

Муниципальное бюджетное общеобразовательное учреждение средняя общеобразовательная школа с.Новый Урух Ирафского района

Утверждаю:
Директор:  Надгериева Д.И.
приказ от 15.07.2022 г №59



План мероприятий по защите персональных данных

Для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных в соответствии требованиями Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» и Постановления Правительства Российской Федерации от 17.11.2007№ 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утвердить нижеперечисленные мероприятия.

В план включены следующие категории мероприятий:

- Организационные (административные);
- технические(аппаратные и программные);
- физические;
- контролирующие.

Мероприятия по защите персональных данных	Документы, соответствующие Мероприятиям по защите ПД
1. Назначение администратора информационной безопасности персональных данных, в случае отсутствия сотрудника, соответствующего квалификационным требованиям – заключить гражданско-правовой договор с юридическим лицом (индивидуальным предпринимателем).	Приказ о назначении администратора Информационной безопасности персональных данных или заключенный гражданско-правовой договор.
2.Разработка/уточнение Перечня информационных систем персональных данных (далее - ИСПДн).	Утвержденный Перечень ИСПДн.
3.Классификация ИСПДн.	Акт классификации уровня защищенности ИСПДн.
4. Обеспечение согласий субъектов ПД на обработку их ПД (в т.ч. проверка гражданско-правовых договоров с субъектами ПД, заключение при необходимости дополнительных соглашений Субъектами ПД).	Согласие субъектов ПД на обработку персональных данных, откорректированные гражданско-правовые договоры.

<p>5. Разработка перечня актуальных угроз безопасности ПД соответствующего класса информационных систем в соответствии с:</p> <ul style="list-style-type: none"> • Базовой моделью угроз безопасности персональных данных при их обработке в информационных системах персональных данных от 15.02.2008(ФСТЭК России); • Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных от 15.02.2008 (ФСТЭК России); • Методическими рекомендациями по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с 	<p>Модель угроз безопасности, перечни актуальных угроз безопасности для ИСПДн.</p>
<p>использованием средств автоматизации" от 21.02.2008 № 149/54-144(ФСБ России).</p>	
<p>6. Разработка мер по защите ПД (на основе моделей угроз), обеспечивающих нейтрализацию предполагаемых угроз безопасности ПД (Постановление Правительства РФ от 17.11.2007 № 781, методические документы ФСТЭК России).</p>	<p>Перечень организационных и технических мер по защите информации, перечень программных и технических средств защиты.</p>
<p>7. Ограничение доступа работников к персональным данным. Утверждение списка лиц, доступ которых к ПД необходим для выполнения служебных обязанностей (полный и ограниченный).</p>	<p>Приказ об утверждении перечня лиц, допущенных к обработке ПД. Определение перечня мест (помещений), где осуществляется обработка ПД. Инструкция о порядке допуска лиц к местам обработки ПД. Положение о разграничении прав доступа к обрабатываемым персональным данным в ИСПДн с матрицами доступа. Инструкция по учету лиц, допущенных к работе с ПДн Журнал учета лиц, допущенных к работе с персональными данными</p>
<p>8. Внесение изменений в должностные регламенты сотрудников (пользователей), обрабатывающих ПД, требования о соблюдении конфиденциальности ПД в период работы и после увольнения, а также ответственности за нарушение конфиденциальности ПД. Ознакомление (под подпись) сотрудников с изменениями в должностных регламентах.</p>	<p>Обновленные должностные обязанности лиц, допущенных к обработке персональных данных. Инструкция пользователю ИСПДн Инструкция администратору информационной безопасности Положение об ответственном за организацию обработки ПДн</p>

<p>9. Организация учета и контроля за соблюдением правил пользования средствами криптографической защиты информации (далее – СКЗИ) и условий их использования, указанных в правилах пользования (эксплуатации) на них (Типовые требования от 21.02.2008 № 149/6/6-622, ФСБ России)</p>	<p>Правила по обеспечению информационной безопасности на рабочем месте.</p>
<p>10. Поэкземплярный учет криптосредств, предназначенных для обеспечения безопасности ПД в ИСПДн, эксплуатационной и технической документации к ним и пользователей криптосредств;</p>	<p>Журнал по экземплярного учета ЭЦП, эксплуатационной и технической документации к ним. Список пользователей ЭЦП.</p>
<p>11. Разбирательство и составление заключений по фактам нарушения условий хранения носителей ПД, которые могут привести к нарушению конфиденциальности ПД или другим нарушениям, приводящим к снижению уровня защищенности ПД, разработку и принятие мер по предотвращению возможных опасных Последствий подобных нарушений.</p>	<p>Инструкция по организации работы с электронными носителями конфиденциальной информации. Положение по работе с инцидентами информационной безопасности Журнал учета инцидентов информационной безопасности</p>
<p>12. Регламенты работы с ИСПДн.</p>	<p>Политика информационной безопасности оператора ИСПДн Инструкция по организации работы с электронными носителями конфиденциальной информации Инструкция по осуществлению внутреннего контроля соответствия обработки персональных данных требованиям, предъявляемым к защите персональных данных.</p>
<p>13. Организация учета носителей информации</p>	<p>Журнал регистрации учета электронных носителей ПД Журнал выдачи/сдачи электронных носителей ПД Журнал передачи носителей ПД</p>
<p>14. Эксплуатация ИСПДн, мониторинг, выявление и реагирование на инциденты информационной безопасности</p>	<p>Совершенствование системы защиты ИСПДн (корректировки документации).</p>