СОГЛАСОВАНО

Педагогическим советом
МАОУ СШ № 3

УТВЕРЖДАЮ

Директор МАОУ СШ № 3
Ю.М. Морозова

Протокол № 18 от « 30 » 08 20 24 г. Приказ № 18 от « 30 » 08 20 24 г.

Порядок

доступа и работы работников МАОУ СШ № 3
в автоматизированных информационных системах персональных данных

І. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий порядок регламентирует обязанности сотрудников, участвующих в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющих доступ к аппаратным средствам, программному обеспечению и данным информационных систем персональных данных (далее ИСПДн), в отношении которых муниципальное автономное общеобразовательное учреждение «Средняя школа № 3» (далее – Школа) выступает в качестве пользователя.

ІІ. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

- 2.1. **Автоматизированная система** – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.
- 2.2. **Автоматизированное рабочее место (АРМ)** – персональный компьютер и подключенные к нему периферийные устройства – принтер, многофункциональные устройства, сканеры и т.д.
- 2.3. **Документированная информация** – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель (ст. 2 Федерального закона РФ от 27.07.2006. № 149 – ФЗ «Об информации, информационных технологиях и защите информации»)
- 2.4. **Доступ к информации** – возможность получения информации и ее использования (ст. 2 Федерального закона РФ от 27.07.2006. № 149 – ФЗ «Об информации, информационных технологиях и защите информации»).
- 2.5. **Защита информации** – деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на информацию, то есть процесс, направленный на достижение информационной безопасности.
- 2.6. **Информация** – сведения (сообщения, данные) независимо от формы их представления (ст. 2 Федерального закона РФ от 27.07.2006. № 149 – ФЗ «Об информации, информационных технологиях и защите информации»).
- 2.7. **Информационная система персональных данных (ИСПДн)** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств (ст. 3 Федерального закона РФ от 27.07.2006. № 152 – ФЗ «О персональных данных»).
- 2.8. **Компрометация пароля** – раскрытие, обнаружение или утеря пароля.
- 2.9. **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 путем изменения (повышения, фальсификации) своих прав доступа.
- 2.10. **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 Федерального закона РФ от 27.07.2006. № 152 – ФЗ «О персональных данных»).

2.11. **Пароль** – Секретная комбинация цифр, знаков, слов, или осмысленное предложение, служащие для защиты информации от несанкционированного доступа к информационным ресурсам.

2.12. **Персональные данные** – любая информация, относящаяся к прямо или косвенно определенному физическому лицу (субъекту персональных данных) (ст. 3 Федерального закона РФ от 27.07.2006. № 152 – ФЗ «О персональных данных»).

2.13. **Распространение персональных данных** – действия, направленные на раскрытие персональных данных неопределенному кругу лиц) (ст. 3 Федерального закона РФ от 27.07.2006. № 152 – ФЗ «О персональных данных»).

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

III. ОБЩИЕ ОБЯЗАННОСТИ РАБОТНИКОВ ШКОЛЫ

Каждый работник Школы, являющийся пользователем ИСПДн, обязан:

3.1. Строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн.

3.2. Знать и строго выполнять правила работы со средствами защиты информации, установленными на его автоматизированном рабочем месте (далее АРМ).

3.3. Осуществлять обработку персональных данных в информационной системе персональных данных, используемых в МАОУ СШ № 3 и нести персональную ответственность за свои действия.

3.4. Соблюдать правила работы с паролем своей учетной записи.

3.5. Соблюдать правила при работе в сетях общего доступа и (или международного обмена – Интернет и других).

3.6. Соблюдать правила доступа в помещение и к АРМ; экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

3.7. Немедленно вызывать системного администратора и поставить в известность директора Школы.

3.4.1. Несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств АРМ.

3.4.3. Отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов АРМ или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения;

3.4.4. Некорректного функционирования установленных на Арм технических средств защиты;

3.4.5. Непредусмотренных отводов кабелей и подключенных к АРМ дополнительных устройств.

3.5. Всем сотрудникам Школы, являющимся пользователями ИСПДн, категорически запрещается:

3.5.1. Использовать компоненты программного и аппаратного обеспечения ИСПДн школы в неслужебных целях;

3.5.2. Самовольно вносить какие-либо изменения в конфигурацию АРМ или устанавливать в АРМ любые программные и аппаратные средства, кроме выданных или разрешенных к использованию ответственным за обеспечение безопасности персональных данных;

3.5.3. Оставлять без присмотра свое АРМ не активизировав блокировки доступа или оставлять свое АРМ включенным по окончании работы;

3.5.4. Оставлять без присмотра документы (любой носитель-накопитель) содержащие персональные данные.

3.5.5. Оставлять открытыми помещения для свободного доступа извне при отсутствии в них сотрудников;

3.5.6. Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к нарушению безопасности персональных данных.

IV. ОБЕСПЕЧЕНИЕ СОХРАННОСТИ ИНФОРМАЦИИ

- 4.1. Для обеспечения сохранности электронных информационных ресурсов МБОУ СШ № 3 необходимо соблюдать следующие требования:
- 4.1.1. Для копирования информации не должны использоваться непроверенные на наличие компьютерных вирусов и других вредных программ носители информации.
- 4.2. Субъектам доступа запрещается:
- 4.2.1. Установка и использование при работе с электронно-вычислительными машинами вредоносных программ, ведущих к блокированию работы сети;
- 4.2.2. Самовольное изменение сетевых адресов;
- 4.2.3. Самовольное вскрытие блоков электронно-вычислительных машин, модернизация и модификация электронно-вычислительных машин и программного обеспечения;
- 4.2.4. Несанкционированная передача компьютеров с прописанными сетевыми настройками. Передача компьютеров из одного подразделения в другое производится только системным администратором с предварительно удаленными сетевыми настройками.
- 4.3. Сведения, содержащиеся в электронных документах и базах данных школы. Должны использоваться только в служебных целях в рамках полномочий сотрудника, работающего с соответствующими материалами.

V. ПАРОЛЬНАЯ ЗАЩИТА

- 5.1. Личные пароли выбираются пользователями информационной системы самостоятельно с учетом следующих требований:
- 5.1.1. Длина пароля должна быть не менее 8 символов;
- 5.1.2. В числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистре, цифры;
- 5.1.3. Пароль не должен включать в себя имя пользователя, легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков (111, qwert!, абвгд и т.д.) общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), аббревиатуры, номера автомобилей, телефонов и другие значимые сочетание букв и знаков, которые можно угадать, основываясь на информации о пользователе;
- 5.1.4. При смене пароля новое значение должно отличаться от предыдущего не менее чем в 5 позициях.
- 5.2. Сотрудникам допускается использовать пароли, составленные из первых букв слов запоминающихся высказываний в разном регистре, смешанные в произвольном порядке со специальными символами (например Кожзгсф7!).
- 5.3. Для обеспечения возможности использования имен и паролей некоторых сотрудников в их отсутствие (например, в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т. п.) сотрудники обязаны сразу же после установки своих паролей передавать их на хранение вместе с именами своих учетных записей администратору безопасности ИСПДн в запечатанном конверте или опечатанном пенале.
- 5.4. При вводе пароля пользователю необходимо исключить произнесение его вслух, возможность его подсматривания посторонними лицами (человек за спиной, наблюдение человеком за движением пальцев в прямой видимости или в отраженном свете) и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т.п.)
- 5.5. Смена пароля должна проводиться регулярно, не реже одного раза в 6 месяцев, самостоятельно каждым пользователем.
- 5.6. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке, мобильном телефоне и любых других предметах и носителях информации.
- 5.7. Запрещается сообщать свой пароль полностью или частично другим пользователям, запрещается спрашивать или подсматривать пароль других пользователей.
- 5.8. Запрещается регистрировать других пользователей в ИСПДн со своим личным паролем, запрещается входить в ИСПДн под учетной записью и паролем другого пользователя.

5.9. В случае утери или компрометации (разглашения, утраты) или подозрения в компрометации пароля пользователя должна быть немедленно проведена внеплановая процедура смены пароля.

IV. АНТИВИРУСНАЯ ЗАЩИТА

6.1. При возникновении подозрения на наличие вредоносного программного обеспечения (частые ошибки в работе программ, появление посторонних графических и звуковых эффектов, искажение данных, неконтролируемое пропадание файлов, появление сообщений о системных ошибках, замедление работы компьютера и т.п.) самостоятельно или вместе с системным администратором провести внеочередной антивирусный контроль своего АРМ. При самостоятельном проведении антивирусного контроля – уведомить о результатах администратора безопасности ИСПДн для определения им факта наличия или отсутствия вредоносного программного обеспечения.

6.2. В случае появления информационного окна средства антивирусной защиты, сигнализирующем об обнаружении вредоносного обеспечения:

6.2.1. Приостановить обработку данных;

6.2.2. Немедленно поставить в известность о факте обнаружения вредоносного программного обеспечения администратора безопасности ИСПДн, владельца зараженных файлов, а также работников Школы, использующие эти файлы в работе;

6.2.3. Совместно с владельцем файлов, зараженных вредоносным программным обеспечением, провести анализ необходимости дальнейшего их использования;

6.2.4. Произвести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта привлечь администратора безопасности ИСПДн).

VII. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ПРАВИЛ РАБОТЫ

7.1. Каждый пользователь ИСПДн несет персональную ответственность за соблюдение требований настоящего Порядка и за все действия, совершенные от имени его учетной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учетной записи.

7.2. За разглашение персональных данных и нарушение порядка работы со средствами ИСПДн, содержащими персональные данные, сотрудники могут быть привлечены к гражданской, уголовной, административной, дисциплинарной и иной предусмотренной законодательством Российской Федерации ответственности.

7.3. Разглашение персональных данных субъекта (передача их посторонним лицам, в том числе другим сотрудникам, не имеющим к ним доступ), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных локальными нормативно-правовыми актами (приказами, распоряжениями) управления, влечет наложение на сотрудника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде: замечания, выговора, увольнение. Работник Школы, имеющий доступ к персональным данным субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба (в соответствии с п. 7 ст. 243 Трудового кодекса РФ).

7.3.1. В отдельных случаях, при разглашении персональных данных, сотрудник, совершивший указанный проступок, несет ответственность в соответствии со ст. 13.14 Кодекса об административных правонарушениях РФ.

7.4. В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушения неприкосновенности частной жизни), предусмотрена ответственность в соответствии со ст. 137 Уголовного кодекса РФ.