

Приложение к Положению о Политике  
в отношении персональных данных



УТВЕРЖДАЮ

Директор МБУ «Школа № 32»

*О. В. Федорахина* О.В.Федорахина

«02» сентября 2015г.

## Инструкция оператора автоматизированной информационной системы обработки персональных данных

### 1. Общие положения

- 1.1. Настоящая Инструкция устанавливает обязанности пользователя информационной системы персональных данных (далее - ИСПДн) в МБУ «Школа № 32» (далее - Школы) по обеспечению безопасности, обрабатываемых в ней персональных данных, запреты на действия пользователя в ИСПДн, а также его права и ответственность.
- 1.2. Доступ пользователя к ИСПДн осуществляется в соответствии с перечнем сотрудников, допущенных к обработке персональных данных.
- 1.3. Привилегии доступа пользователя к автоматизированному рабочему месту (далее – АРМ) назначаются в соответствии с матрицей прав доступа в ИСПДн.
- 1.4. Контроль за выполнением настоящей Инструкции возлагается на ответственного за обеспечение безопасности персональных данных.
- 1.5. Каждый сотрудник подразделения ОУ, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным (в дальнейшем именуемый пользователем), несёт персональную ответственность за свои действия при работе с информационными ресурсами ИСПДн.

### 2. Обязанности пользователя ИСПДн

Пользователь обязан:

- 2.1. При работе с документами, содержащими персональные данные, руководствоваться требованиями организационно-распорядительных документов ИСПДн. Строго соблюдать установленные правила обеспечения безопасности персональных данных при работе с программными и техническими средствами ИСПДн.
- 2.2. Использовать ИСПДн для выполнения служебных задач в соответствии с должностной инструкцией.
- 2.3. Использовать для доступа к ИСПДн собственную уникальную учетную запись (логин) и пароль.
- 2.4. Хранить в тайне пароли и PIN-коды, обеспечивать физическую сохранность ключевого носителя доступа к ИСПДн.
- 2.5. Не допускать при работе с ИСПДн просмотр посторонними лицами персональных данных, отображаемых на дисплее АРМ.
- 2.6. Блокировать экран дисплея АРМ паролем заставкой при оставлении рабочего места. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>
- 2.7. По всем вопросам, связанным с обеспечением защиты персональных данных, содержащихся в базах данных, и работе со средствами защиты информации, возникающими при работе в ИСПДн, обращаться к администратору информационной безопасности.

УТВЕРЖДАЮ

Директор МБУ «Школа № 32»

О.В.Федорахина

«02» сентября 2015г.

## **Инструкция оператора автоматизированной информационной системы обработки персональных данных**

### **1. Общие положения**

- 1.1. Настоящая Инструкция устанавливает обязанности пользователя информационной системы персональных данных (далее - ИСПДн) в МБУ «Школа № 32» (далее - Школы) по обеспечению безопасности, обрабатываемых в ней персональных данных, запреты на действия пользователя в ИСПДн, а также его права и ответственность.
- 1.2. Доступ пользователя к ИСПДн осуществляется в соответствии с перечнем сотрудников, допущенных к обработке персональных данных.
- 1.3. Привилегии доступа пользователя к автоматизированному рабочему месту (далее – АРМ) назначаются в соответствии с матрицей прав доступа в ИСПДн.
- 1.4. Контроль за выполнением настоящей Инструкции возлагается на ответственного за обеспечение безопасности персональных данных.
- 1.5. Каждый сотрудник подразделения ОУ, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным (в дальнейшем именуемый пользователем), несет персональную ответственность за свои действия при работе с информационными ресурсами ИСПДн.

### **2. Обязанности пользователя ИСПДн**

Пользователь обязан:

- 2.1. При работе с документами, содержащими персональные данные, руководствоваться требованиями организационно-распорядительных документов ИСПДн. Строго соблюдать установленные правила обеспечения безопасности персональных данных при работе с программными и техническими средствами ИСПДн.
- 2.2. Использовать ИСПДн для выполнения служебных задач в соответствии с должностной инструкцией.
- 2.3. Использовать для доступа к ИСПДн собственную уникальную учетную запись (логин) и пароль.
- 2.4. Хранить в тайне пароли и PIN-коды, обеспечивать физическую сохранность ключевого носителя доступа к ИСПДн.
- 2.5. Не допускать при работе с ИСПДн просмотр посторонними лицами персональных данных, отображаемых на дисплее АРМ.
- 2.6. Блокировать экран дисплея АРМ паролем заставкой при оставлении рабочего места. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>
- 2.7. По всем вопросам, связанным с обеспечением защиты персональных данных, содержащихся в базах данных, и работе со средствами защиты информации, возникающими при работе в ИСПДн, обращаться к администратору информационной безопасности.

2.8. Немедленно прекращать обработку персональных данных и ставить в известность администратора информационной безопасности при подозрении компрометации пароля, а также при обнаружении:

- нарушений целостности пломб, наклеек на ПЭВМ (персональные электронно-вычислительные машины), при наличии таковых, или иных фактов совершения в его отсутствие попыток несанкционированного доступа (НСД);
- несанкционированных изменений в конфигурации программных или аппаратных средств АРМ;
- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования АРМ;
- непредусмотренных конфигурацией АРМ отводов кабелей и подключенных устройств.

2.9. Немедленно информировать ответственного за обеспечение безопасности персональных данных при их обработке в ИСПДн в случае обнаружения попыток несанкционированного доступа к ИСПДн.

2.10. Немедленно информировать сотрудников, осуществляющих сетевое администрирование ОУ, при появлении сообщений от программного обеспечения антивирусной защиты о возможном вирусном заражении АРМ или возникновении неисправностей (сбоев) в работе сервисов и информационных ресурсов ОУ.

### **3. Организация парольной защиты**

3.1. Личные пароли доступа к элементам ИСПДн выдаются пользователям соответствующими службами.

3.2. Правила формирования пароля:

- пароль не может содержать имя учетной записи пользователя или какую-либо его часть.
- пароль должен состоять не менее чем из 8 символов.
- в пароле должны присутствовать символы трех категорий из числа следующих четырех:
- прописные буквы английского алфавита от А до Z;
- строчные буквы английского алфавита от а до z;
- десятичные цифры (от 0 до 9);
- символы, не принадлежащие алфавитно-цифровому набору (например, !, \$, #, %).
- запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а так же имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, 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.

### 3.3. Правила ввода пароля:

- ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан;
- во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

### 3.4. 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 регистрировать их в системе под своим паролем.

### 3.5. Лица, использующие паролирование, обязаны:

- четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по паролированию;
- своевременно сообщать Администратору информационной безопасности об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.
- Правила работы в сетях общего доступа и (или) международного обмена.

### 3.6. Работа в сетях общего доступа и (или) международного обмена (сети Интернет и других) (далее – Сеть) на элементах ИСПДн, должна проводиться при служебной необходимости.

### 3.7. При работе в Сети запрещается:

- осуществлять работу при отключенных средствах защиты (антивирус и других);
- передавать по Сети защищаемую информацию без использования средств шифрования;
- запрещается скачивать из Сети программное обеспечение и другие файлы;
- запрещается посещение сайтов сомнительной репутации;
- запрещается нецелевое использование подключения к Сети.

## **4. Действия, запрещенные пользователю ИСПДн**

Пользователю ИСПДн запрещается:

- 4.1. Предоставлять доступ к информации, содержащей персональные данные, лицам, не допущенным к их обработке.
- 4.2. Записывать пароль на любые носители, в том числе бумажные.
- 4.3. Сообщать (или передавать) посторонним лицам личные ключи или атрибуты доступа к ресурсам ИСПДн.
- 4.4. Привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение защиты персональных данных.
- 4.5. Работать с персональными данными в присутствии посторонних (не допущенных к данной информации) лиц.
- 4.6. Самостоятельно изменять конфигурацию аппаратно-программных средств ИСПДн.
- 4.7. Осуществлять действия по преодолению установленных ограничений на доступ к ИСПДн.
- 4.8. Отключать или изменять конфигурацию средств защиты информации ИСПДн.
- 4.9. Устанавливать на АРМ программное обеспечение, не связанное с исполнением служебных обязанностей.

## **5. Права пользователя ИСПДн**

Пользователь ИСПДн имеет право:

- 5.1. Получать помощь по вопросам эксплуатации ИСПДн от ответственного за систему защиты информации (далее - СЗИ) ИСПДн.
- 5.2. Обращаться к сотрудникам, осуществляющим сетевое администрирование ОУ, по вопросам дооснащения АРМ техническими и программными средствами, не входящими в штатную конфигурацию АРМ и ИСПДн, необходимыми для автоматизации деятельности в соответствии с возложенными на него должностными обязанностями.
- 5.3. Подавать сотрудникам, осуществляющим сетевое администрирование ОУ, предложения по совершенствованию функционирования ИСПДн.

## **6. Ответственность пользователя ИСПДн**

Пользователь ИСПДн несет ответственность за:

- 6.1. Обеспечение безопасности персональных данных при их обработке в ИСПДн.
- 6.2. Нарушение работоспособности или вывод из строя системы защиты ИСПДн.
- 6.3. Преднамеренные действия, повлекшие модификацию или уничтожение персональных данных в ИСПДн, и несанкционированный доступ к персональным данным в ИСПДн.
- 6.4. Разглашение персональных данных.
- 6.5. Пользователь, имеющий расширенные права «Опытный пользователь» или «Администратор», несет ответственность за корректное функционирование прикладного программного обеспечения ИСПДн.
- 6.6. «Администратор», несет ответственность за корректное функционирование прикладного программного обеспечения ИСПДн.
- 6.7. За нарушение настоящей Инструкции к пользователю могут применяться меры дисциплинарного воздействия.

## **7. Правила работы в информационно-телекоммуникационных сетях международного информационного обмена**

- 7.1. Работа в информационно-телекоммуникационных сетях международного информационного обмена - сети Интернет и других (далее – Сеть) на элементах ИСПДн должна проводиться только при служебной необходимости.
- 7.2. При работе в Сети запрещается:
  - осуществлять работу при отключенных средствах защиты (антивирусных и других);
  - передавать по Сети защищаемую информацию без использования средств шифрования;
  - скачивать из Сети программное обеспечение и другие файлы в неслужебных целях;
  - посещать сайты сомнительной репутации (сайты, содержащие нелегально распространяемое программное обеспечение (ПО), сайты знакомств, онлайн игры и другие не отвечающие задачам).