

Приложение № 5

Утверждаю :

Заведующий МБДОУ

д/с №11 «Радость»

Р.В. Чернецова



Февраль 2007.

## ИНСТРУКЦИЯ администратора безопасности информационных систем персональных данных МБДОУ д/с №11 «Радость»

### I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция определяет основные обязанности и права администратора безопасности информационных систем персональных данных МБДОУ д/с №11 «Радость»(далее -д/с №11 «Радость»).

1.2. Администратор безопасности информационных систем персональных данных (далее – ИСПДн) является сотрудником детского сада и назначается приказом заведующего.

1.3. Решение вопросов обеспечения информационной безопасности входит в прямые служебные обязанности администратора безопасности ИСПДн.

1.4. Администратор безопасности ИСПДн обладает правами доступа к любым программным и аппаратным ресурсам детского сада.

### II. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. Автоматизированное рабочее место (АРМ) – персональный компьютер и подключенные к нему периферийные устройства – принтер, многофункциональные устройства, сканеры и т.д.

2.2. Блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных) (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

2.3. Доступ к информации – возможность получения информации и её использования (ст. 2 ФЗ РФ от 27.07.2006 г. N 149-ФЗ «Об информации, информационных технологиях и защите информации»).

2.4. Защита информации – деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на информацию, то есть процесс, направленный на достижение информационной безопасности.

2.5. Информация - сведения (сообщения, данные) независимо от формы их представления (ст. 2 ФЗ РФ от 27.07.2006 г. N 149-ФЗ «Об информации, информационных технологиях и защите информации»).

2.6. Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

**2.7. Несанкционированный доступ (НСД)** – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т. д. различных организаций путём изменения (повышения, фальсификации) своих прав доступа.

**2.8. Носитель информации** - любой материальный объект или среда, используемый для хранения или передачи информации.

**2.9. Обработка персональных данных** - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

**2.10. Персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

**2.11. Средство защиты информации (СЗИ)** – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

**2.12. Угрозы безопасности персональных данных (УБПДн)** - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных (*Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных* (утверждена заместителем директора ФСТЭК России 14 февраля 2008 г.))

**2.13. Уничтожение персональных данных** - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных (ст. 3 ФЗ РФ от 27.07.2006 г. N 152-ФЗ «О персональных данных»).

### **III. ДОЛЖНОСТНЫЕ ОБЯЗАННОСТИ**

Администратор безопасности ИСПДн обязан:

3.1. Знать перечень и условия обработки персональных данных в школе.

3.2. Знать перечень установленных в кабинетах школы технических средств, в том числе съёмных носителей, конфигурацию ИСПДн и перечень задач, решаемых с её использованием.

3.3. Определять полномочия пользователей ИСПДн (оформление разрешительной системы доступа), минимально необходимых им для выполнения служебных (трудовых) обязанностей.

3.4. Осуществлять учёт и периодический контроль над составом и полномочиями пользователей автоматизированных рабочих мест (далее АРМ).

3.5. Осуществлять оперативный контроль за работой пользователей защищённых АРМ и адекватно реагировать на возникающие нештатные ситуации.

3.6. Блокировать доступ к персональным данным при обнаружении нарушений порядка их обработки.

3.7. Реагировать на попытки несанкционированного доступа к информации в установленном ст. 4 настоящей Инструкции.

3.8. Устанавливать и осуществлять настройку средств защиты информации в рамках компетенции.

- 3.9. Осуществлять непосредственное управление и контроль режимов работы функционирования применяемых в ИСПДн средств защиты информации, осуществлять проверку правильности их настройки (выборочное тестирование).
- 3.10. Периодически контролировать целостность печатей (пломб, наклеек) технических средств, используемых для обработки персональных данных.
- 3.11. Проводить работу по выявлению возможных каналов утечки персональных данных, изучать текущие тенденции в области защиты персональных данных.
- 3.12. Проводить разбирательства и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с техническими и программными средствами ИСПДн, в том числе со средствами защиты информации, или по другим нарушениям, которые могут привести к снижению уровня защищённости персональных данных.
- 3.13. Предоставлять доступ к ИСПДн новым пользователям, предоставлять им возможность задать пароль, соответствующий требованиям «Инструкции по организации парольной защиты».
- 3.14. Производить мероприятия по внеплановой смене паролей в соответствии с «Инструкцией по организации парольной защиты».
- 3.15. Вносить плановые и внеплановые изменения в учётную запись пользователей ИСПДн, в том числе по требованию руководителя отдела и в случае увольнения сотрудника.
- 3.16. Осуществлять периодическое резервное копирование баз персональных данных и сопутствующей защищаемой информации, а также осуществлять внеплановое создание резервных копий по требованию пользователей ИСПДн и в иных случаях, когда это необходимо для обеспечения сохранности персональных данных.
- 3.17. Осуществлять восстановление информации из резервных копий по требованию пользователей ИСПДн и в иных случаях, когда это необходимо для восстановления утраченных сведений.
- 3.18. Хранить дистрибутивы программного обеспечения, установленного в ИСПДн, в том числе дистрибутивы средств защиты информации, в месте, исключающем несанкционированный доступ к ним третьих лиц.
- 3.19. Вносить свои предложения по совершенствованию мер защиты персональных данных в ИСПДн, разработке и принятии мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению уровня защищённости персональных данных.
- 3.20. Знать законодательство РФ о персональных данных, следить за его изменениями.
- 3.21. Выполнять иные мероприятия, требуемые техническими и программными средствами ИСПДн для поддержания их функционирования.

#### **IV. ДЕЙСТВИЯ ПРИ ОБНАРУЖЕНИИ ПОПЫТОК НЕСАНКЦИОНИРОВАННОГО ДОСТУПА**

- 4.1. К попыткам несанкционированного доступа относятся:
- 4.1.1. сеансы работы с ИСПДн незарегистрированных пользователей, или пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истёк, или превышающих свои полномочия по доступу к данным;
- 4.1.2. действия третьего лица, пытающегося получить доступ (или уже получившего доступ) к ИСПДн, при использовании учётной записи администратора или другого пользователя ИСПДн, методом подбора пароля, использования пароля, разглашённого владельцем учётной записи или любым другим методом.
- 4.2. При выявлении факта несанкционированного доступа администратор безопасности ИСПДн обязан:

- 4.2.1. прекратить несанкционированный доступ к ИСПДн;
- 4.2.2. доложить директору школы о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях.

## V. ПРАВА

Администратор безопасности ИСПДн имеет право:

- 5.1. Требовать от пользователей ИСПДн выполнения инструкций в части работы с программными, аппаратными средствами ИСПДн и персональными данными.
- 5.2. Блокировать доступ к персональным данным любых пользователей, если это необходимо для предотвращения нарушения режима защиты персональных данных.
- 5.3. Проводить внеплановые антивирусные проверки при возникновении угрозы появления вредоносных программ.
- 5.4. Производить периодические попытки взлома паролей пользователей в целях тестирования системы контроля доступа на наличие уязвимостей. В случае успешной попытки – вправе требовать у пользователя изменения пароля.
- 5.5. Проводить служебные расследования и опрашивать пользователей по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с техническими и программными средствами ИСПДн, в том числе со средствами защиты информации, или по другим нарушениям, которые могут привести к снижению уровня защищённости персональных данных.

## VI. ОТВЕТСТВЕННОСТЬ

6.1. Администратор безопасности ИСПДн несёт персональную ответственность за соблюдение требований настоящей Инструкции, за средства защиты информации, применяемые в школе, за качество проводимых им работ по обеспечению безопасности персональных данных и за все действия, совершенные от имени его учётной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учётной записи.

6.2. Администратор безопасности ИСПДн при нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несёт дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.