Утверждаю
Заведующая МДОУ
Тисульского детского сада № 4
_____ О.М. Ефимова
Приказ № 173 от 15.11. 2018г.

Инструкция
по проведению мониторинга информационной безопасности и антивирусного контроля

1. Инструкция по проведению мониторинга концепции информационной безопасности и антивирусного контроля (далее – Инструкция) регламентирует порядок планирования и проведения мероприятий, направленных на обеспечение безопасности автоматизированных систем, обрабатывающих персональные данные, от несанкционированного доступа, распространения, искажения и утраты информации, необходимого при работе учреждения

2. Мониторинг работоспособности аппаратных компонентов автоматизированных систем, обрабатывающих персональные данные, осуществляется в процессе их администрирования и при проведении работ по техническому обслуживанию оборудования. Наиболее существенные компоненты системы, имеющие встроенные средства контроля работоспособности (серверы, активное сетевое оборудование), должны постоянно контролироваться в рамках работы администраторов соответствующих систем.

3. Мониторинг парольной защиты предусматривает: контроль соблюдения сроков действия паролей (не более года); периодическую (не реже одного раза в 3 месяца) проверку пользовательских паролей на количество символов и очевидность с целью выявления слабых паролей, которые легко угадать или дешифровать с помощью специализированных программных средств ("взломщиков" паролей).

4. Мониторинг целостности программного обеспечения включает: проверку контрольных сумм и цифровых подписей каталогов и файлов сертифицированных программных средств; проверку и восстановление системных файлов администраторами систем с резервных копий при несовпадении контрольных сумм.

5. Мероприятия, направленные на предупреждение и своевременное выявление попыток несанкционированного доступа.

6. Системный аудит производится ежеквартально и в особых ситуациях. Он включает в себя проведение обзоров безопасности, тестирование системы и контроль внесения изменений в системное программное обеспечение.

7. Обзоры безопасности проводятся с целью проверки соответствия текущего состояния систем, обрабатывающих персональные данные, уровню безопасности, удовлетворяющему требованиям политики безопасности; анализ данных об обнаружении изменений системных файлов со времени проведения последней проверки (контроль целостности системных файлов); проверку прав доступа и других атрибутов системных файлов (команд, утилит и таблиц).

8. Активное тестирование надежности механизмов контроля доступа производится путем осуществления попыток проникновения в информационную систему с помощью автоматического инструментария или вручную.

9. Внесение изменений в системное программное обеспечение осуществляется администраторами систем, обрабатывающих персональные данные.

10. Для защиты от вредоносных программ и вирусов необходимо использовать только лицензионные или сертифицированные свободно распространяемые антивирусные средства.

11. Для защиты серверов и рабочих станций используются: резидентные антивирусные мониторы, контролирующие подозрительные действия программ; утилиты для обнаружения и анализа новых вирусов.

12. При подозрении на наличие не выявленных установленными средствами защиты заражений следует использовать Live CD с другими антивирусными средствами.

13. Установка и настройка средств защиты от вредоносных программ и вирусов на рабочих станциях и серверах автоматизированных систем, обрабатывающих персональные данные, осуществляется администраторами соответствующих систем в соответствии с руководствами по установке приобретенных средств защиты.

14. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено администратором системы на отсутствие вредоносных программ и компьютерных вирусов.

15. Запуск антивирусных программ осуществляется автоматически по заданию, созданному с использованием планировщика задач, входящего в поставку операционной системы либо поставляемого вместе с антивирусными программами.

16. Антивирусный контроль рабочих станций проводится ежедневно в автоматическом режиме. Если проверка всех файлов на дисках рабочих станций занимает неприемлемо большое время, то допускается проводить выборочную проверку загрузочных областей дисков, оперативной памяти, критически важных инсталлированных файлов операционной системы и загружаемых файлов по сети или с внешних носителей. В этом случае полная проверка осуществляется не реже одного раза в неделю в период неактивности пользователя. Пользователям рекомендуется проводить полную проверку во время перерыва на обед.

19. Обязательному антивирусному контролю подлежит любая информация (исполняемые файлы, текстовые файлы любых форматов, файлы данных), получаемая пользователем по сети или загружаемая со съемных носителей (магнитных дисков, оптических дисков, флэш-накопителей и т. п.). Контроль информации проводится антивирусными средствами в процессе или сразу после ее загрузки на рабочую станцию пользователя.

20. Антивирусные базы на всех рабочих станциях и серверах необходимо регулярно обновлять.

21. Если администратор системы, обрабатывающей персональные данные, подозревает или получил сообщение о том, что его система подвергается атаке или уже была скомпрометирована, он должен определить системные ресурсы, безопасность которых была нарушена, и установить: была ли попытка несанкционированного доступа (далее – НСД); когда, как и при каких обстоятельствах была предпринята попытка НСД; продолжается ли НСД в настоящий момент; кто является источником НСД; что является объектом НСД; какова была мотивация нарушителя; точку входа нарушителя в систему; была ли попытка НСД успешной.

22. Для выявления попытки НСД необходимо: установить, какие пользователи в настоящее время работают в системе и на каких рабочих станциях; выявить подозрительную активность пользователей, проверить, все ли пользователи вошли в систему со своих рабочих мест и не работает ли кто из них в системе необычно долго; убедиться, что никто из пользователей не использует подозрительные программы или программы, не относящиеся к его области деятельности.

23. Для обнаружения в системе следов, оставленных злоумышленником в виде файлов, вирусов, троянских программ, изменения системной конфигурации следует: составить базовую схему того, как обычно выглядит система; провести поиск подозрительных файлов, скрытых файлов, имен файлов и каталогов, которые обычно используются злоумышленниками; проверить содержимое системных файлов, которые обычно изменяются злоумышленниками; оценить целостность системных программ; проверить систему аутентификации и авторизации.

30. Особенности мониторинга информационной безопасности персональных данных в отдельных автоматизированных системах могут регулироваться дополнительными инструкциями.

31. Работники организации и лица, выполняющие работы по договорам и контрактам, имеющие отношение к проведению мониторинга информационной безопасности и антивирусного контроля при обработке персональных данных, должны быть ознакомлены с Инструкцией под расписку.

С инструкцией по проведению мониторинга информационной безопасности и антивирусного контроля ознакомлены:

№ п/п	Дата	ФИО	Должность	Подпись