УТВЕРЖДАЮ

_____ _____

«_____» _____ 2020 г.

ПРОЕКТ

Порядок проведения мероприятий
по организации обработки и защите персональных данных
в ОРГАНИЗАЦИЯ

№	Мероприятие	Приказ	Регламент/ Политика	Инструкция/ правила	Журнал учета	Контроль (ФИО/Дата)	Примечания
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1.	Назначить ответственного за организацию обработки персональных данных	Проект приказа (09) «О назначении ответственного за организацию обработки ПДн» *Назначается: ФИО*	Не требуется	(09) Инструкция ответственного лица за организацию обработки персональных данных в данных	(30) Журнал проведения инструктажа по информационной безопасности (ознакомить ответственного)	*ФИО* 20.12.2020	Ответственному пройти повышение квалификации по направлению ИБ. Не критично для коммерческих организаций, но приветствуется регуляторами.
2.	Назначить лицо, представляющее ОРГАНИЗАЦИЮ при проведении проверок	Проект приказа (18) О назначении лица, уполномоченного представлять интересы ОРГАНИЗАЦИИ *Назначается: ФИО*	Не требуется	Не требуется	Не требуется	*ФИО* 20.12.2020	

№	Мероприятие	Приказ	Регламент/ Политика	Инструкция/ правила	Журнал учета	Контроль (ФИО/Дата)	Примечания
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
3.	Утвердить правила внутреннего контроля соответствия обработки ПДн. Утвердить план проведения внутреннего контроля.	Проект приказа (11) «Об утверждении правил внутреннего контроля соответствия…». (29) План проведения внутреннего контроля	Не требуется	(11) Правила осуществления внутреннего контроля	Не требуется	*ФИО* 20.12.2020	
4.	Утвердить план мероприятий по защите ПДн	(28) План мероприятий	Не требуется	Не требуется	Не требуется	*ФИО* 20.12.2020	
5.	Утвердить инструкцию о порядке проведения разбирательств	Утвердить в составе профильного приказа	Не требуется	(22) Инструкция о порядке проведения разбирательств	(30) Журнал проведения инструктажа по информационной безопасности (ознакомить ответственного)	Определить дополнительно	
6.	Утвердить Заключение об оценке вреда, который может быть причинен субъектам ПДн	(21) Акт оценки вреда субъектам ПДн	Не требуется	Не требуется	Не требуется	*ФИО* 20.12.2020	
7.	Утвердить положение по инцидентам ИБ	Проект приказа (20) «Об утверждении положения по инцидентам»	Не требуется	(20) Инструкция по работе с инцидентами	(30) Журнал учета инцидентов ИБ	*ФИО* 20.12.2020	

№	Мероприятие	Приказ	Регламент/ Политика	Инструкция/ правила	Журнал учета	Контроль (ФИО/Дата)	Примечания
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
8.	Утвердить приказ о контролируемой зоне	Проект приказа (03) «О контролируемой зоне»	Не требуется	Не требуется	Не требуется	*ФИО* 20.12.2020	К Контролируемой зоне относят помещения, доступ в которые контролируется, в которых принимаются меры по защите информации, в т.ч. меры по контролю за доступом к конфиденциальной информации и каналами её утечки. Если сотрудник, без специального разрешения, допустил обработку информации за пределами этой зоны - это нарушение; допустил вынос из контролируемой зоны носителей с защищаемой информацией - это нарушение и т.д. Сотрудники

№	Мероприятие	Приказ	Регламент/ Политика	Инструкция/ правила	Журнал учета	Контроль (ФИО/Дата)	Примечания
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
							должны быть уведомлены под роспись о границах контролируемой зоны, т.е. о границах, в пределах которых они имеют право обрабатывать защищаемую информацию. Определяемая контролируемая зона и уведомление сотрудников о её границах используется в дальнейшем, при расследовании инцидентов ИБ и определении нарушителей
9.	Утвердить Положение о порядке обработки и защиты персональных данных	Проект приказа (10) «Об утверждении Положения о порядке обработки и защиты ПДн» *Во исполнение:*	(10) Положение о порядке обработки и защиты персональных данных	(33) Инструкция в области обучения и повышения осведомленности персонала по вопросам	(31) Журнал проведения инструктажа по информационной безопасности (ознакомить	*ФИО* 20.12.2020	Организовать всем работникам ОРГАНИЗАЦИИ внутренние семинары и инструктажи.

№	Мероприятие	Приказ	Регламент/ Политика	Инструкция/ правила	Журнал учета	Контроль (ФИО/Дата)	Примечания
1	2	3	4	5	6	7	8
		Работниками ОРГАНИЗАЦИИ, работниками подрядных организаций		обеспечения информационной безопасности	работников ОРГАНИЗАЦИИ под подпись)		Возможно применение системы дистанционного электронного обучения и тестирования. Возможно применение методов социальной инженерии для поддержания осведомленности («тонуса», «настороженности») персонала в вопросах ИБ.
10.	Утвердить перечень ИСПДн в ОРГАНИЗАЦИИ	Проект приказа (04) «Об утверждении перечня информационных систем персональных данных»	Не требуется	Не требуется	Не требуется	*ФИО* 20.12.2020	
11.	Установить уровень защищенности ПДн при их обработке в ИСПДн	Проект приказа (01) «Об утверждении состава комиссии по установлению уровня защищенности»	Не требуется	(01) Методика определения уровня защищенности (01) Акты определения УЗ	Не требуется	*ФИО* 20.12.2020	Установление уровней защищенности позволяет упорядочить мероприятия по защите ПДн и привести

№	Мероприятие	Приказ	Регламент/ Политика	Инструкция/ правила	Журнал учета	Контроль (ФИО/Дата)	Примечания
1	2	3	4	5	6	7	8
							их в соответствие минимальным нормативным требованиям.
12.	Утвердить перечень обрабатываемых ПДн	(07) Приказ об утверждении перечня ПДн	Не требуется	Не требуется	Не требуется	*ФИО* 20.12.2020	Если при проведении внутреннего контроля обнаружится, что кем-то ведется обработка ПДн отсутствующих в перечне, то это будет являться основанием для проведения разбирательства и привлечения виновных к ответственности. (Обработка любых ПДн должна осуществляться для вполне конкретных законных целей).
13.	Определить правила доступа в помещения, в	Проект приказа (17) «Об утверждении правил доступа в помещения…»	Не требуется	(17) Инструкция по доступу работников ОРГА-	(30) Журнал проведения инструктажа по	*ФИО* 20.12.2020	

№	Мероприятие	Приказ	Регламент/ Политика	Инструкция/ правила	Журнал учета	Контроль (ФИО/Дата)	Примечания
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
	которых ведется обработка ПДн			НИЗАЦИИ в помещения в которых ведется обработка ПДн…	информационной безопасности (ознакомить работников ОРГАНИЗАЦИИ под подпись)		
14.	Определить места хранения материальных носителей ПДн	Проект приказа (05) «Об утверждении мест хранения материальных носителей персональных данных»	Не требуется	Не требуется	Не требуется	*ФИО* 20.12.2020	
15.	Разместить на официальном сайте (сайтах) организации документ, определяющий политику обработки ПДн	Проект приказа (08) «Об утверждении политики в отношении обработки персональных данных» _____ *Разместить на официальных сайтах ОРГАНИЗАЦИИ*	(08) Политика в отношении обработки персональных данных в ОРГАНИЗАЦИИ	Не требуется	Не требуется	*ФИО* 20.12.2020	
16.	Утвердить комплект проектных документов на создание системы технической защиты ПДн	Утвердить в составе профильного приказа	(37-38) Модели угроз и нарушителя; (39) Техническое задание на создание системы обеспе-		Не требуется	*ФИО* 20.12.2020	Согласовать с ответственными лицами

№	Мероприятие	Приказ	Регламент/ Политика	Инструкция/ правила	Журнал учета	Контроль (ФИО/Дата)	Примечания
1	2	3	4	5	6	7	8
			чения информационной безопасности (СОИБ)				
17.	Утвердить перечень должностей, допущенных к обработке ПДн	(06) Проект приказа об утверждении перечня должностей	Не требуется	Не требуется	Не требуется	*ФИО* 20.12.2020	
18.	Утвердить перечень допущенных к обработке ПДн лиц	(32) Проект приказа «О допуске сотрудников ОРГАНИЗАЦИИ к обработке персональных данных	(10) Положение по обработке ПДн	(27) Инструкция для работников, допущенных к обработке персональных данных в ОРГАНИЗАЦИИ	(30) Журнал проведения инструктажа по информационной безопасности (ознакомить работников ОРГАНИЗАЦИИ под подпись)	*ФИО* 20.12.2020	Организовать всем работникам ОРГАНИЗАЦИИ внутренние семинары и инструктажи. Не критично для коммерческих организаций, но приветствуется регуляторами.
19.	Назначить ответственного за защиту информа-	(02) Проект приказа «Об обеспечении безопасности	Не требуется	(02) Инструкция ответственного лица за защиту информации и	(30) Журнал проведения инструктажа по	*ФИО* 20.12.2020	Назначаются: тех. специалист, отвечающий за

№	Мероприятие	Приказ	Регламент/ Политика	Инструкция/ правила	Журнал учета	Контроль (ФИО/Дата)	Примечания
1	2	3	4	5	6	7	8
	ции и обеспечение безопасности ПДн	персональных данных при их обработке в информационных системах		обеспечение безопасности персональных данных.	информационной безопасности (ознакомить работников ОРГАНИЗАЦИИ под подпись)		организационную и техническую защиту ИСПДн
20.	Назначить администратора информационной безопасности	(02) Проект приказа «Об обеспечении безопасности персональных данных при их обработке в информационных системах	Не требуется	(02) Инструкция администратора информационной безопасности	(30) Журнал проведения инструктажа по информационной безопасности (ознакомить работников ОРГАНИЗАЦИИ под подпись)	*ФИО* 20.12.2020	Назначаются: Тех. специалист, обеспечивающий техническую защиту ИСПДн, включая администрирование средств защиты информации. Должность может совмещаться с п.19.
21.	Назначить администратора информационных систем ПДн	(02) Проект приказа «Об обеспечении безопасности персональных данных при их обработке в информационных системах	Не требуется	(02) Инструкция администратора информационных систем персональных данных	(30) Журнал проведения инструктажа по информационной безопасности (ознакомить работников ОРГАНИЗАЦИИ под подпись)	*ФИО* 20.12.2020	Назначаются: Тех. специалист, обеспечивающий администрирование ИСПДн

№	Мероприятие	Приказ	Регламент/ Политика	Инструкция/ правила	Журнал учета	Контроль (ФИО/Дата)	Примечания
1	2	3	4	5	6	7	8
22.	Утвердить инструкции по эксплуатации ИСПДн в части соблюдения мер ИБ	Утвердить в составе профильного приказа	Не требуется	(23) Инструкция по резервированию; (24) Инструкция по организации антивирусной защиты; (25) Инструкция по парольной защите; (26) Инструкция по учету носителей.	(30) Журнал проведения инструктажа по информационной безопасности (ознакомить работников ОРГАНИЗАЦИИ под подпись)	Администратор ИСПДн	
23.	Утвердить комплект организационно-распорядительных документов регулирующих порядок обработки ПДн, включая журналы учета.	Проекты приказов: (12) Проект приказа об Оценке вреда (вкл. Правила оценки); (13) Проект приказа об обезличивании ПДн (вкл. Правила и Состав комиссии); (14) Проект приказа о Порядке рассмотрения обращений (вкл. Регламент реагирования и форма журнала учета обращений);	(10) Политика безопасности ПДн	(30) Инструкция в области обучения и повышения осведомленности персонала по вопросам обеспечения информационной безопасности	(30) Журнал проведения инструктажа по информационной безопасности (ознакомить работников ОРГАНИЗАЦИИ под подпись)	*ФИО* 20.12.2020	Согласовать с ответственными лицами

№	Мероприятие	Приказ	Регламент/ Политика	Инструкция/ правила	Журнал учета	Контроль (ФИО/Дата)	Примечания
1	2	3	4	5	6	7	8
		(15) Проект приказа об уничтожении ПДн (вкл. состав комиссии и порядок уничтожения); (16) Проект приказа об утверждении типовых форм; (30) Проект приказа об утверждении форм журналов учета					
24.	Утвердить порядок неавтоматизированной обработки ПДн	(19) Проект приказа об утверждении правил неавтоматизированной обработки ПДн		(19) Правила неавтоматизированной обработки		*ФИО* 20.12.2020	
25.	Обеспечить включение в договоры со сторонними организациями и физическими лицами условия соблюдения требований по обеспечению защиты передаваемых/получаемых ПДн	Не требуется	(31) Регламент информационного взаимодействия со сторонними ИС	Не требуется	Не требуется	*ФИО* 20.12.2020	Обязательно к выполнению

№	Мероприятие	Приказ	Регламент/ Политика	Инструкция/ правила	Журнал учета	Контроль (ФИО/Дата)	Примечания
1	2	3	4	5	6	7	8
	(банки, гос.органы, контрагенты т.п.)						
26.	Организовать удаление или обезличивание ПДн, цель сбора которых достигнута	Проект приказа (15) «Об уничтожении персональных данных»	Не требуется	(15) Порядок уничтожения персональных данных при достижении целей обработки или при наступлении иных законных оснований	Не требуется	Регламент информационного взаимодействия со сторонними ИС	Удалить с АРМ и серверов папки, файлы с ПДн старше 5 лет (например), или переместить их на учтенный съемный носитель и поместить его в сейф/металлический шкаф
27.	Обеспечить хранение материальных носителей персональных данных (личные дела и т.д.) в сейф/шкаф или организовать помещение архива.	Проект приказа (05) «Об утверждении мест хранения материальных носителей персональных данных»	Не требуется	Не требуется	Не требуется	*ФИО* 20.12.2020	Обеспечить раздельное хранение материальных носителей с ПДн разной категории, с контролем доступа к ним. (напр. Данные ОК хранить отдельно от данных бух. учета и т.п.)
28.	Обеспечить информирование посетителей об осуществлении	Утвердить в составе профильного приказа	Не требуется	Не требуется	Не требуется	*ФИО* 20.12.2020	Разместить информационные таблички при входе, в местах

№	Мероприятие	Приказ	Регламент/ Политика	Инструкция/ правила	Журнал учета	Контроль (ФИО/Дата)	Примечания
1	2	3	4	5	6	7	8
	видеонаблюдения на территории путем размещения соответствующей информации в местах, обеспечивающих гарантированную видимость в дневное и ночное время						общего доступа, в помещениях с видеонаблюдением.
29.	Исключить обработку ПДн, не предусмотренную законодательством РФ в области ПДн, либо несовместимую с целями сбора ПДн	В рамках эксплуатационного контроля				*ФИО* 20.12.2020	Обязательно к выполнению. Ответственность п.1 ст.13.11КоАП
30.	Исключить обработку ПДн без согласия субъекта ПДн	В рамках эксплуатационного контроля				*ФИО* 20.12.2020	Обязательно к выполнению. Ответственность п.2 ст.13.11КоАП
31.	Обеспечить реализацию мероприятий по предоставлению субъектам ПДн	В рамках эксплуатационного контроля				*ФИО* 20.12.2020	Обязательно к выполнению. Ответственность п.4 ст.13.11КоАП

№	Мероприятие	Приказ	Регламент/ Политика	Инструкция/ правила	Журнал учета	Контроль (ФИО/Дата)	Примечания
1	2	3	4	5	6	7	8
	информации, касающейся обработки его ПДн.						
32.	Обеспечить реализацию мероприятий по выполнению требований субъектов ПДн либо уполномоченного органа об уточнении, блокировании или уничтожении ПДн.	В рамках эксплуатационного контроля				*ФИО* 20.12.2020	Обязательно к выполнению. Ответственность п.5 ст.13.11КоАП
33.	Обеспечить сохранность ПДн при хранении материальных носителей ПДн в случае неавтоматизированной обработки ПДн	В рамках эксплуатационного контроля				*ФИО* 20.12.2020	Обязательно к выполнению. Ответственность п.6 ст.13.11КоАП
34.	Обеспечить обезличивание ПДн, а так же разработку и соблюдение требований и/или методов по их обезличиванию	В рамках эксплуатационного контроля				*ФИО* 20.12.2020	Обязательно к выполнению. Ответственность по п.7 ст.13.11 КоАП

№	Мероприятие	Приказ	Регламент/ Политика	Инструкция/ правила	Журнал учета	Контроль (ФИО/Дата)	Примечания
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
35.	Обеспечить выполнение эксплуатационно-технических мероприятий по защите ПДн	В рамках эксплуатационного контроля				*ФИО* 20.12.2020	Учет средств защиты, контроль и разграничение доступа к СЗИ и к установленным параметрам конфигураций
36.	Обеспечить применение необходимых средств защиты информации на автоматизированных рабочих местах (АРМ) и серверах, в т.ч. сертифицированных ФСТЭК России СЗИ, ФСБ России СКЗИ (при необходимости их применения)	В рамках эксплуатационного контроля				*ФИО* 20.12.2020	Контроль версий, действующих сертификатов соответствия и т.д.
37.	Обеспечить установку необходимых параметров конф. используемых СЗИ в соответствии с проектной документацией СЗИ, нормативными	В рамках эксплуатационного контроля				*ФИО* 20.12.2020	Контроль актуальности проектной, эксплуатационно-технической документации и т.д.

№	Мероприятие	Приказ	Регламент/ Политика	Инструкция/ правила	Журнал учета	Контроль (ФИО/Дата)	Примечания
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
	требованиями ФСТЭК России, ФСБ России						
38.	Обеспечить оценку защищенности информационных систем персональных данных	В рамках эксплуатационного контроля				*ФИО* 20.12.2020	Наличие актов, протоколов и т.п. по оценке защищенности
39.	Для АРМ, подключаемых к ИСПДн, обеспечить проведение проверок на соответствие требованиям по защите информации	В рамках эксплуатационного контроля				*ФИО* 20.12.2020	Наличие актов, протоколов и т.п. по оценке защищенности