Утверждено приказом №7п от «19» февраля 2021 года

План мероприятий по защите персональных данных

Для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных в соответствии с 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 с субъектами ПД).	Согласие субъектов ПД на обработку персональных данных, откорректированные гражданско-правовые договоры.
5. Разработка перечня актуальных угроз безопасности ПД соответствующего класса информационных систем в соответствии с: • 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	Модель угроз безопасности, перечни актуальных угроз безопасности для ИСПДн.

использованием средств автоматизации" от 21.02.2008 № 149/54-144 (ФСБ России).	
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).	Перечень организационных и технических мер по защите информации, перечень программных и технических средств защиты.
7. Ограничение доступа работников к персональным данным. Утверждение списка лиц, доступ которых к ПД необходим для выполнения служебных обязанностей (полный и ограниченный).	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
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.	Обновленные должностные обязанности лиц, допущенных к обработке персональных данных. Инструкция пользователю ИСПДн Инструкция администратору информационной безопасности Положение об ответственном за организацию обработки ПДн
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)	Правила по обеспечению информационной безопасности на рабочем месте.
10. Поэкземплярный учет криптосредств, предназначенных для обеспечения безопасности ПД в ИСПДн, эксплуатационной и технической документации к ним и пользователей криптосредств;	Журнал поэкземплярного учета ЭЦП, эксплуатационной и технической документации к ним. Список пользователей ЭЦП.
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.	Инструкция по организации работы с электронными носителями конфиденциальной информации. Положение по работе с инцидентами информационной безопасности Журнал учета инцидентов информационной безопасности

12 Регламенты работы с ИСПДн.	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.
13. Организация учета носителей информации	Журнал регистрации и учета электронных носителей ПД Журнал выдачи/сдачи электронных носителей ПД Журнал передачи носителей ПД
14. Эксплуатация ИСПДн, мониторинг, выявление и реагирование на инциденты информационной безопасности	Совершенствование системы защиты ИСПДн (корректировки документации).

Примечание:
Приведенный перечень мер по защите ПД не является исчерпывающим. Приведены лишь основные меры. Полный набор мер по защите ПД определится в процессе устранения замечаний по результатам комплексной проверки состояния защиты ПД для ИСПДн.
По результатам разработки и утверждения документов, соответствующих мероприятиям по защите ПД, провести аудит соответствия обработки персональных данных требованиям законодательства.