшему классу К4 и самостоятельно определить необходимость и способы их защиты.

Если обезличивание невозможно, то понизить требования по защите персональных данных можно путем сегментирования ИСПДн, отключения от сетей общего пользования, обеспечения обмена между ИСПДн с помощью сменных носителей, создания автономных ИСПДн на выделенных АРМ.

После определения способов понижения требований по защите персональных данных и необходимого повторного обследования оформляются акты классификации ИСПДн, осуществляются определение и анализ типовых моделей угроз и требований, определение необходимых мер и средств защиты ПДн, а также внутренних нормативных документов, регламентирующих порядок обработки и защиты ПДн.

Завершается предпроектная стадия формированием Плана выполнения работ по обеспечению защиты персональных данных.

Предпроектная стадия является важнейшим этапом работ по обеспечению защиты персональных данных, во многом определяющим состав и эффективность реализации мероприятий и необходимые затраты. Поэтому на данном этапе целесообразно привлекать для анализа результатов обследования и консультаций специалистов в области защиты персональных данных.

2. Классификация информационных систем персональных данных и определение актуальных угроз их безопасности

Для проведения классификации ИСПДн, определения категорий персональных данных и экспертной оценки угроз их безопасности целесообразно сформировать комиссию с привлечением специалистов в области информационной безопасности, в том числе по защите государственной тайны.

Перечень типовых ИСПДн определен приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных».Классификация ИСПДн осуществляется в зависимости от ***категории персональных данных (ПДн***), не содержащих сведения, относящиеся к государственной тайне:

категория 1 - ПДн, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;

категория 2 - ПДн, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением ПДн, относящихся к категории 1;

категория 3 - ПДн, позволяющие идентифицировать субъекта персональных данных;

категория 4 - обезличенные и (или) общедоступные персональные данные.

Целесообразно отдельно определять категории ПДн, обрабатываемых в ИСПДн в электронном и в бумажном виде. В последнем случае следует руководствоваться постановлением Правительства Российской Федерации от 15 сентября 2008 г. N 687.

Типовые ИСПДн, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов персональных данных, относятся к классу 1 (***К1***), - к негативным последствиям – к классу 2 (***К2***), ***к незначительным*** негативным ***последствиям*** – к классу 3 (***К3***), для субъектов персональных данных, ***не приводит к*** негативным ***последствиям*** для субъектов персональных данных – к классу 4 (***К4***).

Кроме того, при классификации учитываются объем и территория охвата субъектов персональных данных в порядке, приведенном в приказе ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20.

<table>
<tr><td rowspan="2">Количество субъектов ПДн в системе

Категория ПДн, обрабатываемых в электронном виде</td><td rowspan="2">Более 100 тыс. ПДн</td><td colspan="2">В объеме</td><td rowspan="2">От 1000 до 100000 ПДн</td><td colspan="4">В объеме</td><td rowspan="2">До 1000 ПДн</td></tr>
<tr><td>РФ</td><td>субъекта РФ</td><td>отрасли</td><td>органа власти</td><td>муниципального образования</td><td>организации</td></tr>
<tr><td>1. Расовая, национальная принадлежность, политические взгляды, религиозные и философские убеждения, состояние здоровья, интимная жизнь</td><td colspan="3">1 класс (К1)</td><td colspan="4">1 класс (К1)</td><td>1 класс (К1)</td></tr>
</table>

2. Позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением ПДн, относящихся к категории **1**	**1 класс (К1)**	***2 класс (К2)***	3 класс (К3)
3. Позволяющие идентифицировать субъекта персональных данных	***2 класс (К2)***	3 класс (К3)	3 класс (К3)
4. Обезличенные и (или) общедоступные персональные данные	*4 класс (К4)*	*4 класс (К4)*	*4 класс (К4)*

ИСПДн, обрабатывающие обезличенные или общедоступные персональные данные класса (категории 4) относятся к классу К4. В этом случае обязательные требования по защите ПДн не устанавливаются.

Постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных" определены необходимые мероприятия по защите персональных данных. В их число входят определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз; разработка на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем, и другие мероприятия.

При обработке персональных данных в информационной системе должно быть обеспечено:

а) проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации *(прежде всего, регламентирование доступа сотрудников к обработке персональных данных, парольная и антивирусная защита);*

б) своевременное обнаружение фактов несанкционированного доступа к персональным данным *(прежде всего, регламентирование использования и регулярное обновление антивирусных средств);*

в) ***недопущение*** воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование *(охрана и регламентирование использования технических средств);*

г) ***возможность*** незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним *(прежде всего, путем хранения резервных копий на съемных маркированных носителях);*

д) постоянный контроль за обеспечением уровня защищенности персональных данных *(осуществляемый, в основном, администраторами ИСПДн и иным персоналом).*

При этом следует иметь ввиду, что ***в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» основным обязательным требованием к ИСПДн является обеспечение конфиденциальности****. Если право доступа субъекта к своим персональным данным, их изменения, блокирования или отзыва реализуются не самим субъектом непосредственно, а персоналом ИСПДн при обращении или по запросу субъекта или его законного представителя, либо уполномоченного органа по защите прав субъектов персональных данных, если в ИСПДн не обрабатываются персональные данные 1 категории и не предусмотрено*

принятие решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы на основании исключительно автоматизированной обработки персональных данных, то другие требования (кроме конфиденциальности) менее критичны. Так, в случае выявления неправомерных действий с персональными данными для их устранения законом предусмотрено три рабочих дня с даты такого выявления.

Следует учитывать, что требования к обработке персональных данных и к обработке иной конфиденциальной информации (например, коммерческой тайны) могут различаться. ***Применение к обработке персональных данных положений документов (например, СТР-К), действующих до вступления в силу Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», если эти положения в этом законе или последующих подзаконных актах изложены иначе, юридически некорректно.***

Если система не может быть отнесена к типовой, модель угроз специальной информационной системы разрабатывается на основе ГОСТ Р 51275-2006 специалистами в области информационной безопасности. Типовые модели угроз приводятся в «Базовой модели угроз безопасности персональных данных».

Определение угроз безопасности персональных данных осуществляется на основе утвержденной ФСТЭК России «Базовой модели угроз безопасности персональных данных». Полный перечень угроз определен ГОСТ Р 51275-2006.

Выбор типовой модели угроз осуществляется в зависимости от того, имеют ли ИСПДн подключение к сетям общего пользования и (или) сетям международного информационного обмена, а также от их структуры (автономные автоматизированные рабочие места, локальные сети, распределенные ИСПДн с удаленным доступом).

Наименьшее количество угроз имеют автоматизированные рабочие места и локальные ИСПДн, не подключенные к сетям общего пользования. ***Если ИСПДн нераспределенные и соответствуют классу К3, то необходимые мероприятия по защите персональных данных могут быть осуществлены без привлечения специалистов в области информационной безопасности***.

Для каждой угрозы, приведенной в типовой модели, следует оценить возможную степень ее реализации. Если она окажется высокой, то это может потребовать применения соответствующих дополнительных технических средств защиты информации.

Возможность реализации угрозы зависит от исходной защищенности ИСПДн и вероятности реализации угрозы.

Вероятность реализации угрозы - определяемый экспертным путем показатель, характеризующий, насколько вероятной является реализация конкретной угрозы безопасности ПДн для каждой ИСПДн:

маловероятно - отсутствуют объективные предпосылки для осуществления угрозы (например, отсутствует физическое подключение к сети);

низкая вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, действия персонала оговорены в утвержденном регламенте или имеются средства защиты и инструкции по их применению);

средняя вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны (например, средства защиты имеются, но инструкции по их применению отсутствуют):

высокая вероятность - объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты.

Исходная защищенность ИСПДн определяется в соответствии с утвержденной ФСТЭК России «Методикой определения актуальных угроз безопасности персональных

данных при их обработке в информационных системах персональных данных». Расчет исходной защищенности ИСПДн осуществляется по таблице, приведенной в «Методике...», в зависимости от ряда показателей, по которым подразделяются ИСПДн.

В соответствии с «Методикой...» осуществляется расчет возможности реализации угроз и оценка их опасности.

Определяемый на основе опроса экспертов показатель опасности имеет три значения:

низкая опасность - если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных, что соответствует классу К3;

средняя опасность - если реализация угрозы может привести к негативным последствиям для субъектов персональных данных, что ***соответствует классу К2***;

высокая опасность - если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных, что ***соответствует классу К1***.

Информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, не приводит к негативным последствиям для субъектов персональных данных соответствуют классу К4.

При использовании типовых моделей угроз и соответствующих им требований, приведенных в утвержденных ФСТЭК России «Основных мероприятий по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных» следует учитывать, что ***в ряде случаев возможности реализации отдельных угроз могут быть более высокими и потребовать дополнительных мер защиты персональных данных.*** Например, возможность реализации угроз увеличивается, если:

- помещения не запираются;
- при обработке персональных данных используются микрофон и динамики;
- монитор не отвернут от окна и посетителей;
- используются беспроводные устройства, в т.ч. клавиатура и мышь;
- отсутствует парольная защита BIOS;
- используются средства сетевого взаимодействия по электропроводке или беспроводные;
- запуск неразрешенных приложений не контролируется.

Актуальные угрозы определяются по приведенной в «Методике...» таблице в зависимости от их опасности и возможности реализации.

При отсутствии дополнительных опасных факторов (например, перечисленных) для нераспределенных ИСПДн 3 класса анализ угроз можно провести при окончательном уточнении требований на этапе выбора и реализации системы защиты персональных данных.

Исходя из составленного перечня актуальных угроз и класса ИСПДн на основе утвержденных ФСТЭК России «Рекомендаций по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и «Основных мероприятий по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных» формулируются конкретные требования по защите ИСПДн и осуществляется выбор программных и технических средств защиты информации.

Выписки из документов размещены на официальном сайте ФСТЭК России .

Анализ актуальности угроз и защита персональных данных могут также осуществляться на основании *Методических рекомендаций ФСБ России по обеспечению* ***с помощью криптосредств*** *безопасности персональных данных* при их обработке в информационных системах персональных данных с использованием средств автоматизации. Однако для типовых ИСПДн 3 класса в большинстве случаев это потребует дополнительных затрат.

Если аномально опасные угрозы не выявлены, то ***для ИСПДн 3 класса, как правило, можно ограничиться типовыми требованиями к средствам защиты, приведенными в выписке из «Основных мероприятий по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных» .***

В документе приводятся три варианта требований к ИСПДн 3 класса:

- при ***однопользовательском*** режиме обработки;
- при многопользовательском режиме обработки и ***равных правах доступа***;
- при многопользовательском режиме обработки и ***разных правах доступа***.

В последнем случае при подключении к Интернет нераспределенных ИСПДн класса К3 сертифицированные межсетевые экраны не указаны, как обязательные. Это существенно уменьшает затраты на реализацию системы защиты персональных данных, но требует настройки ИСПДн с учетом прав доступа конкретных пользователей.

3. Определение способов понижения требований по защите персональных данных

По результатам первичной классификации ИСПДн во многих случаях относятся к 1 или 2 классам, требующим существенных затрат и обязательной аттестации. ***Существенно уменьшить обязательные требования и необходимые затраты на защиту персональных данных можно путем обезличивания и сегментирования ИСПДн, отключения сегментов ИСПДн от сетей общего пользования, организации выделенных АРМ и др.***

Основная экономия затрат достигается при этом за счет отключения от Интернет, изменения классификации сегментов ИСПДн на К4 или К3 и замены аттестации на декларирование соответствия, а также за счет уменьшения количества защищаемых АРМ в аттестуемых ИСПДн высоких классов К2 и К1.

Наилучшим результатом является обезличивание и обоснование соответствия ИСПДн классу К4, для которого все персональные данные относятся к категории 4 и являются обезличенными или общедоступными.

При этом необходимо иметь ввиду, что ***объявить персональные данные общедоступными только внутри организации даже с согласия субъектов ПДн нельзя***. В соответствии с Федеральным законом Российской Федерации от 27 июля 2007 г. №152-ФЗ «О персональных данных», общедоступными являются персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности. Поэтому ***в информационных системах бухгалтерского и кадрового учета, учета контингента и успеваемости учащихся обязательно будут иметься персональные данные, которые необходимо защищать***.

В этой связи наиболее эффективным является обезличивание ИСПДн путем замены ФИО субъектов ПДн на их личные коды (табельные номера), используемые для автоматизированного учета в данной организации. Существенным преимуществом этого способа является возможность непосредственной замены всех

ФИО кодами вручную или с помощью встроенных средств в недоступных для самостоятельной модернизации ИСПДн (1С бухгалтерия, Парус и др.).

Вторым по эффективности является полное исключение из ИСПДн сведений 1 категории, касающихся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни. Даже, если в действующих ИСПДн сохранились такие показатели, то их целесообразно исключить или стереть соответствующие им данные, или заменить на условные коды. ***При необходимости учет персональных данных 1 категории следует осуществлять в форме анкет, справок, личных дел и иных документов только на бумажных носителях***. Для формирования и ведения списков лиц с ограниченными возможностями здоровья конкретные данные о состоянии здоровья, как правило, не требуются.

Также следует полностью исключить из ИСПДн и выделить в специальное делопроизводство сведения, относящиеся к государственной тайне.

Персональные данные 2 категории, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию (за исключением ПДн, относящихся к категории 1) ***целесообразно вывести из интегрированных ИСПДн в отдельные локальные системы и отключить от Интернет.***

Персональные данные 3 категории, позволяющие только идентифицировать субъекта персональных данных, в зависимости от объема данных и класса ИСПДн можно обезличивать или обрабатывать в неизменном виде.