Автономное профессиональное образовательное учреждение Ханты-Мансийского автономного округа-Югры
«ЮГОРСКИЙ КОЛЛЕДЖ-ИНТЕРНАТ ОЛИМПИЙСКОГО РЕЗЕРВА»

ПРИКАЗ

от «13» мая 2016 г. № 303 -од

Об организации работы по защите персональных данных, обрабатываемых в Автономном профессиональном образовательном учреждении Ханты-Мансийского автономного округа – Югры «Югорский колледж-интернат олимпийского резерва»

В соответствии с Федеральным законом Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом Российской Федерации от 27 июля 2006 года №152-ФЗ «О персональных данных», **приказываю:**

1. Назначить ответственными за организацию обработки персональных данных в Автономном профессиональном образовательном учреждении Ханты-Мансийского автономного округа – Югры «Югорский колледж-интернат олимпийского резерва» (далее - Учреждение) Максимову Яну Александровну – Начальника организационно-правового отдела - с возложением следующих обязанностей:

1.1 осуществление внутреннего контроля соблюдения Учреждением и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

1.2 доведение до сведения работников Учреждения положений законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

1.3 организация приема и обработки обращений и запросов субъектов персональных данных или их представителей и осуществление контроля приема и обработки таких обращений и запросов.

2. Назначить ответственным за обеспечение мер по защите сведений, обрабатываемых в информационных системах персональных данных Учреждения (администратором информационной безопасности), Тарасенко Дмитрия Константиновича – инженера-программиста отдела

охраны труда и инженерного обеспечения с возложением следующих обязанностей:

2.1 заведение и удаление учетных записей пользователей, управление полномочиями пользователей информационных систем и поддержание правил разграничения доступа в информационных системах;

2.2 управление средствами защиты информации в информационных системах, в том числе параметрами настройки программного обеспечения, включая программное обеспечение средств защиты информации, управление учетными записями пользователей, восстановление работоспособности средств защиты информации, генерация, смена и восстановление паролей;

2.3 установка обновлений программного обеспечения, включая программное обеспечение средств защиты информации, выпускаемых разработчиками (производителями) средств защиты информации или по их поручению;

2.4 централизованное управление системой защиты информации информационных систем (при необходимости);

2.5 сопровождение функционирования системы защиты информации информационных систем в ходе ее эксплуатации, включая корректировку эксплуатационной документации на нее и организационно-распорядительных документов по защите информации;

2.6 информирование пользователей об угрозах безопасности информации, о правилах эксплуатации системы защиты информации информационных систем и отдельных средств защиты информации, а также их обучение;

2.7 контроль (мониторинг) за обеспечением уровня защищенности информации, содержащейся в информационных системах:

2.8 контроль за событиями безопасности и действиями пользователей в информационных системах;

2.9 анализ и оценка функционирования системы защиты информации информационных систем, включая выявление, анализ и устранение недостатков в функционировании системы защиты информации информационных систем;

2.10 периодический анализ изменения угроз безопасности информации в информационных системах, возникающих в ходе ее эксплуатации, и принятие мер защиты информации в случае возникновения новых угроз безопасности информации;

2.11 документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в информационных системах;

2.12 принятие решения по результатам контроля (мониторинга) за обеспечением уровня защищенности информации о доработке

(модернизации) системы защиты информации информационных систем, повторной аттестации информационных систем или проведении дополнительных аттестационных испытаний.

2.13 взаимодействие с лицензиатами Федеральной службы по техническому и экспортному контролю (ФСТЭК) России и Федеральной службы безопасности (ФСБ) России в целях приведения информационных систем персональных данных Школы в соответствие с законодательством Российской Федерации о персональных данных;

2.14 разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

2.15 разработка и представление руководству предложений по обеспечению безопасности персональных данных.

3. Утвердить:

3.1 «Перечень персональных данных, обрабатываемых в информационной системе персональных данных «Сотрудники» (Приложение № 1 к настоящему приказу);

3.2 «Перечень лиц, имеющих право доступа к обработке персональных данных, содержащихся в информационной системе персональных данных «Сотрудники» (Приложение № 2 к настоящему приказу);

3.3 «Перечень лиц, имеющих право самостоятельного (неконтролируемого) пребывания в помещениях размещения ОТСС информационной системы персональных данных «Сотрудники» (Приложение № 3 к настоящему приказу);

3.4 «План мероприятий по обеспечению безопасности информации, обрабатываемой в информационной системе персональных данных «Сотрудники» на 2016 - 2017 год» (Приложение № 5 к настоящему приказу).

4. Ознакомить под роспись заинтересованных сотрудников Учреждения с настоящим приказом.

5. Контроль за исполнением приказа оставляю за собой.

Директор В.В. Малышкин