Утверждаю:
Директор ГБОУ РШИ с. Камышла

"23" сентября 2023 г. N 323

_____ /Садриев З.Г./
(подпись) Ф.И.О.

М.П

ИНСТРУКЦИЯ
ПО ПРОВЕДЕНИЮ ПРОВЕРОК СОСТОЯНИЯ ЗАЩИТЫ ИСПДн

1. Назначение и область применения

1.1. Настоящий документ определяет порядок проведения проверочных мероприятий по контролю соблюдения порядка обработки и защищенности информационной системы персональных данных в Учреждении.

2. Порядок контроля защищенности персональных данных

2.1. В целях контроля изучения и оценки фактического состояния защищенности информационной системы персональных данных, своевременного реагирования на нарушения установленного порядка их обработки, а также для совершенствования порядка обработки и обеспечения его соблюдения, в Учреждении на регулярной основе должны проводиться контрольные мероприятия.

2.2. Контрольные мероприятия (проверки) проводятся на плановой основе, а также внепланово – по фактам выявления инцидентов в области безопасности персональных данных, а также при изменениях в составе пользователей и при существенных изменениях в среде обработки персональных данных.

2.3. Контрольные мероприятия (проверки) утверждаются директором и организуются лицом, ответственным за обеспечение безопасности информационной системы персональных данных.

2.4. Плановые проверки проводятся на периодичной основе и включают в себя:

2.4.1. Проверку деятельности сотрудников Учреждения, допущенных к работе с ИСПДн в информационных системах персональных данных (далее – ИСПДн) Учреждения на соответствие порядку обработки и обеспечения безопасности ПДн, установленному в Учреждении;

2.4.2. Проверку компетентности персонала, задействованного в обработке ИСПДн;

2.4.3. Проверку актуальности нормативно-организационных документов;

2.4.4. Проверку работоспособности и эффективности технических средств ИСПДн и средств защиты ПДн;

2.4.5. Проверку ведения копий средств защиты;

2.4.6. Проверку проведения процедуры резервного копирования защищаемой информации;

2.4.7. Проверку соблюдения прав доступа пользователей к ПДн;

2.4.8. Контроль над выполнением парольной защиты;

2.4.9. Проверку отсутствия на АРМ пользователей средств разработки программного обеспечения;

2.4.10. Проверку отсутствия на АРМ пользователей нештатного ПО;

2.4.11. Мониторинг журналов протоколирования событий аутентификации;

2.4.12. Контроль над выполнением антивирусной защиты;

2.4.13. Контроль над соблюдением режима защиты при подключении к сетям общего пользования и (или) международного обмена;

2.4.14. Организацию анализа и пересмотра имеющихся угроз безопасности ПДн, а также предсказание появления новых, еще неизвестных, угроз.

2.5. Ответственный за обеспечение безопасности информационной системы персональных данных составляет план проверочных мероприятий, утверждаемый руководителем Учреждения.

2.6. Выявленные в ходе проверок нарушения, а также отметки об их устранении, фиксируются в «Журнале учета выявленных нарушений в порядке обработки и обеспечения безопасности информационной системы персональных данных». Форма Журнала учета выявленных нарушений в порядке обработки и обеспечения безопасности информационной системы персональных данных приведена в Приложении № 1 к настоящей инструкции.

2.7. Результаты проверок оформляются актами. Форма Акта о результатах проведения проверки приведена в Приложении № 2 к настоящей инструкции. Акт составляется в двух экземплярах, как правило, на месте, подписывается председателем и членами комиссии, докладывается под роспись руководителю подразделения.

2.8. Выявленные нарушения расследуются, результаты расследования направляются на имя руководителя Учреждения. При необходимости принятия решений по результатам проверок руководителю Учреждения готовятся соответствующие докладные записки.

Приложения: 1. Журнале учета выявленных нарушений в порядке обработки и обеспечения безопасности информационной системы персональных данных». на 1 л. в 1 экз.

2. Акт о результатах проведения проверки на 1 л. в 1 экз.