МИНИСТЕРСТВО
ОБРАЗОВАНИЯ И НАУКИ
РЕСПУБЛИКИ ТАТАРСТАН

ТАТАРСТАН РЕСПУБЛИКАСЫ
МӘГАРИФ ҺӘМ ФӘН
МИНИСТРЛЫГЫ

УКАЗАНИЕ **КҮРСӘТМӘ**

_____ г. Казань № _____

Руководителям отделов (управлений) образования исполнительных комитетов муниципальных образований Республики Татарстан

О состоянии информационной безопасности

Уважаемые коллеги!

Министерство образования и науки Республики Татарстан (далее – Министерство) информирует, что в период с 12 по 23 марта 2018 года Управление Федеральной службы безопасности Российской Федерации по Республике Татарстан проводит плановую выездную проверку в отношении Министерства по вопросу выполнения требований постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных».

С учетом изложенного дошкольным и общеобразовательным организациям вашего муниципального образования необходимо **в срок до 10 марта 2018 года** произвести обследование текущей инфраструктуры на предмет уязвимостей и актуализировать комплект организационно-распорядительной документации по вопросам информационной безопасности и обработки персональных данных в соответствии с примерным перечнем документов (приложение № 1), а также произвести регистрацию организации в качестве оператора по обработке персональных данных, если регистрация не производилась ранее.

Обращаем ваше внимание, что в связи со вступившими в силу с 1 июля 2017 года изменениями законодательства, в случае выявления нарушений по защите

персональных данных в ходе проверок соответствующими органами производится наложение штрафных санкций: на должностных лиц – до 20 тыс.рублей за одно нарушение, а также на юридических лиц (организацию) – до 75 тыс.рублей за одно нарушение (ст. 13.11 КоАП РФ), в особых случаях наступает уголовная ответственность (ст. 137, 272, 274 УК РФ) – лишение свободы на срок до 5 лет.

Просим довести указанную информацию до дошкольных и общеобразовательных организаций вашего муниципального образования и обеспечить контроль выполнения вышеуказанных мероприятий.

Приложения: 1. Примерный перечень организационно-распорядительной документации на 3 л. в 1 экз.

2. Таблица штрафов за нарушение законодательства в области персональных данных (ст. 13.11 КоАП РФ) на 3 л. в 1 экз.

Заместитель Премьер-министра
Республики Татарстан – министр **Р.Т.Бурганов**

А.А.Кравцов
(843) 294 95 75

Приложение № 1

Примерный перечень организационно-распорядительной документации

№ п/п	Наименование документа	Основание	КИ	ПДн	Примечание
	Приказы				
1	Приказ о назначении работника (структурного подразделения), ответственного за обеспечение безопасности конфиденциальной информации, в том числе ПДн	ФСТЭК	+	+	
2	Приказ о назначении работника (структурного подразделения), ответственного за выполнение работ по технической и криптографической защите ПДн	ФСБ		+	В случае использования СКЗИ
3	Приказ о составе комиссии по классификации автоматизированных систем	ФСТЭК	+		
4	Приказ о составе комиссии по классификации информационных систем персональных данных			+	
5	Приказ о выделении помещения (помещений) в котором производится обработка конфиденциальной информации, в том числе ПДн (в соответствии с тем в каких отделах, подразделениях организации обрабатываются ПДн). Приложение: список допущенных сотрудников	Роскомнадзор, ФСТЭК	+	+	
6	Приказ о назначении администраторов безопасности СЗ конфиденциальной информации, в том числе ПДн в целом и прикладных администраторов	ФСТЭК	+	+	
7	Приказ об утверждении мест хранения материальных носителей персональных данных	Роскомнадзор		+	В случае неавтоматизированной обработке ПДн
8	Приказ о назначении комиссии по уничтожению документов с ПД	Роскомнадзор		+	
9	Приказы <u>(на этапе ввода в эксплуатацию):</u> на проектирование объекта информатизации и назначение ответственных исполнителей: на проведение работ по защите информации; о назначении лиц, ответственных за эксплуатацию объекта информатизации; на обработку в АС (обсуждение в ЗП) конфиденциальной информации	ФСТЭК	+		
	Инструкции				
1	Инструкция по порядку учета и хранению съемных носителей конфиденциальной информации	ФСТЭК	+	+	
2	Инструкция, определяющая порядок охраны, внутри объектовый режим и порядок допуска лиц в помещения, в которых ведется обработка конфиденциальной информации, в том числе персональные данные	ФСТЭК	+	+	
	Положения				
1	Положение о порядке организации и проведения работ по защите конфиденциальной информации или приложение к руководству по защите информации от утечки по техническим каналам	ФСТЭК	+	+	
2	Положение о порядке обработки и обеспечении безопасности персональных данных	ФСТЭК, Роскомнад		+	

№ п/п	Наименование документа	Основание	КИ	ПДн	Примечание
		зор			
3	Положение о подразделении, осуществляющем функции по организации защиты персональных данных	ФСТЭК		+	При наличии
4	Положение (инструкция) о резервировании и восстановлении работоспособности ТС и ПО, баз данных и средств СЗПДн	ФСТЭК	+	+	
	Руководства				
1	Руководство пользователя по эксплуатации технических и программных средств защиты конфиденциальной информации	ФСТЭК	+	+	
2	Руководство администратора по эксплуатации технических и программных средств защиты конфиденциальной информации	ФСТЭК	+	+	
3	Руководство пользователя по обеспечению безопасности ИСПДн	ФСТЭК		+	
4	Руководство администратора по обеспечению безопасности ИСПДн	ФСТЭК		+	
	Журналы				
1	Журнал учета бумажных и съемных носителей конфиденциальной информации, в том числе ПДн	ФСТЭК	+	+	
2	Журнал регистрации и учета обращений субъектов персональных данных	ФСТЭК		+	Возможно ведение в электронной форме
3	Журнал ознакомления ответственных за обеспечение безопасности ПДн, за выполнение работ по защите ПДн под расписку с Типовыми требованиями и другими документами, регламентирующими организацию и обеспечение безопасности ПДн при их обработке в ИСПДн	ФСБ		+	
4	Журнал учета криптосредств, эксплуатационной и технической документации к ним	ФСБ		+	В случае использования СКЗИ
5	Журнал учета ключевых носителей	ФСБ		+	В случае использования СКЗИ
6	Журнала учета персональных данных для пропуска субъекта персональных данных на территорию оператора	ПП		+	При неавтоматизированной обработке
	Перечни				
1	Перечень используемых сертифицированных технических средств защиты информации (всех ТЗИ, так как все должны быть сертифицированы)	ФСТЭК	+	+	
2	Перечень сведений конфиденциального характера, подлежащих защите, в том числе ПДн и лист ознакомления к нему.	ФСТЭК	+	+	
3	Перечень АС и ИС, обрабатывающих конфиденциальную информацию и персональные данные	ФСТЭК	+	+	
4	Перечень эксплуатационной и технической документации, применяемых средств защиты информации	ФСТЭК	+	+	
5	Перечень носителей персональных данных	ФСТЭК		+	
	Списки				
1	Список помещений, в которых разрешена обработка конфиденциальной информации	ФСТЭК	+	+	Приложение к приказу
2	Утвержденный список лиц, допущенных в ЗП	ФСТЭК	+	+	
3	Утвержденный список лиц, допущенных к работе на автоматизированных системах (АС), также в ИСПДн	ФСТЭК	+	+	
4	Утвержденный список лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых)	ФСТЭК		+	

№ п/п	Наименование документа	Основание	КИ	ПДн	Примечание
	обязанностей				
	Акты				
1	Акт классификации АС	ФСТЭК	+		
2	Акт классификации ИСПДн и лист ознакомления сотрудников, в части касающейся	ФСТЭК		+	
3	Акт об уничтожении персональных данных субъекта (ов) персональных данных (в случае достижения цели обработки) (как в информационных системах, так и на бумажном носителе)	Роскомнадзор		+	в случае достижения цели обработки
	Модели				
1	Модель угроз безопасности информации	ФСТЭК	+		
2	Модель нарушителя	ФСТЭК	+		
3	Частная модель угроз безопасности ПДн	ФСТЭК		+	
	Планы				
1	План мероприятий по технической защите информации	ФСТЭК	+	+	
2	План мероприятий по защите персональных данных	ФСТЭК		+	
3	План внутренних проверок состояния защиты конфиденциальной информации	ФСТЭК	+		
4	План внутренних проверок состояния защиты персональных данных	ФСТЭК		+	
5	Планы устранения недостатков, выявленных в ходе проверок вопросов защиты информации	ФСТЭК	+	+	
	Другие				
1	Политика информационной безопасности органа исполнительной власти	ФСТЭК	+	+	
2	матрица доступа персонала к сведениям конфиденциального характера и разграничение доступа в соответствии с матрицей	ФСТЭК	+	+	
3	Описание конфигурации и топологии АС (ИСПДн), физических, функциональных и технологических связей внутри этих систем, так и с другими системами различного уровня и назначения, а также режимов обработки ПДн	ФСТЭК	+	+	
4	Условия расположения объекта информатизации относительно границы КЗ	ФСТЭК	+	+	
5	Технический паспорт объекта информатизации	ФСТЭК	+		
6	Технический паспорт на защищаемое помещение	ФСТЭК	+		
7	Ведомость приема зачетов по знанию действующего законодательства у лиц, допущенных к автоматизированной обработке конфиденциальной информации	ФСТЭК	+		
8	Заключение о готовности СЗИ к эксплуатации	ФСТЭК	+	+	
9	Копия уведомления об обработке персональных данных	Роскомнадзор		+	
10	Разделы должностных инструкций (должностного регламента) сотрудников имеющих доступ к ИСПДн, в части обеспечения безопасности ПДн	Роскомнадзор		+	
11	Типовые формы документов, предполагающие или допускающие содержание персональных данных	Роскомнадзор		+	
12	Копии договоров, заключённых между оператором и субъектом по основным направлениям деятельности, подтверждающего согласие субъекта персональных данных на их обработку	Роскомнадзор, 152-ФЗ		+	Если имеются
13	Письменное согласие субъектов персональных данных на обработку их персональных данных (типовая форма)	Роскомнадзор, 152-ФЗ		+	
14	Распечатка (копия) шаблона содержания персональных данных (формы и поля заполнения), определенных оператором, заверенных оператором и государственным инспектором, проводящим проверку	Роскомнадзор, 152-ФЗ		+	

Приложение № 2

Таблица штрафов за нарушение законодательства в области персональных данных, в соответствии со ст. 13.11 Кодекса об административных правонарушениях РФ

№ части статьи	Состав административного правонарушения	Нарушаемая статья законодательства	Возможность наложения предупреждения	Штраф для граждан	Штраф для должностных лиц	Штраф для ИП	Штраф для юридических лиц
1	**Обработка персональных данных в случаях, не предусмотренных законодательством РФ**, либо обработка персональных данных, несовместимая с целями сбора персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи	Ст.5, ст.6 ФЗ №152	да	1 — 3 тысячи рублей	5 — 10 тысяч рублей	не предусмотрен	30 — 50 тысяч рублей
2	**Обработка персональных данных без согласия** в письменной форме субъекта персональных данных в случаях, когда такое согласие должно быть получено в соответствии с законодательством РФ, если эти действия не содержат уголовно наказуемого деяния, либо обработка персональных данных с нарушением установленных законодательством РФ требований к составу сведений, включаемых в согласие в письменной форме субъекта персональных данных на обработку его персональных данных	Ст.9 ФЗ №152	нет	3 — 5 тысячи рублей	10 — 20 тысяч рублей	не предусмотрен	15 — 75 тысяч рублей
3	**Невыполнение оператором предусмотренной законодательством РФ обязанности по опубликованию** или обеспечению иным образом неограниченного доступа к документу, определяющему **политику оператора в отношении обработки персональных данных**, и сведениям о реализуемых требованиях к защите персональных данных	Ст.18.2 ФЗ №152	нет	700 — 1500 рублей	3 — 6 тысяч рублей	не предусмотрен	15 — 30 тысяч рублей

4	**Невыполнение оператором** предусмотренной законодательством РФ **обязанности по предоставлению субъекту** персональных данных **информации, касающейся обработки его персональных данных**	Ст.14, ст.20 ФЗ №152	да	1 — 2 тысячи рублей	4 — 6 тысяч рублей	10 — 15 тысяч рублей	20 — 40 тысяч рублей
5	**Невыполнение оператором** в сроки, установленные законодательством РФ, **требования субъекта** персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных **об уточнении** персональных данных, их **блокировании или уничтожении** в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки	Ст.21 ФЗ №152	да	1 — 2 тысячи рублей	4 — 10 тысяч рублей	10 — 20 тысяч рублей	25 — 45 тысяч рублей
6	**Невыполнение оператором** при обработке персональных данных без использования средств автоматизации **обязанности по соблюдению** условий, обеспечивающих в соответствии с законодательством РФ **сохранность** персональных данных при хранении материальных носителей персональных данных и исключающих несанкционированный к ним доступ, если это повлекло неправомерный или случайный доступ к персональным данным, их уничтожение, изменение, блокирование, копирование, предоставление, распространение либо иные неправомерные действия в отношении персональных данных, при отсутствии признаков уголовно наказуемого деяния	ПП №687	нет	700 — 2000 рублей	4 — 10 тысяч рублей	10 — 20 тысяч рублей	25 — 50 тысяч рублей

7	**Невыполнение оператором**, являющимся государственным или муниципальным органом, предусмотренной законодательством РФ **обязанности по обезличиванию персональных данных**, либо несоблюдение установленных требований или методов по обезличиванию персональных данных	ПП №211, приказ РКН №996	да	не предусмотрен	3 — 6 тысяч рублей	не предусмотрен	не предусмотрен

Лист согласования к документу № исх-275/18 от 15.02.2018
Инициатор согласования: Зинатуллин Р.Г. Ведущий советник отдела развития информационных технологий и безопасности
Согласование инициировано: 14.02.2018 13:35

Лист согласования Тип согласования: **смешанное**

N°	ФИО	Срок согласования	Результат согласования	Замечания
Тип согласования: **последовательное**				
1	Кравцов А.А.		Согласовано 14.02.2018 - 13:52	-
Тип согласования: **параллельное**				
2	Поминов А.И.		Согласовано 14.02.2018 - 15:49	-
3	Хадиуллин И.Г.		Согласовано 14.02.2018 - 14:41	-
4	Шарапов А.Р.		Согласовано 14.02.2018 - 22:06	-
Тип согласования: **последовательное**				
5	Бурганов Р.Т.		Подписано 14.02.2018 - 23:24	-