

## **Инструкция пользователя информационных систем персональных данных**

### **1. ОБЩИЕ ПОЛОЖЕНИЯ**

**1.1.** Настоящий документ разработан в соответствии с нормативными документами по безопасности информации и определяет порядок обеспечения информационной безопасности при проведении работ пользователями информационных систем персональных данных (далее – ИСПДн) МОУ «ООШ №4 г. Катав-Ивановска» (далее – Учреждение).

**1.2.** Субъектами доступа к ресурсам ИСПДн являются администратор безопасности (далее – АБ), пользователи и обслуживающий персонал.

**1.3.** Обрабатываемая в ИСПДн информация относится к сведениям, составляющим персональные данные (далее – ПДн).

**1.4.** Машинные носители информации имеют пометку «ПДн».

**1.5.** Пользователи получают свои права на доступ к ресурсам ИСПДн через АБ.

**1.6.** Пользователи имеют право письменно вносить предложения по изменению и дополнению данной Инструкции.

**1.7.** Изменения и дополнения к данной Инструкции утверждаются в установленном порядке.

**1.8.** Право толкования положений настоящей Инструкции возлагается на Руководителя Учреждения.

### **2. 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. Доступ к информации** – возможность получения информации и ее использования.

**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.

**2.6. Информационная система персональных данных (ИСПДн)** – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

**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 путем изменения (повышения, фальсификации) своих прав доступа.

**2.8. 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.

**2.9. Персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

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

### **3. ОБЯЗАННОСТИ**

Пользователь обязан:

**3.1.** Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций и распоряжений, регламентирующих порядок действий по защите информации.

**3.2.** Выполнять на автоматизированном рабочем месте (далее – АРМ) только те процедуры, которые определены технологическим процессом обработки ПДн.

**3.3.** Знать и соблюдать установленные требования к обработке ПДн, учету и хранению носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов.

**3.4.** Соблюдать требования парольной политики в соответствии с «Инструкцией по организации парольной защиты».

**3.5.** Получить уникальное имя и персональный идентификатор (при его наличии) от АБ. Пользователь обязан помнить и соблюдать в тайне свои имена и пароли, не допускается их запись на каких-либо носителях в целях напоминания.

**3.6.** Во время работы располагать экран монитора так, чтобы затруднить посетителям просмотр отображаемой информации. Жалюзи на окнах должны быть закрыты.

**3.7.** При возникновении подозрения на наличие вредоносного программного обеспечения (частые ошибки в работе программ, появление посторонних графических и звуковых эффектов, искажения данных, неконтролируемое пропадание файлов, появление сообщений о системных ошибках, замедление работы компьютера и т.п.) самостоятельно или вместе с АБ ИСПДн провести внеочередной антивирусный контроль своего АРМ. При

самостоятельном проведении антивирусного контроля - уведомить о результатах АБ ИСПДн для определения им факта наличия или отсутствия вредоносного программного обеспечения.

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

**3.8.1.** приостановить обработку данных;

**3.8.2.** немедленно поставить в известность о факте обнаружения вредоносного программного обеспечения АБ ИСПДн, владельца зараженных файлов, а также смежные структурные подразделения, использующие эти файлы в работе;

**3.8.3.** совместно с владельцем файлов, зараженных вредоносным программным обеспечением, провести анализ необходимости дальнейшего их использования;

**3.8.4.** произвести лечение или уничтожение зараженных файлов (для выполнения требований данного пункта привлечь АБ ИСПДн).

**3.9.** Немедленно вызывать АБ ИСПДн и поставить в известность руководителя структурного подразделения при обнаружении:

**3.9.1.** нарушений целостности пломб (наклеек, нарушений или несоответствии номеров печатей) на аппаратных средствах АРМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа к защищаемой АРМ;

**3.9.2.** несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств АРМ;

**3.9.3.** 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;

**3.9.4.** некорректного функционирования установленных на АРМ технических средств защиты;

**3.9.5.** непредусмотренных отводов кабелей и подключенных к АРМ дополнительных устройств.

**3.10.** При утере или подозрении на утечку своего имени, пароля и персональных идентификаторов пользователь должен немедленно сообщить об этом АБ.

**3.11.** Обо всех выявленных нарушениях, связанных с информационной безопасностью Учреждения, а так же для получения консультаций по вопросам информационной безопасности, необходимо обратиться к АБ.

**3.12.** При отсутствии визуального контроля за рабочей станцией доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>.

**3.13.** В ИСПДн осуществляется блокирование сеанса доступа пользователя после 20 минут его бездействия (неактивности) в информационной системе.

**3.14.** Принимать меры по реагированию в случае возникновения внештатных ситуаций и аварийных ситуаций с целью ликвидации их последствий в пределах

возложенных на него функций.

### **3.15. Пользователям запрещается:**

- разглашать **защищаемую информацию** посторонним лицам;
- копировать защищаемую информацию на неучтенные внешние носители;
- самостоятельно устанавливать, тиражировать или модифицировать программное и аппаратное обеспечение, изменять установленный порядок функционирования технических и программных средств;
- подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства;
- отключать (блокировать) средства защиты информации;
- выполнять на АРМ работы, не предусмотренные технологическим процессом обработки ПДн;
- сообщать (или передавать) посторонним лицам параметры своей учетной записи (имя, персональный идентификатор (при его наличии) и пароль) в ИСПДн;
- оставлять без присмотра и передавать другим лицам персональный идентификатор;
- привлекать посторонних лиц для ремонта или настройки АРМ без согласования с ответственным за обеспечение безопасности ПДн;
- оставлять без присмотра свое АРМ, не активизировав блокировку доступа, или оставлять свое АРМ включенным по окончании работы;
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к нарушению безопасности персональных данных.

## **4. ПОРЯДОК РАБОТЫ ПОЛЬЗОВАТЕЛЯ С РЕСУРСАМИ ИСПДН**

### **4.1. Начало работы на ПЭВМ**

При включении ПЭВМ необходимо дождаться завершения загрузки и готовности системы защиты информации (далее – СЗИ) и операционной системы (далее – ОС) к идентификации пользователя. Идентификация пользователя осуществляется по уникальному имени и паролю с использованием персонального идентификатора, если таковой предусмотрен комплектацией СЗИ. Для получения доступа к ресурсам ИСПДн пользователь должен приложить к считывателю персональный идентификатор (при его наличии) и ввести с клавиатуры свой пароль. Если после ввода пароля СЗИ выдаст сообщение об ошибке, пользователь должен обратиться к АБ.

### **4.2. Завершение работы на ПЭВМ**

По окончании работы пользователь должен либо завершить штатными средствами сеанс своей работы (без выключения ПЭВМ), либо завершить работу ПЭВМ стандартным способом (при этом выключить ПЭВМ).

### **4.3. Требования к распечатыванию информации**

Все распечатываемые документы должны быть учтены. Бракованные бумажные носители и черновики документов должны быть уничтожены.

При отсутствии пользователя на рабочем месте либо в присутствии лиц, не имеющих допуска к ресурсам ИСПДн, все документы, содержащие ПДн, должны быть недоступны для просмотра и иного их использования.

## **5. ОРГАНИЗАЦИЯ ПАРОЛЬНОЙ ЗАЩИТЫ**

**5.1.** Личные пароли доступа к элементам ИСПДн выдаются пользователям АБ или создаются самостоятельно.

**5.2.** Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 12 месяцев.

**5.3.** Правила формирования пароля:

- пароль должен состоять не менее чем из 6 символов;
- в пароле должны присутствовать символы из числа прописных и строчных букв английского алфавита от А до Z; десятичных цифр (от 0 до 9); символы, не принадлежащие алфавитно-цифровому набору (например, !, \$, #, %);
- запрещается использовать в качестве пароля имя учетной записи, простые пароли типа «123», «111», «qwerty» и им подобные, а также имена и даты рождения пользователей ИСПДн и их родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно вычислить, основываясь на информации о пользователе;
- запрещается использовать в качестве пароля один и тот же повторяющийся символ, либо повторяющуюся комбинацию из нескольких символов;
- запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);
- запрещается выбирать пароли, которые уже использовались ранее.

**5.4.** Правила ввода пароля:

- ввод пароля должен осуществляться с учетом регистра, в котором пароль был задан;
- во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами.

**5.5.** Правила хранения пароля:

- запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах;
- запрещается сообщать другим пользователям личный пароль и/или регистрировать их в системе под своей учетной записью.

**5.6.** Лица, использующие паролирование, обязаны:

- четко знать и строго выполнять требования настоящей Инструкции и других руководящих документов по паролированию;
- своевременно сообщать АБ об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

## **6. ОТВЕТСТВЕННОСТЬ**

**6.1.** Пользователь несет персональную ответственность за:

- сохранность носителей информации и содержащейся на них информации (в рабочее время);
- соблюдение требований данной Инструкции, неправомерное использование ресурсов ИСПДн 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.

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