Утверждено
И.о. директора ГБОУ СОШ №1 «ОЦ»
им. В.И. Фокина с. Большая Глушица
_____ О.А. Соколова
«01» сентября 2021 г.

ЭП

C=RU, O="ГБОУ СОШ №1 ""ОЦ"" им. В.И. Фокина с. Большая Глушица", CN=И.о. директора школы Соколова Ольга Александровна, E=shool1_bgl@samara.edu.ru
00a5938c76835cedd6
2021.11.26 14:30:27+04'00'

ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ ЛИЦА,
ОТВЕТСТВЕННОГО ЗАОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ
ПЕРСОНАЛЬНЫХ ДАННЫХ

1.Общие положения.

1.1. Данная должностная инструкция лица, ответственного за обеспечение безопасности персональных данных в ГБОУ СОШ №1 «ОЦ» им. В.И. Фокина с. Большая Глушица (далее-Инструкция) определяет основные обязанности и права ответственного за обеспечение безопасности персональных данных в ГБОУ СОШ №1 «ОЦ» им. В.И. Фокина с. Большая Глушица (далее – учреждение).
1.2. Ответственный за обеспечение безопасности персональных данных является штатным сотрудником Техникума.
1.3. Ответственный за обеспечение безопасности персональных данных назначается директором Техникума.
1.4. Решение вопросов обеспечения безопасности персональных данных входит в прямые служебные обязанности ответственного за обеспечение безопасности персональных данных.
1.5. Ответственный за обеспечение безопасности персональных данных обладает правами доступа к любым программным и аппаратным ресурсам, а также во все помещения, где ведется обработка персональных данных.

2.Должностные обязанности

Ответственный за обеспечение безопасности персональных данных обязан:
2.1. Знать перечень персональных данных и технических средств, входящих в информационные системы персональных данных (далее – ИСПДн) учреждения.
2.2. Представлять на утверждение список лиц, доступ которых к персональным данным, обрабатываемым в информационных системах, необходим для выполнения служебных (трудовых) обязанностей, а также изменений к нему.
2.3. По указанию руководства своевременно и точно отражать изменения в организационно-распорядительных и нормативных документах, касающихся обеспечения безопасности ПДн в Техникуме.
2.4. Доводить до сведения сотрудников Техникума положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных.

2.5. Осуществлять контроль выполнения требований локальных нормативных актов по защите ПДн сотрудниками Техникума.
2.6. Обеспечивать контроль действий администратора безопасности ИСПДн Техникума по обеспечению информационной безопасности.
2.7. Организовать учет применяемых средств защиты информации, эксплуатационной
и технической документации к ним, носителей персональных данных.
2.8. Вести журналы, необходимые для обеспечения безопасности ПДн.
2.9. Проводить разбирательства 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.
2.10. Обеспечить прекращение обработки персональных данных пользователям информационной системы при обнаружении нарушений порядка обработки персональных данных.
2.11. Участвовать в работе комиссии по уничтожению ПДн.
2.12. Организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов.
2.13. Осуществлять учет и периодический контроль за составом и полномочиями пользователей различных АРМ ИСПДн.
2.14. Периодически контролировать целостность печатей (пломб, наклеек) на устройствах защищенных АРМ.
2.15. Проводить работу по выявлению возможных каналов вмешательства в процесс функционирования ИС и осуществления НСД к информации и техническим средствам АРМ.
2.16. Участвовать в расследовании причин совершения нарушений и возникновения серьезных кризисных ситуаций в результате НСД.
2.17. Участвовать в работе комиссий по пересмотру планов защиты.

3.Права

Ответственный за обеспечение безопасности ПДн имеет право:
3.1. Требовать от пользователей информационных ресурсов выполнения требований локальных нормативных актов по защите персональных данных, в том числе выполнение инструкций, а также проводить проверку соблюдения данных требований.
3.2. Проводить служебные расследования по фактам нарушения установленных
Требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИСПДн.
3.3. Вносить свои предложения по совершенствованию мер защиты в ИСПДн.

4.Действия при обнаружении попыток несанкционированного доступа

4.1. К попыткам несанкционированного доступа относятся:
4.1.1. Сеансы работы с персональными данными незарегистрированных пользователей, пользователей, нарушивших установленную периодичность доступа или срок действия полномочия которых истек или превышающих свои полномочия по доступу к данным.
4.1.2. Действия постороннего лица, пытающегося получить доступ или уже получившего доступ к ИСПДн, при использовании учетной записи администратора или другого пользователя ИСПДн, методом подбора пароля, использования пароля, разглашенного владельцем учетной записи или любым другим методом.
4.2. При выявлении факта несанкционированного доступа Ответственный обязан:
4.2.1. По возможности пресечь дальнейший несанкционированный доступ к персональным данным.
4.2.2. Доложить должностному лицу Учреждения служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях.
4.2.3. Известить и.о. директора от имени учетной записи которого была осуществлена попытка несанкционированного доступа, о факте несанкционированного доступа.

4.2.4. Известить ответственного за организацию обработки персональных данных и администратора безопасности о факте несанкционированного доступа.

5.Ответственность

5.1. Ответственный за обеспечение безопасности персональных данных несет ответственность за соблюдение требований настоящей Инструкции, а также других нормативных документов в области защиты информации.

5.2. Ответственный за обеспечение безопасности персональных данных за разглашение информации ограниченного распространения, а также за нарушение порядка работы с документами или машинными носителями, содержащими такую информацию, может быть привлечен к дисциплинарной или иной, предусмотренной законодательством, ответственности.

5.3. Ответственный за обеспечение безопасности персональных данных несет ответственность за все действия, совершенные от имени его учетной записи или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.