ПРИЛОЖЕНИЕ №4
УТВЕРЖДЕНО
Приказом «О вводе в действие комплекта организационно-распорядительной документации по организации обработки и защиты персональных данных» МБОУ Сокольская СШ
от 30.08.2024г. № 595

План внутреннего контроля обработки и защиты персональных данных в МБОУ Сокольская СШ

№ п/п	Содержание планируемого мероприятия	Периодичность	Дата проведения мероприятия	Ответственный
1.	Осуществление аудита (в том числе проведение инвентаризации информационных ресурсов с целью выявления в них ПДн) по установлению соответствия обработки персональных данных (далее- ПДн) Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон) и принятым в соответствии с ним нормативным правовым актам (наличие правовых оснований для обработки ПДн по каждой категории ПДн, независимо от способа обработки ПДн, а также соответствие целей обработки ПДн содержанию и объему обрабатываемых ПДн). (п.4. ч.1 ст.18.1. Федерального закона)	не реже одного раза в год		- ответственный за организацию обработки ПДн; - руководители структурных подразделений, работниками которых осуществляется обработка ПДн; - администратор безопасности информационных систем
2.	Проверка ознакомления работников, непосредственно осуществляющих обработку ПДн, с положениями законодательства Российской Федерации о ПДн, в том числе требованиями к защите ПДн, локальными актами по вопросам обработки и обеспечения безопасности ПДн.	не менее одного раза в полгода		- ответственный за организацию обработки ПДн; - руководители структурных подразделений, работниками которых осуществляется обработка ПДн;

	(п.6. ч.1 ст.18.1. Федерального закона)			
3.	Осуществление проверки получения согласий субъектов ПДн на обработку ПДн в случаях, когда этого требует законодательство Российской Федерации. (ст.9 Федерального закона)	не реже одного раза в полгода		- ответственный за организацию обработки ПДн; - руководители структурных подразделений, работниками которых осуществляется обработка ПДн
4.	Проверка подписания работниками, осуществляющими обработку ПДн, форм документов, необходимых в целях выполнения требований законодательства в сфере обработки и защиты ПДн, в том числе:			
4.1.	- документа об информировании о факте обработки ПДн без использования средств автоматизации; (п. 6 Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденного постановлением Правительства Российской Федерации от 15.09.2008 № 687);	не менее одного раза в полгода		- ответственный за организацию обработки ПДн; - руководители структурных подразделений, где осуществляется обработка ПДн с использованием бумажных носителей информации
4.2.	- обязательства о соблюдении конфиденциальности ПДн; (ст.7 Федерального закона)	не реже одного раза в полгода		- ответственный за организацию обработки ПДн; - администратор безопасности информационных систем; - руководитель подразделения кадрового аппарата
4.3.	- листов ознакомления с положениями законодательства Российской Федерации о ПДн, локальными актами МБОУ Сокольская СШ по вопросам обработки ПДн; (п.2 ч.4 ст.22.1 Федерального закона)	не менее одного раза в полгода		- ответственный за организацию обработки ПДн; - руководитель подразделения кадрового аппарата

4.4.	- разъяснения субъекту ПДн юридических последствий отказа предоставить свои ПДн. (ч.2 ст.18 Федерального закона)	не менее одного раза в полгода		- ответственный за организацию обработки ПДн; - руководитель подразделения кадрового аппарата
5.	Проверка в поручении (в случае заключения соответствующего договора) на обработку персональных данных: перечня действия (операций) с персональными данными, которые будут совершаться лицом, осуществляющим обработку персональных данных, цели обработки, обязанности соблюдения конфиденциальности персональных данных, обеспечения безопасности персональных данных при их обработке, а также требований к защите обрабатываемых персональных данных со статьей 19 Федерального закона. (ч.3 ст.6 Федерального закона)	не менее одного раза в год		- ответственный за организацию обработки ПДн; - руководители структурных подразделений, ответственных за подготовку договора
6.	Осуществление проверки фактического уничтожения ПДн, материальных носителей ПДн (бумажных и машинных), а также ПДн на носителях информации с составлением соответствующих актов уничтожения в порядке, установленном в МБОУ Сокольская СШ. (п.7 ст.5 Федерального закона)	не менее одного раза в полгода		- ответственный за организацию обработки ПДн; - руководители структурных подразделений, работниками которых осуществляется обработка ПДн
7.	Проверка ведения Журнала обращений субъектов ПДн или их представителей, а также обеспечение учета предоставления ПДн субъектов ПДн по письменным запросам третьих лиц, в порядке установленном Федеральным законом и действующим законодательством Российской Федерации. (ст.14 Федерального закона)	не менее одного раза в полгода		- ответственный за организацию обработки ПДн; - руководители структурных подразделений, работниками которых осуществляется обработка ПДн

8.	Осуществление проверки на предмет выявления изменений в правилах обработки и защиты ПДн, установленных в МБОУ Сокольская СШ в соответствии с действующим законодательством Российской Федерации. (ч.2. ст.24 Федерального закона, п.3 Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденного постановлением Правительства Российской Федерации от 15.09.2008 № 687)	не реже одного раза в год		- ответственный за организацию обработки ПДн; - руководители структурных подразделений, работниками которых осуществляется обработка ПДн; - администратор безопасности информационных систем
9.	Проверка наличия и актуальности Перечня персональных данных по каждой категории персональных данных, обрабатываемых в МБОУ Сокольская СШ, и Перечня информационных систем персональных данных в МБОУ Сокольская СШ. (ч.1 ст.10.1 Федерального закона, пп. «б» п.1 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 и муниципальными органами, утвержденного постановлением Правительства Российской Федерации от 15.09.2008 № 687)	Не реже одного раза в полгода		- ответственный за организацию обработки ПДн; - руководители структурных подразделений, работниками которых осуществляется обработка ПДн;
10.	Проверка соответствия установленных прав доступа к персональным данным в информационной системе (системах) персональных данных трудовым обязанностям работников Организации. (п.6. ч.2 ст.19 Федерального закона, п.8.2. Состава и содержания мер по обеспечению безопасности ПДн,	Не реже одного раза в полгода		- ответственный за организацию обработки ПДн; - руководители структурных подразделений, работниками которых осуществляется обработка ПДн; - администратор безопасности

	необходимых для обеспечения каждого из уровней защищенности ПДн, утвержденных приказом ФСТЭК России от 18.02.2013 № 21)			Информационных систем
11.	Реализация мероприятий по проверке актуализации Перечня мест хранения материальных носителей ПДн, соблюдения условий хранения материальных носителей ПДн, исключающих несанкционированный доступ к ним, а также раздельного хранения ПДн в случаях их обработки без использования средств автоматизации при несовместимости целей обработки ПДн. (п. 5 ч.2 ст.19 Федерального закона, п.14 и п.15 Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденного постановлением Правительства Российской Федерации от 15.09.2008 № 687, п.8.4. Состава и содержания мер по обеспечению безопасности ПДн, необходимых для обеспечения каждого из уровней защищенности ПДн, утвержденных приказом ФСТЭК России от 18.02.2013 № 21)	не менее одного раза в полгода		- ответственный за организацию обработки ПДн; - руководители структурных подразделений, работниками которых осуществляется обработка ПДн
12.	Проверка актуальности сведений, содержащихся в реестре операторов, осуществляющих обработку ПДн, которые размещены на официальном сайте уполномоченного органа по защите прав субъектов ПДн. (ст.22 Федерального закона).	не реже одного раза в полгода		- ответственный за организацию обработки ПДн
13.	Осуществление проверки по организации мероприятий по поддержанию в актуальном состоянии организационно-распорядительных документов по вопросам обработки ПДн, в том числе документов, определяющих политику Организации в отношении	не реже одного раза в полгода		- ответственный за организацию обработки ПДн; - руководители структурных подразделений, работниками которых осуществляется обработка ПДн,

	обработки ПДн. Обеспечение неограниченного доступа к Политике Организации в отношении обработки ПДн и сведениям о реализуемых требованиях к защите ПДн, в том числе размещение их на официальном сайте Организации в информационно-телекоммуникационной сети. (п.2 ч.1 ст.18.1 Федерального закона)			- администратор безопасности Информационных систем
14.	Проверка организации анализа и пересмотра имеющихся актуальных угроз безопасности ПДн. (п.2 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 01.11.2012 № 1119)	не реже одного раза в год		- ответственный за организацию обработки ПДн; - администратор безопасности Информационных систем
15.	Осуществление оценки вреда, который может быть причинен субъектам ПДн в случае нарушения Федерального закона с учетом соотношения указанного вреда и принимаемых Организацией мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом. (п.5 ч.1 ст.18.1 Федерального закона)	не реже одного раза в год		- ответственный за организацию обработки ПДн; - администратор безопасности Информационных систем
16.	Осуществление сверки Перечня помещений, в которых размещена информационная система персональных данных, утвержденного в Организации, фактическому размещению оборудования информационной системы персональных данных, включая средства защиты информации. (пп. «а» п. 13 Требований к защите персональных данных при их обработке в информационных системах персональных данных , утвержденных постановлением Правительства Российской Федерации от 01.11.2012 № 1119; п.8.12 Состава и содержания мер по	не реже одного раза в год		- ответственный за организацию обработки ПДн; - руководители структурных подразделений, работниками которых осуществляется обработка ПДн; - администратор безопасности Информационных систем

	обеспечению безопасности ПДн, необходимых для обеспечения каждого из уровней защищенности ПДн, утвержденных приказом ФСТЭК России от 18.02.2013 № 21)			
17.	Осуществление проверки актуальности утвержденного в Организации перечня лиц, доступ которых к ПДн, обрабатываемым в Организации, необходим для выполнения ими трудовых обязанностей. (пп. «в» п. 13 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 01.11.2012 № 1119, п.13 Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденного постановлением Правительства Российской Федерации от 15.09.2008 № 687)	не реже одного раза в полгода		- ответственный за организацию обработки ПДн; - руководители структурных подразделений, работниками которых осуществляется обработка ПДн; - администратор безопасности Информационных систем
18.	Проверка применения для обеспечения безопасности ПДн средств защиты информации, прошедших в установленном порядке процедуру соответствия. (п.3 ч.2 ст.19 Федерального закона)	не реже одного раза в полгода		- ответственный за организацию обработки ПДн; - администратор безопасности Информационных систем
19.	Проведение оценки эффективности принимаемых мер по обеспечению безопасности ПДн до ввода в эксплуатацию информационной системы ПДн (далее -Информационных систем). (п.4 ч.2 ст.19 Федерального закона, п.6 Состава и содержания мер по обеспечению безопасности ПДн, необходимых для обеспечения каждого из уровней защищенности ПДн, утвержденных приказом ФСТЭК России от 18.02.2013 № 21, п. 32 Порядка организации и проведения работ по аттестации объектов	до издания приказа о вводе в эксплуатацию информационной системы ПДн, далее - 1 раз в 3 года. В случае проведения такого мероприятия в форме аттестации –		- ответственный за организацию обработки ПДн; - администратор безопасности Информационных систем

	информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утвержденного приказом ФСТЭК России от 29.04.2021 № 77)	не реже одного раза в 2 года с направлением протокола контроля защиты информации в ФСТЭК России		
20.	Проведение проверки по обеспечению контроля за учетом машинных носителей персональных данных, на которых хранятся и (или) обрабатываются ПДн в информационной системе путем проведения сверки соответствия количества учтенных носителей фактическому, а также сверки заводских и учетных номеров, фактической проверки условий хранения и использования машинных носителей ПДн. (п.5 ч.2 ст.19 Федерального закона, п.8.4. Состава и содержания мер по обеспечению безопасности ПДн, необходимых для обеспечения каждого из уровней защищенности ПДн, утвержденных приказом ФСТЭК России от 18.02.2013 № 21)	не реже одного раза в полгода		- ответственный за организацию обработки ПДн; - администратор безопасностиИнформационных систем
21.	Проверка наличия приказа Организации о назначении работника, ответственного за обеспечение безопасности ПДн в Информационных систем (далее - администратор безопасности). (п. 14 Требований к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 01.11.2012 № 1119)	не реже одного раза в полгода		ответственный за организацию обработки ПДн
22.	Обеспечение контроля за принимаемыми мерами в связи с изменениями в структурно-функциональные характеристики Информационных систем.	не реже одного раза в квартал		- ответственный за организацию обработки ПДн; - администратор безопасности

	(абзац 2 п.9 Состава и содержания мер по обеспечению безопасности ПДн, необходимых для обеспечения каждого из уровней защищенности ПДн, утвержденных приказом ФСТЭК России от 18.02.2013 № 21)			Информационных систем
23.	Проверка реализации установленного в Организации порядка идентификации и аутентификации пользователей Информационных систем в соответствии с Инструкцией по идентификации и аутентификации. (п.8.1 Состава и содержания мер по обеспечению безопасности ПДн, необходимых для обеспечения каждого из уровней защищенности ПДн, утвержденных приказом ФСТЭК России от 18.02.2013 № 21)	не реже одного раза в квартал		- ответственный за организацию обработки ПДн; - администратор безопасности Информационных систем
24.	Проверка регистрации событий информационной безопасности в Информационных систем в соответствии с Инструкцией по управлению событиями информационной безопасности, утвержденной в Организации. (п.8.5 Состава и содержания мер по обеспечению безопасности ПДн, необходимых для обеспечения каждого из уровней защищенности ПДн, утвержденных приказом ФСТЭК России от 18.02.2013 № 21)	не реже одного раза в полгода		- ответственный за организацию обработки ПДн; - администратор безопасности Информационных систем
25.	Осуществление проверки реализации в Организации выявления инцидентов информационной безопасности и реагирования на них при наличии запланированных работ по аттестации Информационных систем. (п.6 ч.2 ст.19 Федерального закона, пп. «ж» п. 11	не реже одного раза в год		- ответственный за организацию обработки ПДн; - администратор безопасности Информационных систем

	Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утвержденного приказом ФСТЭК России от 29.04.2021 № 77)			
26.	Проверка организации антивирусной защиты в Информационных систем и регулярности обновления базы данных признаков вредоносных программ (вирусов). (п.8.6 Состава и содержания мер по обеспечению безопасности ПДн, необходимых для обеспечения каждого из уровней защищенности ПДн, утвержденных приказом ФСТЭК России от 18.02.2013 № 21)	не реже одного раза в полгода		- ответственный за организацию обработки ПДн; - администратор безопасности Информационных систем
27.	Осуществление проверки по реализации мероприятий по выявлению, анализу и устранению уязвимостей в Информационных систем при наличии запланированных работ по проведению аттестации Информационных систем. (пп. «з» п. 11 Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утвержденного приказом ФСТЭК России от 29.04.2021 № 77)	не реже одного раза в год		- ответственный за организацию обработки ПДн; - администратор безопасности Информационных систем
28.	Организация проведения проверки по реализации мероприятий по установке обновлений программного обеспечения, в том числе обновление программного обеспечения средств защиты информации.	не реже одного раза в год		- ответственный за организацию обработки ПДн; - администратор безопасности Информационных систем

	(АНЗ.2 в Приложении к Составу и содержанию мер по обеспечению безопасности ПДн, необходимых для обеспечения каждого из уровней защищенности ПДн, утвержденных приказом ФСТЭК России от 18.02.2013 № 21)			
29.	Проверка организации размещения технических средств отображения информации Информационных систем, исключая ее несанкционированный просмотр, в соответствии с Инструкцией по защите технических средств Информационных систем, утвержденной в Организации. (п.6 ч.2 ст.19 Федерального закона, ЗТС.4 в Приложении к Составу и содержанию мер по обеспечению безопасности ПДн, необходимых для обеспечения каждого из уровней защищенности ПДн, утвержденных приказом ФСТЭК России от 18.02.2013 № 21)	не менее одного раза в квартал		- ответственный за организацию обработки ПДн; - руководители структурных подразделений, работниками которых осуществляется обработка ПДн; - администратор безопасности Информационных систем
30.	Проверка состояния работы по реализации процесса управления конфигурацией Информационных систем и системы защиты ПДн в случае, если запланировано проведение работ по аттестации Информационных систем. (пп. «ж» п. 11 Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утвержденного приказом ФСТЭК России от 29.04.2021 № 77)	не менее одного раза в год		- ответственный за организацию обработки ПДн; - администратор безопасности Информационных систем
31.	Проверка состава технических средств, программного обеспечения и средств защиты информации, входящих в состав Информационных	не реже одного раза в полгода		- ответственный за организацию обработки ПДн; - руководители структурных

	систем на соответствие Техническому паспорту Информационных систем в случае, если запланировано проведение работ по аттестации Информационных систем. (п. 33 Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утвержденного приказом ФСТЭК России от 29.04.2021 № 77)			подразделений, работниками которых осуществляется обработка ПДн; - администратор безопасности Информационных систем