

ПРИКАЗ

20.03.2019

№ 147

Об утверждении Правил обработки персональных данных в информационных системах персональных данных в Отделе образования Администрации Обливского района

Во исполнение ст.86 Трудового Кодекса РФ от 30.12.2001 №197-ФЗ, ст.13.11. КоАП РФ от 30.12.2001 № 195-ФЗ, Федерального закона от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации" (с изменениями и дополнениями от 08.06.2020) Федерального закона от 27 июля 2006 г. № 152-ФЗ "О персональных данных" (с изменениями и дополнениями от 24.04.2020г.), Постановления Правительства РФ от 1 ноября 2012 г. № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", и в целях упорядочения особенностей хранения, защиты и обработки персональных данных работников Отдела образования

ПРИКАЗЫВАЮ:

1. Утвердить настоящие правила обработки персональных данных в информационных системах (программных продуктах) персональных данных («Контур-Экстерн», «1С-Бухгалтерия», «АЦК-финансы», «Сбербанк- Онлайн» (Приложение № 1).

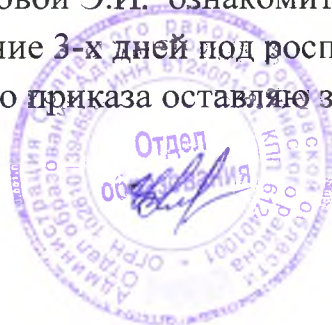
2. Назначить ответственных лиц за получение, обработку и хранение персональных данных:

- в части кадровой работы инспектора по кадрам Попову Э.И.;
- в части использования персональных данных для финансовых взаимодействий: главного бухгалтера – Лаптеву Л.А., зам.главного бухгалтера – Колесникову., бухгалтеров Марянину Е.Ю. и Севастьянову м.Г.

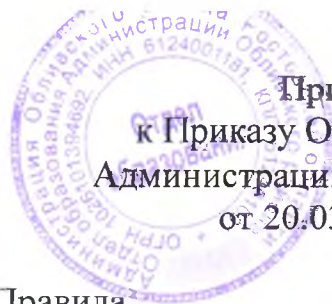
3. Инспектору по кадрам Поповой Э.И. ознакомить вышеуказанных работников с данным приказом в течение 3-х дней под роспись.

4. Контроль исполнения настоящего приказа оставляю за собой.

Заведующий Отделом образования
Администрации Обливского района



Н.А. Малахова



Приложение
к Приказу Отдела образования
Администрации Обливского района
от 20.03.2019 № 147

Правила
обработки персональных данных в информационных системах
(программных продуктах) персональных данных

1. Общие положения

1.1. Настоящие Правила разработаны в соответствии с положениями ФЗ "О персональных данных", постановления Правительства РФ от 6 июля 2008 г. № 512 "Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных", постановления Правительства РФ от 15 сентября 2008 г. № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации", постановления Правительства РФ от 1 ноября 2012 г. № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".

1.2. Настоящие Правила определяют особенности обработки персональных данных сотрудников в информационных системах персональных данных Отдела образования.

1.3. Безопасность персональных данных при их обработке в информационных системах персональных данных (далее - информационные системы) обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы.

1.4. Под актуальными угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, представление, распространение персональных данных, а также иные неправомерные действия.

2. Особенности обработки персональных данных в информационных системах

2.1. Обработка персональных данных в информационных системах осуществляется после завершения работ по созданию системы защиты персональных данных в информационной системе, ее проверки и оценки соответствия информационной системы персональных данных требованиям безопасности информации.

2.2. Безопасность персональных данных при их обработке в информационной системе обеспечивает оператор этой системы, который обрабатывает персональные данные, или лицо, осуществляющее обработку персональных данных по поручению оператора на основании заключаемого с этим лицом договора.

2.3. Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии.

2.4. Состав и содержание мер по защите информации в информационных системах зависят от установленного уровня защищенности информационной системы.

2.5. Установление уровня защищенности (пересмотр уровня защищенности) информационной системы персональных данных проводится инженером-электроником Отдела образования.

2.6. Разрешением на обработку персональных данных на объекте информационной системы является приказ руководителя о вводе указанного объекта в эксплуатацию.

2.7. Безопасность персональных данных, обрабатываемых с использованием средств автоматизации, достигается путем исключения несанкционированного, в том числе случайного доступа к персональным данным.

2.8. Персональные данные могут быть предоставлены для ознакомления:

а) сотрудникам, допущенным к обработке персональных данных с использованием средств автоматизации, в части, касающейся их должностных обязанностей.

2.9. Уполномоченными сотрудниками при обработке персональных данных в информационных системах персональных данных должна быть обеспечена их безопасность с помощью системы защиты, включающей организационные меры и средства защиты информации, в том числе шифровальные (криптографические) средства.

2.10. Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации организационных мер и путем применения программных и технических средств.

2.11. Доступ пользователей к персональным данным в информационных системах персональных данных разрешается после обязательного прохождения процедуры идентификации и аутентификации.

2.12. Лицами, ответственными за обеспечение безопасности персональных данных при их обработке в информационных системах, должно быть обеспечено:

а) своевременное обнаружение фактов несанкционированного доступа к персональным данным и немедленное доведение этой информации до руководства;

б) недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

в) возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

г) постоянный контроль за обеспечением уровня защищенности персональных данных;

д) знание и соблюдение условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

е) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

ж) при обнаружении нарушений порядка предоставления персональных данных незамедлительное приостановление предоставления персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин;

з) 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, разработка и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

2.13. В случае выявления нарушений порядка обработки персональных данных в информационных системах Отдела образования принимаются меры по установлению причин нарушений и их устранению.

Заведующий Отделом образования
Администрации Обливского района



Н.А. Малахова