УТВЕРЖДАЮ:
Заведующий МБДОУ
«Вагановский д/с»

_____ С.Л. Савченко
«___»_____ 2021 года

План
мероприятий по защите информации в информационной системе МБДОУ «Вагановский д/с»

1. Общие положения

1.1. План мероприятий по защите информации в информационной системе **МБДОУ «Вагановский д/с»** (далее – План) содержит перечень мероприятий и требований.

1.2. План разработан в соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

1.3. План содержит следующую информацию:

- формирование требований к защите информации, содержащейся в информационной системе МБДОУ «Вагановский д/с» (далее – ИС);
- разработка системы защиты информации ИС;
- внедрение системы защиты информации ИС;
- обеспечение защиты информации в ходе эксплуатации ИС;

2. Планирование мероприятий

1.1. Для обеспечения защиты информации, содержащейся в ИС, проводятся мероприятия, которые представлены в Таблице 1.

Таблица 1. План мероприятий.

№ п/п	Мероприятие	Сроки (периодичность) выполнения	Примечание
1	2	3	4
1. Формирование требований к защите информации, содержащейся в ИС			
1.1.	Принятие решения о необходимости защиты информации, содержащейся в ИС	-	-
1.2.	Классификация ИС по требованиям защиты информации и определение уровня защищенности персональных данных (далее – ПДн) при их обработке в ИС	Перед созданием системы защиты и при необходимости в ходе эксплуатации ИС	Определение класса защищенности ИС и уровня защищенности ПДн при их обработке в ИС осуществляется при создании ИС, а также в ходе эксплуатации при изменении состава, структуры ИС или технических особенностей ее построения (при изменении программного обеспечения, топологии и т.д.).
1.3.	Определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в ИС, и разработка на их основе модели угроз безопасности информации	Перед созданием системы защиты и в ходе эксплуатации ИС при выявлении новых уязвимостей	РазрабатываетсяУточняетсяМодель угроз безопасности и модель нарушителя безопасности информации.
1.4.	Определение требований к системе защиты информации ИС	Перед созданием системы защиты	Разрабатывается техническое задание на создание системы защиты информации ИС.
2. Разработка системы защиты информации ИС			
2.1.	Проектирование системы защиты информации ИС	До ввода в эксплуатацию и при необходимости	Разработка Проекта на систему защиты. Выбор мер по защите информации проводится исходя из класса защищенности ИС, уровня защищенности ПДн при их обработке в ИС и угроз безопасности информации, включенных в Модель угроз безопасности, а также с учетом структурно-функциональных характеристик ИС. Определяются виды и типы средств защиты информации, обеспечивающие реализациютехнических мер защиты информации. Определяется структура системы защиты информации ИС, включаясостав (количество) и места размещения ее элементов. Осуществляется выбор средств защиты информации, сертифицированных на соответствиетребованиям по безопасности информации, с учетом их стоимости, совместимости синформационными технологиями и техническими средствами, функций безопасности
2.2.	Разработка эксплуатационной документации на систему защиты информации ИС		

№ п/п	Мероприятие	Сроки (периодичность) выполнения	Примечание
1	2	3	4
			этихсредств и особенностей их реализации, а также класса защищенности ИС и уровня защищенности ПДн при их обработке в ИС. Определяются требования к параметрам настройки программного обеспечения, включаяпрограммное обеспечение средств защиты информации, обеспечивающие реализацию мерзащиты информации, а также устранение возможных уязвимостей ИС,приводящих к возникновению угроз безопасности информации.
3. Внедрение системы защиты информации ИС			
3.1.	Установка и настройка средств защиты информации в ИС	До ввода в эксплуатацию и при необходимости	Установка и настройка средств защиты информации в соответствии с эксплуатационной документацией на систему защитыинформации ИС и документацией на средства защиты информации.
3.2.	Разработка документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в ИС в ходе ее эксплуатации	До ввода в эксплуатацию и при необходимости	Разработка организационно-распорядительных документов по защите информации.
3.3.	Внедрение организационных мер защиты информации	До ввода в эксплуатацию и при необходимости	Реализация правил разграничения доступа, регламентирующих права доступа субъектов доступа к объектам доступа, и введение ограничений на действия пользователей, а также на изменение условий эксплуатации, состава и конфигурации технических средств и программного обеспечения; Проверка полноты и детальности описания в организационно-распорядительных документах по защите информации действий пользователей и администраторов ИС по реализации организационных мер защиты информации; Отработка действий должностных лиц и подразделений, ответственных за реализацию мер защиты информации.
3.4.	Предварительные испытания системы защиты информации ИС	До ввода в эксплуатацию и при необходимости	Проверка работоспособностисистемы защиты информации ИС, а также принятие решения овозможности опытной эксплуатации системы защиты информации ИС.

№ п/п	Мероприятие	Сроки (периодичность) выполнения	Примечание
1	2	3	4
3.5.	Опытная эксплуатация системы защиты информации ИС	До ввода в эксплуатацию и при необходимости	Проверка функционирования системы защиты информации ИС, в том числе реализованных мер защиты информации, а также готовность пользователей и администраторов к эксплуатации системы защиты информации ИС.
3.6.	Анализ уязвимостей ИС и принятие мер защиты информации по их устранению	До ввода в эксплуатацию и при необходимости	Проведение анализа уязвимостей средствзащиты информации, технических средств и программного обеспечения ИС. Уточнениемодели угроз безопасности информации и при необходимости принятие дополнительныемеры защиты информации, в случае выявления уязвимостей ИС, приводящих к возникновению дополнительных угроз безопасности информации.
3.7.	Приемочные испытания системы защиты информации ИС	До ввода в эксплуатацию и при необходимости	Проверка выполнения требований к системе защиты информации ИС в соответствии с техническим заданием насоздание системы защиты информации ИС.
3.8.	Аттестация ИС по требованиям защиты информации и ввод ее в действие	До ввода в эксплуатацию и при необходимости	Проводится совместно с лицензиатами ФСТЭК России.
4. Обеспечение защиты информации в ходе эксплуатации аттестованной ИС			
4.1.	Планирование мероприятий по защите информации в ИС	Вместе с вводомИС в эксплуатацию	Разработка, утверждение и актуализация плана мероприятий по защите информации в ИС.
4.2.	Анализ угроз безопасности информации в ИС	Не реже одного раза в квартал; При внедрении новых узлов и/или технологий в ИС; При появлении информации о новых уязвимостях	В ходе анализа угроз безопасности информации в ИС в ходе ееэксплуатации осуществляются: выявление, анализ и устранение уязвимостей ИС; анализ изменения угроз безопасности информации в ИС; оценка возможных последствий реализации угроз безопасности информации в ИС.
4.3.	Управление (администрирование) системой защиты информации ИС	Постоянно в ходе эксплуатации ИС	В ходе управления (администрирования) системой защиты информации ИС осуществляются: управление учетными записями пользователей и поддержание в актуальном состоянии правил разграничения доступа в ИС; управление средствами защиты информации ИС;

№ п/п	Мероприятие	Сроки (периодичность) выполнения	Примечание
1	2	3	4
			управление обновлениями программных и программно-аппаратных средств, в том числе средств защиты информации, с учетом особенностей функционирования ИС; мониторинг и анализ события безопасности зарегистрированных в ИС; обеспечение функционирования системы защиты информации информационной системы в ходе ее эксплуатации, включая ведение эксплуатационной документации и организационно-распорядительных документов по защите информации.
4.4.	Управление конфигурацией аттестованной ИС и ее системой защиты информации	Постоянно в ходе эксплуатации ИС	В ходе управления конфигурацией ИС и ее системы защитыинформации осуществляются: определение компонентов ИС и ее системы защиты информации,подлежащих изменению в рамках управления конфигурацией; управление изменениями ИС и ее системы защиты информации: разработка параметров настройки, обеспечивающих защиту информации, анализ потенциального воздействия планируемых изменений на обеспечение защиты информации, санкционирование внесения изменений в ИС и ее систему защиты информации, документирование действий по внесению изменений в ИС и сохранение данных об изменениях конфигурации; контроль действий по внесению изменений в ИС и ее систему защиты информации.
4.5.	Выявление инцидентов и реагирование на них	Постоянно в ходе эксплуатации ИС; Не реже одного раза в год проведение внутреннего аудита информационной безопасности	В ходе реагирования на инциденты осуществляются: обнаружение и идентификация инцидентов, в том числе отказов в обслуживании, сбоев(перезагрузок) в работе технических средств, программного обеспечения и средств защитыинформации, нарушений правил разграничения доступа, неправомерных действий по сборуинформации, внедрений вредоносных компьютерных программ

№ п/п	Мероприятие	Сроки (периодичность) выполнения	Примечание
1	2	3	4
			(вирусов) и иных событий,приводящих к возникновению инцидентов; своевременное информирование пользователями и администраторами лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов винформационной системе; анализ инцидентов, в том числе определение источников и причин возникновенияинцидентов, а также оценка их последствий; планирование и принятие мер по устранению инцидентов, в том числе по восстановлениюИС и ее сегментов в случае отказа в обслуживании или после сбоев,устранению последствий нарушения правил разграничения доступа, неправомерных действийпо сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иныхсобытий, приводящих к возникновению инцидентов.
4.6.	Информирование и обучение персонала ИС	Не реже одного раза в два года	В ходе информирования и обучения персонала ИС осуществляются: информирование персонала ИС о появлении актуальных угроз безопасности информации, о правилах безопасной эксплуатации ИС; доведение до персонала ИС требований по защите информации, а также положений организационно-распорядительных документов по защите информации с учетом внесенных в них изменений; обучение персонала ИС правилам эксплуатации отдельных средств защиты информации; проведение практических занятий и тренировок с персоналом ИС по блокированию угроз безопасности информации и реагированию на инциденты; контроль осведомленности персонала ИС об угрозах безопасности информации и уровня знаний

№ п/п	Мероприятие	Сроки (периодичность) выполнения	Примечание
1	2	3	4
			персонала по вопросам обеспечения защиты информации.
4.7.	Контрольза обеспечением уровня защищенности информации, содержащейся в ИС	Не реже одного раза в два года	В ходе контроля за обеспечением уровня защищенности информации, содержащейсяв ИС, осуществляются: контроль (анализ) защищенности информации с учетом особенностей функционирования ИС; анализ и оценка функционирования ИС и ее системы защитыинформации, включая анализ и устранение уязвимостей и иных недостатков вфункционировании системы защиты информации ИС; документирование процедур и результатов контроля за обеспечением уровнязащищенности информации, содержащейся в ИС; принятие решения по результатам контроля за обеспечением уровня защищенностиинформации, содержащейся в ИС, о необходимости доработки(модернизации) ее системы защиты информации. Контроль за обеспечением уровня защищенности информации, содержащейся в ИС, проводится самостоятельно и (или) с привлечениеморганизации, имеющей лицензию на деятельность по технической защите конфиденциальнойинформации.
5.	**Обеспечение защиты информации при выводе из эксплуатации аттестованной ИС или после принятия решения об окончании обработки информации**		
5.1.	Архивирование информации, содержащейся в ИС	При выводе из эксплуатации аттестованной ИС или после принятия решения об окончании обработки информации	Архивирование информации, содержащейся в ИС, должноосуществляться при необходимости ее дальнейшего использования.
5.2.	Уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации	При выводе из эксплуатации аттестованной ИС или после принятия решения об окончании обработки информации	Уничтожение (стирание) данных и остаточной информации с машинных носителейинформации производится при необходимости передачи машинного носителя информациидругому пользователю ИС. При выводе из эксплуатации машинных носителей

№ п/п	Мероприятие	Сроки (периодичность) выполнения	Примечание
1	2	3	4
			информации, на которыхосуществлялись хранение и обработка информации, осуществляется физическое уничтожениеэтих машинных носителей информации.

В План могут быть включены следующие последовательно реализуемые пункты порядка создания системы:

- разработка документации на систему и ее части;
- разработка рабочей документации на систему и ее части;
- разработка или адаптация программного обеспечения;
- пусконаладочныеработы.