

УТВЕРЖДАЮ

Приказ № 2050 от «15» 06 2018 г.

Директор школы-интерната № 1 им. К.К. Грота



А.В. Мухин

**Инструктаж по обеспечению безопасности персональных
данных, обрабатываемых в информационной системе
персональных данных
Государственного бюджетного общеобразовательного учреждения
школы-интерната № 1 имени К. К. Грота Красногвардейского района
Санкт-Петербурга**

Санкт-Петербург
2018г.

1. Общие положения

- 1.1 Настоящая Инструкция устанавливает обязанности пользователя информационных систем персональных данных (далее - ИСПДн) в ГБОУ школы-интерната №1 им. К. К. Грота Красногвардейского района Санкт-Петербурга (далее – Школы-интерната) по обеспечению безопасности обрабатываемых в них персональных данных, запреты на действия пользователя в ИСПДн, а также его права и ответственность.
- 1.2 Наиболее вероятными каналами утечки информации для ИСПДн являются:
- несанкционированный доступ к информации, обрабатываемой в ИСПДн;
 - хищение технических средств, с хранящейся в них информацией, или отдельных носителей информации;
 - просмотр информации с экранов дисплеев мониторов и других средств ее отображения с помощью оптических устройств;
 - воздействие на технические или программные средства в целях нарушения целостности (уничтожения, искажения) информации, работоспособности технических средств, средств защиты информации, через специально внедренные электронные и программные средства.
- 1.3 Доступ пользователя к ИСПДн осуществляется в соответствии с перечнем сотрудников, допущенных к обработке персональных.
- 1.4 Привилегии доступа пользователя к автоматизированному рабочему месту (далее - АРМ) назначаются в соответствии с матрицей прав доступа для ИСПДн.
- 1.5 Контроль за выполнением настоящей Инструкции возлагается на ответственного по защите персональных данных.

2. Обязанности работников Школы-интерната, имеющих доступ к ИСПДн

- 2.1 Работники, получившие доступ к персональным данным, обязаны хранить в тайне данные сведения, ставшие им известными во время работы или иным путем и пресекать действия других лиц, которые могут привести к разглашению такой информации. О таких фактах, а также о других причинах или условиях возможной утечки информации немедленно информировать руководителя структурного подразделения Школы-интерната, ответственного по защите персональных данных.
- 2.2 Персональные данные не подлежат разглашению. Прекращение доступа к такой информации не освобождает работника от взятых им обязательств о неразглашении конфиденциальных сведений.
- 2.3 В случае оставления занимаемой должности работник обязан вернуть все документы и материалы, относящиеся к деятельности Школы-интерната. В том числе отчеты, инструкции, переписку, списки сотрудников, компьютерные программы, а также все прочие материалы и копии названных материалов, имеющих какое-либо отношение к деятельности Школы-интерната, полученные в течение срока работы.
- 2.4 Работники при работе с ИСПДн обязаны:
- Использовать ИСПДн для выполнения служебных задач в соответствии с должностной инструкцией.
 - Использовать для доступа к ИСПДн собственную уникальную учетную запись (логин) и пароль.
 - Хранить в тайне уникальную учетную запись (логин) и пароль, обеспечивать физическую сохранность ключевого носителя доступа к ИСПДн.
 - Использовать для работы, только учетные съемные накопители информации.
 - АРМ используемое для работы с конфиденциальной информацией, должно быть размещено таким образом, чтобы исключалась возможность визуального

просмотра экрана монитора, не имеющими отношения к конкретно обрабатываемой информации сотрудниками.

- Блокировать экран дисплея АРМ парольной заставкой при оставлении рабочего места.
- Контролировать обновление антивирусных баз и в случае необходимости обновления сообщить данную информацию сотрудникам, осуществляющим сетевое администрирование Школы-интерната и ответственному по защите персональных данных.
- В случае обнаружения попыток несанкционированного доступа к ИСПДн немедленно информировать сотрудников, осуществляющих сетевое администрирование Школы-интерната и ответственного по защите персональных данных.
- При появлении сообщений от программного обеспечения антивирусной защиты о возможном вирусном заражении АРМ или возникновении неисправностей (сбоев) в работе сервисов и информационных ресурсов Школы-интерната немедленно информировать сотрудников, осуществляющих сетевое администрирование.
- В случае утери носителя с конфиденциальной информацией или при подозрении компрометации логина и пароля немедленно информировать сотрудников, осуществляющих сетевое администрирование Школы-интерната и ответственного по защите персональных данных.

3. Действия, запрещенные пользователю ИСПДн

3.1 Сотрудникам Школы-интерната, имеющим доступ к ИСПДн запрещается:

- Предоставлять доступ к информации, содержащей персональные данные, лицам, не допущенным к их обработке.
- Записывать и хранить персональные данные на неучтенных носителях информации.
- Самостоятельно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн, или устанавливать дополнительно любые программные и аппаратные средства.
- Оставлять включенным без присмотра АРМ, не активизировав средства защиты от несанкционированного доступа (блокировка экрана дисплея парольной заставкой).
- Осуществлять действия по преодолению установленных ограничений на доступ к ИСПДн.
- Отключать или изменять конфигурацию средств защиты информации ИСПДн.

4. Права пользователя ИСПДн

4.1 Пользователь ИСПДн имеет право:

- Получать помощь по вопросам эксплуатации ИСПДн, от ответственного за СЗИ ИСПДн.
- Обращаться к сотрудникам, осуществляющим сетевое администрирование Учреждения, 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.
- Подавать сотрудникам, осуществляющим сетевое администрирование Учреждения, предложения по совершенствованию функционирования ИСПДн.

5. Ответственность пользователя ИСПДн

5.1 Пользователь ИСПДн несет ответственность за:

- Обеспечение безопасности персональных данных при их обработке в ИСПДн.
- Нарушение работоспособности или вывод из строя системы защиты ИСПДн.
- Преднамеренные действия, повлекшие модификацию или уничтожение персональных данных в ИСПДн, и несанкционированный доступ к персональным данным в ИСПДн.
- За соблюдение требований настоящей инструкции, а также других документов в области защиты информации.
- За нарушение настоящей Инструкции к пользователю могут применяться меры дисциплинарного воздействия.
- За нарушение правил обработки персональных данных, их неправомерное разглашение или распространение, виновные лица несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством.