МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

по определению состава и содержания технических и организационных мер по защите персональных данных при их обработке в информационной системе персональных данных

Содержание

1. Общие положения

1.1. Введение

Согласно статье 19 Федерального закона от 27.07.2006 № 152 «О персональных данных» (далее – ФЗ № 152) оператор информационной системы персональных данных (далее – ИСПДн) обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных (далее – ПДн) при их обработке в ИСПДн от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении ПДн.

Оператор ИСПДн – это государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн (ст. 3 ФЗ № 152).

Таким образом, органы исполнительной власти (далее – ОИВ) и органы местного самоуправления (далее – ОМСУ) Кировской области (далее – КО) должны обеспечивать безопасность ПДн при их обработке в ИСПДн.

Для выполнения работ по обеспечению безопасности ПДн при их обработке в ИСПДн в соответствии с законодательством Российской Федерации могут привлекаться на договорной основе юридическое лицо или индивидуальный предприниматель, имеющие лицензию на деятельность по технической защите конфиденциальной информации.

В соответствии с ч. 1 ст. 22 ФЗ № 152 оператор до начала обработки ПДн обязан уведомить уполномоченный орган по защите прав субъектов ПДн (Роскомнадзор по Кировской области) о своём намерении осуществлять обработку ПДн.

Исключение составляют случаи, предусмотренные ч. 2 комментируемой статьи, при обработке ПДн:

1) обрабатываемых в соответствии с трудовым законодательством;

2) полученных оператором в связи с заключением договора, стороной которого является субъект ПДн, если персональные данные не распространяются, а также не предоставляются третьим лицам без согласия субъекта ПДн и используются оператором исключительно для исполнения указанного договора и заключения договоров с субъектом ПДн;

3) относящихся к членам (участникам) общественного объединения или религиозной организации и обрабатываемых соответствующими общественным объединением или религиозной организацией, действующими в соответствии с законодательством Российской Федерации, для достижения законных целей, предусмотренных их учредительными документами, при условии, что ПДн не будут распространяться или раскрываться третьим лицам без согласия в письменной форме субъектов ПДн;

4) сделанных субъектом ПДн общедоступными;

5) включающих в себя только фамилии, имена и отчества субъектов ПДн;

6) необходимых в целях однократного пропуска субъекта ПДн на территорию, на которой находится оператор, или в иных аналогичных целях;

7) включенных в ИСПДн, имеющих в соответствии с федеральными законами статус государственных автоматизированных информационных систем, а также в государственные информационные системы персональных данных, созданные в целях защиты безопасности государства и общественного порядка;

8) обрабатываемых без использования средств автоматизации в соответствии с федеральными законами или иными нормативными правовыми актами Российской Федерации, устанавливающими требования к обеспечению безопасности ПДн при их обработке и к соблюдению прав субъектов ПДн;

9) обрабатываемых в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

Уведомление должно быть направлено в письменной форме и подписано должностным лицом или направлено в электронной форме и подписано электронной цифровой подписью в соответствии с законодательством Российской Федерации.

Образец формы уведомления об обработке ПДн и методические рекомендации по его заполнению размещены на официальном сайте Роскомнадзора (www.rsoc.ru).

Кроме того, на портале Персональные данные (http://pd.rkn.gov.ru/) реализована функция по заполнению уведомлений об обработке ПДн в электронной форме.

Рекомендуется иметь копию направленного в Роскомнадзор уведомления.

1.2. Назначение методических рекомендаций

Методические рекомендации разработаны министерством информационных технологий и связи Кировской области с целью упрощения процесса работы ОИВ и ОМСУ КО по обеспечению безопасности ПДн при их обработке в ИСПДн, операторами которых они являются, на основе законодательства Российской Федерации в области защиты ПДн:

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

- Постановления Правительства Российской Федерации от 21.03.2012 № 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, операторами, являющимися государственными или муниципальными органами»;

- приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (далее – приказ ФСТЭК № 21),

- Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее – ПП № 1119),

- приказа ФСБ РФ от 10 июля 2014 г. № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищённости» (далее – приказ ФСБ № 378).

Настоящий документ определяет порядок выбора ОИВ и ОМСУ КО состава и содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн.

Меры по обеспечению безопасности персональных данных при их обработке в государственных информационных системах принимаются в соответствии с требованиями о защите информации, содержащейся в государственных информационных системах, устанавливаемыми приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и требованиями к защите ПДн при их обработке в ИСПДн, утверждённых ПП № 1119.

1.3. Область действия методических рекомендаций

Настоящий документ рекомендуется использовать ОИВ и ОМСУ КО при определении требований по защите ПДн при их обработке в ИСПДн, операторами которых они являются.

ИСПДн – это совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств.

ПДн – это любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту ПДн), в том числе, его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы и другая информация.

Таким образом, информационная система персонального кадрового учёта (например, 1С: Кадровый резерв), предназначенная для персонального кадрового учёта, управления кадровым резервом, проведения аттестации, повышения квалификации и решения других вопросов, связанных с управлением персоналом, является ИСПДн, так как содержит фамилию, имя, отчество и другую информацию, относящуюся к прямо или косвенно определённому или определяемому физическому лицу.

Также к ИСПДн относится, например, информационная система 1С: Зарплата и кадры и другие.

2. Порядок действий по определению уровня защищённости ПДн, обрабатываемых в ИСПДн ОИВ и ОМСУ КО

В зависимости от требуемого уровня защищённости (или защиты) ПДн предъявляются разные требования по обеспечению их безопасности: чем выше требуемый уровень защищённости ПДн, тем шире перечень необходимых мер. Поэтому прежде чем определить состав и содержание технических и организационных мер по защите ПДн, необходимо определить уровень защищённости ПДн.

Требуемый уровень защищённости ПДн при их обработке в ИСПДн зависит от:

1) типа угроз, актуальных для ИСПДн, и

2) категории обрабатываемых ПДн.

Таким образом, сначала необходимо определить тип актуальных угроз и категорию обрабатываемых ПДн. Порядок действий по определению типа актуальных угроз перечислен в пункте 2.1 настоящего документа, а порядок действий по определению вида ИСПДн перечислен в пункте 2.2 настоящего документа.

2.1. Порядок действий по определению типа актуальных угроз

Тип актуальных угроз определяется следующим образом (п. 6 ПП № 1119):

Для ИСПДн актуальны **угрозы 1-го типа**, если для неё в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в ИСПДн (т. е. если работа с ИСПДн осуществляется на персональном компьютере с операционной системой (например, Windows),

имеющей функциональные возможности, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности и (или) целостности обрабатываемой информации).

Для ИСПДн актуальны **угрозы 2-го типа**, если для неё в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в ИСПДн.

Для ИСПДн актуальны **угрозы 3-го типа**, если для неё актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в ИСПДн.

2.2. Порядок действий по определению вида ИСПДн

После определения типа актуальных угроз определяется вид ИСПДн. В зависимости от категории обрабатываемых ПДн выделяют следующие виды ИСПДн (п. 5 ПП № 1119):

а) Информационная система является информационной системой, обрабатывающей **специальные категории** ПДн, если в ней обрабатываются ПДн, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов ПДн.

б) Информационная система является информационной системой, обрабатывающей **биометрические** ПДн, если в ней обрабатываются сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта ПДн, и не обрабатываются сведения, относящиеся к специальным категориям ПДн.

в) Информационная система является информационной системой, обрабатывающей **общедоступные** ПДн, если в ней обрабатываются ПДн субъектов ПДн, полученные только из общедоступных источников ПДн, созданных в соответствии со статьей 8 ФЗ № 152.

г) Информационная система является информационной системой, обрабатывающей **иные категории** ПДн, если в ней не обрабатываются ПДн, указанные в абзацах втором - четвёртом настоящего пункта.

При этом каждая из четырех перечисленных систем может обрабатывать ПДн сотрудников оператора или ПДн субъектов ПДн, не являющихся сотрудниками оператора.

Информационная система является информационной системой, обрабатывающей ПДн сотрудников оператора, если в ней обрабатываются ПДн только указанных сотрудников. В остальных случаях ИСПДн является информационной системой, обрабатывающей ПДн субъектов ПДн, не являющихся сотрудниками оператора.

После определения типа актуальных угроз и вида ИСПДн определяется требуемый уровень защищённости ПДн при их обработке в ИСПДн. Согласно ПП № 1119 при обработке ПДн в ИСПДн устанавливаются 4 уровня защищённости ПДн. Самый низкий – четвертый, самый высокий – первый. Порядок определения уровня защищённости ПДн описан далее.

Необходимость обеспечения **1-го уровня защищённости** ПДн при их обработке в ИСПДн устанавливается при наличии хотя бы одного из следующих условий:

а) для ИСПДн актуальны угрозы 1-го типа и ИСПДн обрабатывает либо специальные категории ПДн, либо биометрические ПДн, либо иные категории ПДн;

б) для ИСПДн актуальны угрозы 2-го типа и ИСПДн обрабатывает специальные категории ПДн более чем 100000 субъектов ПДн, не являющихся сотрудниками оператора.

Необходимость обеспечения **2-го уровня защищённости** ПДн при их обработке в ИСПДн устанавливается при наличии хотя бы одного из следующих условий:

а) для ИСПДн актуальны угрозы 1-го типа и ИСПДн обрабатывает общедоступные ПДн;

б) для ИСПДн актуальны угрозы 2-го типа и ИСПДн обрабатывает специальные категории ПДн сотрудников оператора или специальные категории ПДн менее чем 100000 субъектов ПДн, не являющихся сотрудниками оператора;

в) для ИСПДн актуальны угрозы 2-го типа и ИСПДн обрабатывает биометрические ПДн;

г) для ИСПДн актуальны угрозы 2-го типа и ИСПДн обрабатывает общедоступные ПДн более чем 100000 субъектов ПДн, не являющихся сотрудниками оператора;

д) для ИСПДн актуальны угрозы 2-го типа и ИСПДн обрабатывает иные категории ПДн более чем 100000 субъектов ПДн, не являющихся сотрудниками оператора;

е) для ИСПДн актуальны угрозы 3-го типа и ИСПДн обрабатывает специальные категории ПДн более чем 100000 субъектов ПДн, не являющихся сотрудниками оператора.

Необходимость обеспечения **3-го уровня защищённости** ПДн при их обработке в ИСПДн устанавливается при наличии хотя бы одного из следующих условий:

а) для ИСПДн актуальны угрозы 2-го типа и ИСПДн обрабатывает общедоступные ПДн сотрудников оператора или общедоступные ПДн менее чем 100000 субъектов ПДн, не являющихся сотрудниками оператора;

б) для ИСПДн актуальны угрозы 2-го типа и ИСПДн обрабатывает иные категории ПДн сотрудников оператора или иные категории ПДн менее чем 100000 субъектов ПДн, не являющихся сотрудниками оператора;

в) для ИСПДн актуальны угрозы 3-го типа и ИСПДн обрабатывает специальные категории ПДн сотрудников оператора или специальные категории ПДн менее чем 100000 субъектов ПДн, не являющихся сотрудниками оператора;

г) для ИСПДн актуальны угрозы 3-го типа и ИСПДн обрабатывает биометрические ПДн;

д) для ИСПДн актуальны угрозы 3-го типа и ИСПДн обрабатывает иные категории ПДн более чем 100000 субъектов ПДн, не являющихся сотрудниками оператора.

Необходимость обеспечения **4-го уровня защищённости** ПДн при их обработке в ИСПДн устанавливается при наличии хотя бы одного из следующих условий:

а) для ИСПДн актуальны угрозы 3-го типа и ИСПДн обрабатывает общедоступные ПДн;

б) для ИСПДн актуальны угрозы 3-го типа и ИСПДн обрабатывает иные категории ПДн сотрудников оператора или иные категории ПДн менее чем 100000 субъектов ПДн, не являющихся сотрудниками оператора.

Уровень защищённости ПДн определяется комиссией по информационной безопасности. Результаты определения уровня защищённости ПДн оформляются актом классификации (см. шаблоны «Акт определения уровня защищенности информационной системы персональных данных «СЭД «ДЕЛО-АКО» министерства информационных технологий и связи Кировской области по требованиям защиты информации», приказ о создании комиссии по информационной безопасности).

После определения уровня защищённости ПДн, выбирается состав технических и организационных мер по защите ПДн при их обработке в ИСПДн. В зависимости от требуемого уровня защищённости ПДн к ИСПДН предъявляются разные требования по защите информации. Порядок определения состава и содержания технических и организационных мер по защите ПДн описан в пункте 3 настоящего документа.

Таблица – Определение уровня защищённости ПДн

Тип ИСПДн	Категории субъектов	Количество субъектов	Тип актуальных угроз		
			1	2	3
ИСПДн, в которых обрабатываются ПДн специальных категорий	не сотрудники	менее 100 000	УЗ 1	УЗ 2	УЗ 3
		более 100 000	УЗ 1	УЗ 1	УЗ 2
	сотрудники	менее 100 000	УЗ 1	УЗ 2	УЗ 3
		более 100 000	УЗ 1	УЗ 2	УЗ 3
ИСПДн, в которых обрабатываются биометрические ПДн	не сотрудники	менее 100 000	УЗ 1	УЗ 2	УЗ 3
		более 100 000	УЗ 1	УЗ 2	УЗ 3
	сотрудники	менее 100 000	УЗ 1	УЗ 2	УЗ 3
		более 100 000	УЗ 1	УЗ 2	УЗ 3
ИСПДн, в которых обрабатываются иные категории ПДн	не сотрудники	менее 100 000	УЗ 1	УЗ 3	УЗ 4
		более 100 000	УЗ 1	УЗ 2	УЗ 3
	сотрудники	менее 100 000	УЗ 1	УЗ 3	УЗ 4
		более 100 000	УЗ 1	УЗ 3	УЗ 4
ИСПДн, в которых обрабатываются общедоступные ПДн	не сотрудники	менее 100 000	УЗ 2	УЗ 3	УЗ 4
		более 100 000	УЗ 2	УЗ 2	УЗ 4
	сотрудники	менее 100 000	УЗ 2	УЗ 3	УЗ 4
		более 100 000	УЗ 2	УЗ 3	УЗ 4

УЗ – уровень защищённости.

3. Порядок определения состава и содержания технических и организационных мер по защите ПДн при их обработке в ИСПДн

В данном пункте перечисляются конкретные меры по обеспечению безопасности ПДн при их обработке в ИСПДн, состав и содержание которых устанавливается приказом ФСТЭК № 21, ПП № 1119 и приказом ФСБ № 378 в соответствии с уровнем защищённости ПДн (1, 2, 3 или 4), определяемого согласно ПП № 1119.

3.1. Порядок определения состава и содержания технических и организационных мер по защите ПДн при их обработке в ИСПДн согласно приказу ФСТЭК № 21

Сначала определяется базовый набор мер по обеспечению безопасности ПДн для выбранного по пункту 2 настоящего документа уровня защищённости ПДн. Порядок определения базового набора мер по обеспечению безопасности ПДн описан в пункте 3.1.1 настоящего документа.

3.1.1. Базовый набор мер по обеспечению безопасности ПДн при их обработке в ИСПДн для каждого уровня защищённости ПДн

Базовый набор мер по обеспечению безопасности ПДн – это набор мер, который определяется из таблицы 1 на основе выбранного по пункту 2 настоящего документа уровня защищённости ПДн (таблица взята из приказа ФСТЭК № 21). Для определённого уровня защищённости ПДн выписываем меры по обеспечению безопасности ПДн, обозначенные знаком "+".

Таблица 1 – Содержание мер по обеспечению безопасности ПДн

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности персональных данных			
		4	3	2	1
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)					
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+	+	+	+
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных			+	+
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+	+	+	+
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	+	+	+	+
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	+	+	+	+
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	+	+	+	+
II. Управление доступом субъектов доступа к объектам доступа (УПД)					
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	+	+	+	+
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	+	+	+	+
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами	+	+	+	+
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	+	+	+	+
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	+	+	+	+
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	+	+	+	+
УПД.7	Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры по обеспечению безопасности персональных данных, и о необходимости соблюдения				

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности персональных данных			
		4	3	2	1
	установленных оператором правил обработки персональных данных				
УПД.8	Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему				
УПД.9	Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя информационной системы				
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу		+	+	+
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации		+	+	+
УПД.12	Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки				
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	+	+	+	+
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа	+	+	+	+
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств	+	+	+	+
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	+	+	+	+
УПД.17	Обеспечение доверенной загрузки средств вычислительной техники			+	+
III. Ограничение программной среды (ОПС)					
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения				
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения			+	+
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов				+

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности персональных данных			
		4	3	2	1
ОПС.4	Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов				
IV. Защита машинных носителей персональных данных (ЗНИ)					
ЗНИ.1	Учет машинных носителей персональных данных			+	+
ЗНИ.2	Управление доступом к машинным носителям персональных данных			+	+
ЗНИ.3	Контроль перемещения машинных носителей персональных данных за пределы контролируемой зоны				
ЗНИ.4	Исключение возможности несанкционированного ознакомления с содержанием персональных данных, хранящихся на машинных носителях, и (или) использования носителей персональных данных в иных информационных системах				
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители персональных данных				
ЗНИ.6	Контроль ввода (вывода) информации на машинные носители персональных данных				
ЗНИ.7	Контроль подключения машинных носителей персональных данных				
ЗНИ.8	Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания		+	+	+
V. Регистрация событий безопасности (РСБ)					
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	+	+	+	+
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	+	+	+	+
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	+	+	+	+
РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти				
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них			+	+
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе				
РСБ.7	Защита информации о событиях безопасности	+	+	+	+

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности персональных данных			
		4	3	2	1
VI. Антивирусная защита (АВЗ)					
АВЗ.1	Реализация антивирусной защиты	+	+	+	+
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	+	+	+	+
VII. Обнаружение вторжений (СОВ)					
СОВ.1	Обнаружение вторжений			+	+
СОВ.2	Обновление базы решающих правил			+	+
VIII. Контроль (анализ) защищенности персональных данных (АНЗ)					
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей		+	+	+
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	+	+	+	+
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации		+	+	+
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации		+	+	+
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе			+	+
IX. Обеспечение целостности информационной системы и персональных данных (ОЦЛ)					
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации			+	+
ОЦЛ.2	Контроль целостности персональных данных, содержащихся в базах данных информационной системы				
ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций				
ОЦЛ.4	Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама)			+	+
ОЦЛ.5	Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и (или) контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из				

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности персональных данных			
		4	3	2	1
	информационной системы				
ОЦЛ.6	Ограничение прав пользователей по вводу информации в информационную систему				
ОЦЛ.7	Контроль точности, полноты и правильности данных, вводимых в информационную систему				
ОЦЛ.8	Контроль ошибочных действий пользователей по вводу и (или) передаче персональных данных и предупреждение пользователей об ошибочных действиях				
X. Обеспечение доступности персональных данных (ОДТ)					
ОДТ.1	Использование отказоустойчивых технических средств				
ОДТ.2	Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы				
ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование				+
ОДТ.4	Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных			+	+
ОДТ.5	Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала			+	+
XI. Защита среды виртуализации (ЗСВ)					
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	+	+	+	+
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	+	+	+	+
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре		+	+	+
ЗСВ.4	Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры				
ЗСВ.5	Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией				

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности персональных данных			
		4	3	2	1
ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных			+	+
ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций			+	+
ЗСВ.8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры			+	+
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре		+	+	+
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей		+	+	+
XII. Защита технических средств (ЗТС)					
ЗТС.1	Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам				
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования				
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены	+	+	+	+
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	+	+	+	+
ЗТС.5	Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов)				
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)					
ЗИС.1	Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты персональных данных, функций по обработке персональных данных и иных функций информационной системы				+
ЗИС.2	Предотвращение задержки или прерывания выполнения				

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности персональных данных			
		4	3	2	1
	процессов с высоким приоритетом со стороны процессов с низким приоритетом				
ЗИС.3	Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи	+	+	+	+
ЗИС.4	Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации)				
ЗИС.5	Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств				
ЗИС.6	Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с персональными данными, при обмене ими с иными информационными системами				
ЗИС.7	Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода				
ЗИС.8	Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи				
ЗИС.9	Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации				
ЗИС.10	Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам				
ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов			+	+
ЗИС.12	Исключение возможности отрицания пользователем факта отправки персональных данных другому пользователю				
ЗИС.13	Исключение возможности отрицания пользователем факта получения персональных данных от другого пользователя				

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности персональных данных			
		4	3	2	1
ЗИС.14	Использование устройств терминального доступа для обработки персональных данных				
ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных			+	+
ЗИС.16	Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер или внутри разрешенных сетевых протоколов				
ЗИС.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы			+	+
ЗИС.18	Обеспечение загрузки и исполнения программного обеспечения с машинных носителей персональных данных, доступных только для чтения, и контроль целостности данного программного обеспечения				
ЗИС.19	Изоляция процессов (выполнение программ) в выделенной области памяти				
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе		+	+	+
XIV. Выявление инцидентов и реагирование на них (ИНЦ)					
ИНЦ.1	Определение лиц, ответственных за выявление инцидентов и реагирование на них			+	+
ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов			+	+
ИНЦ.3	Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами			+	+
ИНЦ.4	Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий			+	+
ИНЦ.5	Принятие мер по устранению последствий инцидентов			+	+
ИНЦ.6	Планирование и принятие мер по предотвращению повторного возникновения инцидентов			+	+
XV. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)					
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных		+	+	+

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности персональных данных			
		4	3	2	1
УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты персональных данных		+	+	+
УКФ.3	Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных		+	+	+
УКФ.4	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных		+	+	+

Разъяснение (указание каким образом и в каком объёме должна быть реализована каждая мера защиты информации) перечисленных в таблице 1 требований по обеспечению безопасности ПДн приводится в подразделах «**требования к реализации меры защиты информации**» для каждой меры защиты раздела 3 методического документа «Меры защиты информации в государственных информационных системах», утверждённом ФСТЭК России 11.02.2014 (далее – методический документ ФСТЭК).

В случае, если для ИСПДн актуальны угрозы 1-го и 2-го типов, дополнительно к мерам по обеспечению безопасности ПДн, указанным в таблице 1, могут применяться следующие меры:

- проверка системного и (или) прикладного программного обеспечения, включая программный код, на отсутствие недекларированных возможностей с использованием автоматизированных средств и (или) без использования таковых;

- тестирование информационной системы на проникновения;

- использование в информационной системе системного и (или) прикладного программного обеспечения, разработанного с использованием методов защищённого программирования.

Указанные меры применяются по решению оператора. При этом порядок их применения, а также форма и содержание документов определяются оператором самостоятельно.

3.1.2. Адаптация базового набора мер

Далее необходимо выполнить адаптацию базового набора мер с учётом структурно-функциональных характеристик ИСПДн, информационных технологий, особенностей функционирования ИСПДн, то есть изменение изначально выбранного базового набора мер (определённого согласно п. 3.1.1 настоящего документа) в части его максимальной адаптации применительно к структуре, реализации и особенностям эксплуатации ИСПДн (в том числе исключение из базового набора мер).

Таким образом, при адаптации базового набора мер по обеспечению безопасности ПДн применяются меры по обеспечению безопасности ПДн, не обозначенные знаком "+", и (или) исключаются меры, обозначенные знаком "+".

Исключение мер, как правило, непосредственно связано с информационными технологиями, не используемыми в ИСПДн, или структурно-функциональными характеристиками, не свойственными ИСПДн. В качестве примера можно рассмотреть

исключение из базового набора мер защиты информации мер по защите среды виртуализации, в случае если в ИСПДн не применяется технология виртуализации, или исключение из базового набора мер защиты информации мер по защите мобильных технических средств, если такие мобильные устройства не применяются или их применение запрещено. В таблице 2 приводятся примеры обоснования изменения базового набора мер с указанием причин добавления, исключения или компенсирования мер.

Таблица 2 – Основания для исключения/добавления/компенсирования мер базового набора по обеспечению безопасности ПДн

Описание меры	**Основания для исключения/добавления/компенсирования**
УПД.13 Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	Действие: **Исключить из перечня мер** Технология обработки информации не предполагает удаленного доступа к ресурсам данных ИС
УПД.14 Регламентация и контроль использования в ИС технологий беспроводного доступа	Действие: **Исключить из перечня мер** Технология обработки информации не предполагает использования технологий беспроводного доступа к ресурсам данных ИС
УПД.15 Регламентация и контроль использования в ИС мобильных технических средств	Действие: **Исключить из перечня мер** Технология обработки информации не предполагает использования мобильных технических средств в данных ИС
ЗСВ.1 Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	Действие: **Исключить из перечня мер** Технология обработки информации не предполагает использования виртуальной инфраструктуры в данных ИС
ЗСВ.2 Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	Действие: **Исключить из перечня мер** Технология обработки информации не предполагает использования виртуальной инфраструктуры в данных ИС
ЗИС.3 Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы КЗ, в том числе беспроводным каналам связи	Действие: **Исключить из перечня мер** Технология обработки информации не предполагает передачи информации за пределы КЗ

3.1.3. Уточнение адаптированного базового набора мер

Уточнение определённого в п. 3.1.2 настоящего документа адаптированного базового набора мер осуществляется с учётом не выбранных ранее из таблицы 1 защитных мер, в результате чего определяются меры защиты информации, обеспечивающие блокирование (нейтрализацию) всех угроз безопасности информации, включённых в модель угроз.

Таким образом, исходными данными при уточнении адаптированного базового набора мер защиты информации является перечень угроз безопасности информации, включённый в модель угроз безопасности информации.

Модель угроз безопасности информации представляет собой формализованное описание угроз безопасности информации для конкретной информационной системы или группы информационных систем в определенных условиях их функционирования. Модель угроз безопасности информации разрабатывается обладателем информации (оператором, разработчиком (проектировщиком)) и должна по содержанию соответствовать требованиям по обеспечению безопасности ПДн при их обработке

в ИСПДн, утверждённым приказом ФСТЭК № 21, ПП № 1119, приказа ФСБ № 378 (все требования выписаны и перечислены в пунктах 3.1.1 и 3.2 настоящего документа).

Определение угроз безопасности информации и разработка модели угроз безопасности информации осуществляется в соответствии с руководящими документами ФСТЭК и ФСБ в области обеспечения безопасности ПДн при их обработке в ИСПДн (см. шаблон модель угроз).

В случае, если адаптированный базовый набор мер защиты информации, определённый в пункте 3.1.2 с учётом особенностей ИСПДн, не обеспечивает блокирование (нейтрализацию) всех угроз безопасности информации в него дополнительно вновь из таблицы 1 включаются другие меры защиты информации, не выбранные ранее.

В зависимости от уровня защищённости ПДн и потенциала нарушителя минимальные требования к реализации уточненного адаптированного базового набора мер защиты информации (приводится в подразделах «**требования к реализации меры защиты информации**» раздела 3 методического документа ФСТЭК) подлежат усилению для повышения уровня защищённости ПДн. Все возможные усиления мер защиты информации приведены в подразделах «**требования к усилению меры защиты информации**» для каждой меры защиты информации раздела 3 методического документа ФСТЭК.

Усиления мер защиты информации применяются дополнительно к требованиям по реализации мер защиты информации, приведенным в подразделах «**требования к реализации меры защиты информации**».

Итоговое содержание каждой усиленной уточненной адаптированной базовой меры защиты информации, которое как минимум, должно быть реализовано в ИСПДн, приведено в таблице подраздела «**содержание базовой меры защиты информации**».

Усиления мер защиты информации, приведенных в подразделе «**требования к усилению меры защиты информации**» и не включенные в таблицу с содержанием базовой меры защиты информации в подразделе «**содержание базовой меры защиты информации**», применяются по решению обладателя информации, заказчика и (или) оператора не только для уточнения адаптированного базового набора мер защиты информации, но и при адаптации (пункт 3.1.2 настоящего документа), а также для повышения уровня защищённости ПДн и разработке компенсирующих мер защиты информации.

3.1.4. Дополнение уточненного адаптированного базового набора мер

Настоящий пункт подразумевает дополнение уточненного адаптированного базового набора мер по обеспечению безопасности ПДн мерами, обеспечивающими выполнение требований к защите персональных данных, установленными иными нормативными правовыми актами в области обеспечения безопасности ПДн и защиты информации (например, в случае появления новых, исключения и (или) усиления (ужесточения) существующих требований к некоторым мерам защиты информации).

Рисунок 2 – Общий порядок действий по выбору мер защиты информации для их реализации в информационной системе

При невозможности реализации в ИСПДн отдельных выбранных мер защиты на этапах адаптации базового набора мер защиты информации или уточнения адаптированного базового набора мер защиты информации могут разрабатываться иные (компенсирующие) меры защиты информации, обеспечивающие адекватное блокирование (нейтрализацию) угроз безопасности информации.

3.2. Порядок определения состава и содержания технических и организационных мер по защите ПДн при их обработке в ИСПДн согласно ПП № 1119 и приказу ФСБ № 378

Кроме мер, установленных приказом ФСТЭК № 21, для обеспечения требуемого уровня защищённости ПДн должны выполняться требования ПП № 1119 и приказа ФСБ № 378. Эти меры для каждого уровня защищённости сведены в таблице 3.

Таблица 3 – Требования приказа ФСБ № 378

Требование	Уровни защищенности персональных данных			
	1	**2**	**3**	**4**
Организация режима обеспечения безопасности помещений, в которых размещена ИСПДн (далее – Помещения)				
Оснащение Помещений входными дверьми с замками, обеспечения постоянного закрытия дверей Помещений на замок и их открытия только для санкционированного прохода, а также опечатывания Помещений по окончании рабочего дня или оборудование Помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии Помещений	+	+	+	+
Утверждение правил доступа в Помещения в рабочее и нерабочее время, а также в нештатных ситуациях	+	+	+	+
Утверждение перечня лиц, имеющих право доступа в Помещения	+	+	+	+
Оборудование окон Помещений, расположенных на первых и (или) последних этажах зданий, а также окон Помещений, находящихся около пожарных лестниц и других мест, откуда возможно проникновение в Помещения посторонних лиц, металлическими решетками или ставнями, охранной сигнализацией или другими средствами, препятствующими неконтролируемому проникновению посторонних лиц в помещения	+			
Оборудование окон и дверей Помещений, в которых размещены серверы ИСПДн, металлическими решетками, охранной сигнализацией или другими средствами, препятствующими неконтролируемому проникновению посторонних лиц в помещения	+			
Обеспечение сохранности носителей персональных данных				
Хранение съемных машинных носителей персональных данных в сейфах (металлических шкафах), оборудованных внутренними замками с двумя или более дубликатами ключей и приспособлениями для опечатывания замочных скважин или кодовыми замками. В случае если на съемном машинном носителе персональных	+	+	+	+

Требование	Уровни защищенности персональных данных			
	1	**2**	**3**	**4**
данных хранятся только персональные данные в зашифрованном с использованием СКЗИ виде, допускается хранение таких носителей вне сейфов (металлических шкафов)				
Поэкземплярный учет машинных носителей персональных данных, который достигается путем ведения журнала учета носителей персональных данных с использованием регистрационных (заводских) номеров	+	+	+	+
Ведение электронного журнала сообщений				
Утверждение руководителем оператора списка лиц, допущенных к содержанию электронного журнала сообщений, и поддержание указанного списка в актуальном состоянии	+	+		
Обеспечение ИСПДн автоматизированными средствами, регистрирующими запросы пользователей ИСПДн на получение ПДн, а также факты предоставления ПДн по этим запросам в электронном журнале сообщений	+	+		
Обеспечение ИСПДн автоматизированными средствами, исключающими доступ к содержанию электронного журнала сообщений лиц, не указанных в утвержденном руководителем оператора списке лиц, допущенных к содержанию электронного журнала сообщений	+	+		
Обеспечение периодического контроля работоспособности автоматизированных средств (не реже 1 раза в полгода)	+	+		
Обеспечение ИСПДн автоматизированными средствами, позволяющими автоматически регистрировать в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к ПДн, содержащимся в ИСПДн	+			
Отражение в электронном журнале безопасности полномочий сотрудников оператора ПДн по доступу к ПДн, содержащимся в ИСПДн. Указанные полномочия должны соответствовать должностным обязанностям сотрудников оператора	+			
Назначение оператором лица, ответственного за периодический контроль ведения электронного журнала безопасности и соответствия отраженных в нем полномочий сотрудников оператора их должностным обязанностям (не реже 1 раза в месяц)	+			
Регламентация и контроль доступа к ПДн				
Разработка и утверждение документа, определяющего перечень лиц, доступ которых к ПДн, обрабатываемым в ИСПДн, необходим для выполнения ими служебных (трудовых) обязанностей	+	+	+	+
Поддержание в актуальном состоянии документ, определяющий перечень лиц, доступ которых к ПДн, обрабатываемым в ИСПДн, необходим для выполнения ими служебных (трудовых) обязанностей	+	+	+	+
Назначение обладающего достаточными навыками должностного лица (работника) оператора ответственным за обеспечение безопасности персональных данных в информационной системе	+	+	+	
Создание отдельного структурного подразделения, ответственного за обеспечение безопасности ПДн в ИСПДн, либо возложение его функций на одно из существующих структурных подразделений	+			
Проведение анализа целесообразности создания отдельного структурного подразделения, ответственного за обеспечение безопасности ПДн в ИСПДн	+			
Использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации				
Получение исходных данных для формирования совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак	+	+	+	+
Формирование и утверждение руководителем оператора совокупности предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак, и определение на этой основе и с учетом типа актуальных угроз требуемого класса средств криптографической защиты информации (далее – СКЗИ)	+	+	+	+

Таблица 4 – Классы СКЗИ

Класс защищённости ПДн	Класс СКЗИ
1	КА*/КВ и выше**
2	КА*/ КВ и выше**/КС1 и выше***
3	КВ и выше**/КС1 и выше***
4	КС1 и выше

Примечание:

* в случаях, когда для ИСПДн актуальны угрозы 1 типа;

** в случаях, когда для ИСПДн актуальны угрозы 2 типа;

*** в случаях, когда для ИСПДн актуальны угрозы 3 типа.

Примечание. Конкретные наименования СКЗИ перечисленных классов (КС1, КС2 и т.д.) выбираются согласно выписке из перечня средств защиты информации, сертифицированных ФСБ России (http://clsz.fsb.ru/certification.htm).

Требования к некриптогрфическим средствам защиты информации в зависимости от уровня защищённости ПДн следующие (пункт 12 приказа ФСТЭК № 21**)** приведены в таблице5.

Таблица 5 – Требования к некриптогрфическим средствам защиты информации

<table>
<tr><td rowspan="2">Наименование средства защиты информации</td><td colspan="4">Уровень защищённости ПДн</td></tr>
<tr><td>1</td><td>2</td><td>3</td><td>4</td></tr>
<tr><td>Средства вычислительной техники</td><td>не ниже 5 класса</td><td>не ниже 5 класса</td><td>не ниже 5 класса</td><td>не ниже 6 класса</td></tr>
<tr><td rowspan="2">Системы обнаружения вторжений</td><td rowspan="2">не ниже 4 класса</td><td rowspan="2">не ниже 4 класса</td><td>не ниже 4 класса***</td><td rowspan="2">не ниже 5 класса</td></tr>
<tr><td>не ниже 5 класса****</td></tr>
<tr><td rowspan="2">Средства антивирусной защиты</td><td rowspan="2">не ниже 4 класса</td><td rowspan="2">не ниже 4 класса</td><td>не ниже 4 класса***</td><td rowspan="2">не ниже 5 класса</td></tr>
<tr><td>не ниже 5 класса****</td></tr>
<tr><td rowspan="2">Межсетевые экраны</td><td>не ниже 3 класса*</td><td>не ниже 3 класса*</td><td>не ниже 3 класса***</td><td rowspan="2">5 класса</td></tr>
<tr><td>не ниже 4 класса**</td><td>не ниже 4 класса**</td><td>не ниже 4 класса****</td></tr>
<tr><td>Проверка наличия недекларированных возможностей</td><td>не ниже чем по 4 уровню контроля</td><td>не ниже чем по 4 уровню контроля</td><td>не ниже чем по 4 уровню контроля*****</td><td>–</td></tr>
</table>

* - в случае актуальности угроз 1-го или 2-го типов или взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена;

** - в случае актуальности угроз 3-го типа и отсутствия взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена;

*** - в случае актуальности угроз 2-го типа или взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена и системы обнаружения вторжений и средства

антивирусной защиты не ниже 5 класса защиты;

**** - в случае актуальности угроз 3-го типа и отсутствия взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена;

***** - в случае актуальности угроз 2-го типа.

Для обеспечения 1 и 2 уровней защищенности персональных данных, а также для обеспечения 3 уровня защищенности персональных данных в информационных системах, для которых к актуальным отнесены угрозы 2-го типа, применяются средства защиты информации, программное обеспечение которых прошло проверку не ниже чем по 4 уровню контроля отсутствия недекларированных возможностей.

Примечание. Конкретные наименования некриптографических средств защиты информации перечисленных классов защиты (3 класс, 4 класс и т.д.) выбираются из Государственного реестра сертифицированных средств защиты информации № РОСС RU.0001.01БИ00 (реестр размещён на официальном сайте ФСТЭК России (http://fstec.ru/) в разделе Техническая защита информация – Сертификация – Реестры).

Средства вычислительной техники выбираются согласно руководящему документу «Средства вычислительной техники. Защита от несанкционированного доступа к информации Показатели защищенности от несанкционированного доступа к информации», утверждённому 30 марта 1992 г.

После определения перечня мер по пунктам 3.1 и 3.2 настоящего документа итоговый перечень мер заносится в п. 2 шаблона «Состав и содержание мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (в шаблоне приведён пример перечня мер для 3-его уровня защищённости ПДн).

Контроль за выполнением настоящих требований организуется и проводится оператором (уполномоченным лицом) самостоятельно и (или) с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации. Указанный контроль проводится не реже 1 раза в 3 года в сроки, определяемые оператором (уполномоченным лицом).

При использовании в ИСПДн новых информационных технологий и выявлении дополнительных угроз безопасности ПДн, для которых не определены меры обеспечения их безопасности, должны разрабатываться соответствующие меры.