УТВЕРЖДАЮ
Заведующий МБДОУ «Детский сад №17»
_____И.А.Шестопалова
«06» июня 2017 г.

ИНСТРУКЦИЯ
АДМИНИСТРАТОРА БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Инструкция администратора безопасности информационной системы персональных данных (далее – Инструкция) разработана в целях обеспечения необходимого уровня состояния защиты информационной системы персональных данных, правильности настройки средств защиты, организации выдачи, хранения и уничтожения материальных носителей персональных данных.

1.2. Администратор безопасности информационной системы персональных данных (далее - администратор безопасности) назначается и освобождается от исполнения своих обязанностей приказом заведующего МБДОУ «Детский сад №17» (далее – Организация), в пределах полномочий подчиняется ответственному лицу за организацию обработки персональных данных.

II. ОБЯЗАННОСТИ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

2.1. Администратор безопасности обязан:

2.1.1. Утверждать изменения состава и конфигурации технических и программных средств после их анализа на соответствие политике безопасности.

2.1.2. Проверять добавляемые компоненты на работоспособность и отсутствие вирусов.

2.1.3. Разрабатывать и исполнять утверждённый план проведения мониторинга информационной безопасности автоматизированных систем, обрабатывающих персональные данные, от несанкционированного распространения и доступа, искажения и утраты информации.

2.1.4. Вести разъяснительную работу с работниками Организации по вопросам информационной безопасности.

2.1.5. Обеспечивать полное уничтожение персональных данных с электронных носителей в случаях их передачи для обслуживания или ремонта.

2.1.6. Обеспечивать уничтожение со съёмных носителей персональных данных, не предназначенных для дальнейшего использования, методом многократной перезаписи без возможности восстановления.

2.1.7. Проверять электронный журнал обращений к информационной системе персональных данных.

2.1.8. Контролировать надлежащее функционирование программных и технических средств защиты информации, входящих в состав информационной системы персональных данных, во всех режимах работы, а именно:

- использование только лицензионного (сертифицированного) программного обеспечения;
- использование только сертифицированных средств защиты информации;
- соблюдение условий использования и правильность конфигурирования (настройки) средств защиты информации.

2.1.9. Проводить разбирательства и составлять заключения по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации.

2.1.10. Осуществлять уничтожение пришедших в негодность материальных носителей персональных данных с составлением акта.

III. ВИДЫ МОНИТОРИНГА

3.1. Мониторинг парольной защиты и контроль надёжности пользовательских паролей предусматривают:

3.1.1. Установление минимального и максимального сроков действия паролей.

3.1.2. Периодическую проверку пользовательских паролей на количество символов и очевидность с целью выявления слабых паролей.

3.2. Мониторинг целостности программного обеспечения включает следующие действия:

3.2.1. Проверка контрольных сумм и цифровых подписей каталогов и файлов сертифицированных программных средств защиты при загрузке операционной системы.

3.2.2. Обнаружение дубликатов идентификаторов пользователей.

3.2.3. Восстановление системных файлов администраторами систем с резервных копий при несовпадении контрольных сумм.

3.3. Антивирусный контроль:

3.3.1. Регулярное обновление антивирусных баз на рабочих станциях и серверах.

IV. СИСТЕМНЫЙ АУДИТ

4.1. Системный аудит проводится ежеквартально и в особых ситуациях. Он включает проведение обзоров безопасности, тестирование системы, контроль внесенных изменений в системное программное обеспечение.

4.2. Обзоры безопасности проводятся с целью проверки текущего уровня безопасности систем, обрабатывающих персональные данные, выявление всех несоответствий между текущим состоянием системы и состоянием, соответствующем специально составленному списку для проверки.

4.3. Обзоры безопасности содержат:

4.3.1. Отчёты о безопасности пользовательских ресурсов, включающие наличие повторяющихся пользовательских имён и идентификаторов, неправильных форматов регистрационных записей, пользователей без пароля, неправильной установки домашних каталогов пользователей и уязвимостей пользовательских окружений.

4.3.2. Проверку правомочности предоставления прав доступа пользователей к сетевым ресурсам.

4.3.3. Проверку содержимого файлов конфигурации на соответствие списку для проверки.

4.3.4. Обнаружение изменений системных файлов со времени проведения последней проверки (контроль целостности системных файлов).

4.3.5. Проверку прав доступа и других атрибутов системных файлов.

4.3.6. Проверку правильности настройки механизмов аутентификации и авторизации сетевых сервисов.

4.3.7. Проверку корректности конфигурации системных и активных сетевых устройств (мостов, маршрутизаторов, концентраторов и сетевых экранов).

4.4. Активное тестирование надёжности механизмов контроля доступа производится путём осуществления попыток проникновения в систему (с помощью автоматического инструментария или вручную).

4.5. Пассивное тестирование механизмов контроля доступа осуществляется путём анализа конфигурационных файлов системы. Информация об известных уязвимостях извлекается из документации и внешних источников. Затем осуществляется проверка конфигурации системы с целью выявления опасных состояний системы, т.е. таких состояний, в которых могут проявлять себя известные уязвимости.

V. АНАЛИЗ ИНЦИДЕНТОВ

5.1. Если администратор безопасности информационной системы персональных данных подозревает или получил сообщение о том, что система подвергается атаке или уже была скомпрометирована, то он должен установить:

- факт попытки несанкционированного доступа;
- продолжается ли несанкционированный доступ в настоящий момент;
- кто является источником несанкционированного доступа;
- что является объектом несанкционированного доступа;
- когда происходила попытка несанкционированного доступа;
- как и при каких обстоятельствах была предпринята попытка несанкционированного доступа;
- точка входа нарушителя в систему;
- была ли попытка несанкционированного доступа успешной;
- определить системные ресурсы, безопасность которых была нарушена;
- какова мотивация попытки несанкционированного доступа.

5.2. Для выявления попытки несанкционированного доступа необходимо установить, какие пользователи в настоящее время работают в системе, на каких рабочих станциях. Выявить подозрительную активность пользователей, проверить, что все пользователи вошли в систему со своих рабочих мест и никто из них не работает в системе необычно долго. Кроме того, необходимо проверить, что никто из пользователей не выполняет подозрительных программ и программ, не относящихся к его области деятельности.

5.3. При анализе системных журналов администратору безопасности необходимо произвести следующие действия:

5.3.1. Проверить наличие подозрительных записей системных журналов, сделанных в период предполагаемой попытки несанкционированного доступа, включая вход в систему пользователей, которые должны бы были отсутствовать в этот период времени, входы в систему из неожиданных мест, в необычное время и на короткий период времени.

5.3.2. Проверить, не уничтожен ли системный журнал и нет ли в нем пробелов.

5.3.3. Просмотреть списки команд, выполненных пользователями в рассматриваемый период времени.

5.3.4. Проверить наличие мест в системных журналах, которые выглядят необычно.

5.3.5. Выявить попытки получить полномочия суперпользователя или другого привилегированного пользователя.

5.3.6. Выявить наличие неудачных попыток входа в систему.

5.4. В ходе анализа журналов активного сетевого оборудования (мостов, переключателей, маршрутизаторов, шлюзов) необходимо:

5.4.1. Проверить наличие подозрительных записей системных журналов, сделанных в период предполагаемой попытки несанкционированного доступа.

5.4.2. Проверить, не уничтожен ли системный журнал и нет ли в нем пробелов.

5.4.3. Проверить наличие мест в журналах, которые выглядят необычно.

5.4.4. Выявить попытки изменения таблиц маршрутизации и адресных таблиц.

5.4.5. Проверить конфигурацию сетевых устройств с целью определения возможности нахождения в системе программы, просматривающей весь сетевой трафик.

5.5. Для обнаружения в системе следов, оставленных злоумышленником, в виде файлов, вирусов, троянских программ, изменения системной конфигурации необходимо:

5.5.1. Составить базовую схему того, как обычно выглядит система.

5.5.2. Провести поиск подозрительных файлов и каталогов, которые могли быть использованы злоумышленниками.

5.5.3. Проверить содержимое системных файлов, которые могли быть изменены злоумышленниками.

5.5.4. Проверить целостность системных программ.

5.5.5. Проверить систему аутентификации и авторизации.

5.6. В случае заражения значительного количества рабочих станций после устранения его последствий проводится системный аудит.

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

VI. КОНТРОЛЬ РЕЗЕРВНОГО КОПИРОВАНИЯ И ВОССТАНОВЛЕНИЯ ИНФОРМАЦИИ

6.1. На этапе исполнения администратором информационных систем плана резервного копирования администратор безопасности обязан контролировать сроки создания копий, анализировать состояние носителей (количество сбойных участков, объем свободного места) и незамедлительно докладывать руководителю Организации обо всех произошедших или ожидаемых отклонениях от плана.

6.2. Администратор безопасности согласовывает разработанный администратором информационной системы персональных данных регламент восстановления повреждённых или утраченных данных информационной системы.

VII. ШИФРОВАНИЕ ДАННЫХ

7.1. При необходимости шифрования данных, обрабатываемых с помощью технических средств информационной системы персональных данных, и/или резервных копий администратор безопасности производит следующие действия:

7.1.1. Выдача персональных идентификаторов или ключевых носителей средств криптографической защиты информации пользователям информационной системы персональных данных.

7.1.2. Ведение журнала регистрации, учёта и выдачи носителей информации поэкземплярного учёта средств криптографической защиты, эксплуатационной и технической документации к ним, ключевых документов.

7.1.3. Шифрование резервных копий, содержащих персональные данные, обрабатываемые в информационной системе, сертифицированными алгоритмами.

7.2. Дополнительные требования к администратору безопасности в связи с использованием средств шифрования данных могут быть определены в специальных регламентах работы с шифрованием информации информационной системы персональных данных.

VIII. ДЕЙСТВИЯ ПО ФАКТАМ НЕСОБЛЮДЕНИЯ ТРЕБОВАНИЙ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. При выявлении фактов несоблюдения условий и требований по защите персональных данных и использования средств защиты персональных данных, администратор безопасности обязан произвести следующие действия:

8.1.1. Незамедлительно сообщить о произошедшем руководителю Организации.

8.1.2. Собрать возможные факты (свидетельства) несоблюдения условий и требований по защите персональных данных и использования средств защиты персональных данных.

8.1.3. Сформировать экспертную комиссию по расследованию инцидента (при необходимости с привлечением внешних экспертов, представителей лицензиатов ФСТЭК России).

8.2. Экспертная комиссия составляет заключение условий и требований по защите персональных данных и использования средств защиты персональных данных.

8.3. Составленное экспертной комиссией заключение является основанием для применения дисциплинарного взыскания к виновным лицам.

8.4. Экспертная комиссия при расследовании инцидентов, связанных с нарушением обеспечения защищенности персональных данных, вправе производить обследование объектов информационной системы персональных данных с согласия ответственного лица за организацию обработки персональных данных.

IX. ПОРЯДОК ПРИОСТАНОВКИ ПРЕДОСТАВЛЕНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1. Администратор безопасности, при получении информации или самостоятельно выявив нарушения порядка предоставления персональных данных, предпринимает следующие действия:

9.1.1. Незамедлительно приостанавливает работу с персональными данными субъектов.

9.1.2. Сообщает о произошедшем руководителю Организации.

9.1.3. Самостоятельно или с привлечением дополнительных специалистов выявляет причины возникновения нарушения.

9.2. В случае выявления и устранения причины нарушения администратор безопасности восстанавливает работу с персональными данными субъектов и сообщает о причинах нарушения и своих действиях непосредственному руководителю.

9.3. В случаях невозможности оперативного выявления причин нарушения, проводится служебное разбирательство. Только по его завершению и устранению причин нарушения восстанавливается работа с персональными данными.

9.4. Все действия в процессе реагирования на нарушение порядка предоставления персональных данных должны фиксироваться администратором безопасности в Журнале учета нарушений порядка предоставления персональных данных» (Приложение 1).

X. ПРАВА АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

10.1. Администратор безопасности имеет право:

10.1.1. Требовать от работников Комитета соблюдения правил работы со средствами защиты информации, средствами криптографической защиты информации, входящими в состав информационной системы персональных данных.

10.1.2. Осуществлять взаимодействие (давать необходимые рекомендации, проводить консультации, получать необходимые сведения) с работниками Комитета по вопросам эксплуа-

тации технических и программных систем (подсистем) защиты персональных данных с целью улучшения качества их работы, а также своевременного предупреждения аварийных ситуаций.

XI. ОТВЕТСТВЕННОСТЬ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

11.1. Администратор безопасности несёт ответственность за:

11.1.1. Неисполнение (ненадлежащее исполнение) своих обязанностей, предусмотренных настоящей инструкцией.

11.1.2. Совершенные в процессе осуществления своей деятельности правонарушения в пределах определённых действующим административным, уголовным и гражданским законодательством Российской Федерации.

11.1.3. Причинение материального ущерба в пределах, определённых действующим трудовым, уголовным и гражданским законодательством Российской Федерации.

Приложение 1

ЖУРНАЛ

учета нарушений порядка предоставления персональных данных

№ п/п	Дата, время обнаружения нарушения	Информационная система персональных данных, в которой обнаружено нарушение	Дата, время устранения нарушения	Результат	Подпись ответст-венного работника	Примеча-ния
1	2	3	4	5	6	7

С инструкцией ознакомлен.

Фамилия, Имя, Отчество	Дата	Подпись