Процедура внедрения организационно-распорядительной документации в сфере обработки и обеспечения безопасности персональных данных ООО «Сатурн»

Москва 2018

Содержание

1 Информация о документе....5
1.1 Назначение документа....5
1.2 Цель принятия документа....5
1.3 Область применения документа....5
1.4 Вводимые сокращения и термины....5
1.5 Внешние нормативные и распорядительные документы....6
1.6 Пересмотр документа....7
2 Порядок внедрения....8
2.1 Основные этапы внедрения....8
2.2 Формирование рабочей группы....8
2.3 Назначение ответственных лиц....8
2.4 Адаптация организационно-распорядительных документов в области обработки и обеспечения безопасности персональных данных....9
2.5 Проведение организационных мероприятий по приведению процессов обработки персональных данных в соответствие....9
2.6 Создание системы защиты персональных данных....9
2.7 Проведение контролирующих мероприятий....10
3 Методика адаптации типовых проектов организационно-распорядительных документов....11
3.1 Политика в отношении обработки персональных данных....11
3.2 Публичная политика обработки персональных данных....11
3.3 Положение об организации обработки персональных данных....11
3.4 Перечень персональных данных, обрабатываемых в ООО «Сатурн»....12
3.5 Регламент взаимодействия с субъектами персональных данных....12
3.6 Регламент предоставления доступа к персональным данным....12
3.7 Перечень структурных подразделений и должностей, допущенных к обработке персональных данных....13
3.8 Регламент обмена персональными данными с третьими лицами....13
3.9 Перечень мест хранения бумажных носителей персональных данных в ООО «Сатурн»....13
3.10 Регламент обработки персональных данных без использования средств автоматизации....14
3.11 Регламент обращения с машинными носителями персональных данных....14
3.12 Регламент обезличивания персональных данных....14
3.13 Регламент уничтожения персональных данных....14
3.14 Регламент доступа в помещения, в которых ведется обработка персональных данных....15
3.15 Регламент взаимодействия с уполномоченными органами в сфере обработки и обеспечения безопасности персональных данных....15
3.16 Регламент ответственного за организацию обработки персональных данных....15
3.17 Положение об обеспечении безопасности персональных данных....16
3.18 Регламент ответственного за обеспечение безопасности персональных данных....16
3.19 Регламент оценки возможного вреда субъектам персональных данных....16
3.20 Регламент выделения информационных систем персональных данных и определения необходимого уровня защищенности персональных данных....17
3.21 Перечень информационных систем персональных данных....17
3.22 Регламент выбора мер по обеспечению безопасности персональных данных....17
3.23 Регламент управления инцидентами информационной безопасности....17
3.24 Регламент проведения периодических проверок в области обработки и обеспечения безопасности персональных данных....18
3.25 Приказ о порядке обработки персональных данных....18
3.26 Приказ о назначении ответственного за организацию обработки персональных данных....18
3.27 Приказ о назначении ответственного за обеспечение безопасности персональных данных....18
3.28 Приказ о создании комиссии по обеспечению безопасности персональных данных....19

3.29 Приказ об организации режима обеспечения безопасности помещений, в которых осуществляется обработка персональных данных....19
3.30 Приказ о создании системы защиты персональных данных....19
4 Методика внедрения типовых проектов организационно-распорядительных документов....1
4.1 Ролевая модель....1
4.2 Целевая аудитория документов....1

1 Информация о документе

1.1 Назначение документа

1.1.1 Настоящая процедура внедрения организационно-распорядительной документации в сфере обработки и обеспечения безопасности персональных данных ООО «Сатурн» определяет порядок адаптации и внедрения документов в ООО «Сатурн».

1.2 Цель принятия документа

1.2.1 Настоящая Процедура принята в целях унификации и упрощения процесса внедрения организационно-распорядительной документации в сфере обработки и обеспечения безопасности персональных данных.

1.3 Область применения документа

1.3.1 Настоящий документ обязаны знать и использовать в работе лица, назначенные ответственными за организацию обработки персональных данных, лица, назначенные ответственными за обеспечение безопасности персональных данных, а также члены комиссии по обеспечению безопасности персональных данных.

1.4 Вводимые сокращения и термины

Таблица 1 — Перечень сокращений

Сокращение	Расшифровка сокращения
ИСПДн	информационная система персональных данных
ИТ	информационные технологии
ПДн	персональные данные
ПП-1119	Постановление Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
П-21	Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
ФЗ-152	Федеральный закон от 27 июля 2006 г. № 152-ФЗ (ред. от 23.07.2013) «О персональных данных»
П-378	Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»

Таблица 2 — Перечень терминов

Термин	Определение термина
автоматизированная обработка персональных данных	обработка персональных данных с помощью средств вычислительной техники
доступ к информации	возможность получения информации и ее использования
информационная система персональных данных	совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств
обработка персональных данных	любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных
оператор персональных данных	государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными
персональные данные	любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)
предоставление персональных данных	действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц
трансграничная передача персональных данных	передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу
уровень защищенности персональных данных	комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных

1.5 Внешние нормативные и распорядительные документы

Таблица 3 — Внешние нормативные и распорядительные документы

№ п/п	Наименование документа
1	Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
2	Федеральный закон от 27 июля 2006 г. № 152-ФЗ (ред. от 23.07.2013) «О персональных данных»
3	Постановление Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
4	Постановление Правительства РФ от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

№ п/п	Наименование документа
5	Методические рекомендации по применению приказа Роскомнадзора от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных» (утв. Роскомнадзором 13.12.2013)
6	Разъяснения Роскомнадзора от 14.12.2012 «Вопросы, касающиеся обработки персональных данных работников, соискателей на замещение вакантных должностей, а также лиц, находящихся в кадровом резерве»
7	Разъяснения Роскомнадзора от 30.08.2013 «О вопросах отнесения фото- и видео-изображения, дактилоскопических данных и иной информации к биометрическим персональным данным и особенности их обработки»
8	Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
9	«Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (Выписка) (утв. ФСТЭК России 15.02.2008)
10	«Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. ФСТЭК России 14.02.2008)
11	Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»
12	«Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. ФСБ России 21.02.2008 № 149/6/6-622)
13	«Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации» (утв. ФСБ России 21.02.2008 № 149-54-144)

1.6 Пересмотр документа

1.6.1 Пересмотр настоящего документа должен осуществляться в следующих случаях, но не реже одного раза в три года:

- при изменении действующих нормативных правовых актов в области обеспечения безопасности персональных данных;
- при существенном изменении процессов обработки персональных данных ООО «Сатурн».

2 Порядок внедрения

2.1 Основные этапы внедрения

2.1.1 Внедрение организационно-распорядительной документации в ООО «Сатурн», включает в себя следующие этапы:

а) формирование рабочей группы по внедрению в ООО «Сатурн»;

б) назначение ответственных лиц;

в) адаптация организационно-распорядительных документов в области обработки и обеспечения безопасности персональных данных;

г) проведение организационных мероприятий по приведению процессов обработки персональных данных в соответствие;

д) выбор мер обеспечения безопасности персональных данных;

е) внедрение системы защиты персональных данных;

ж) проведение контролирующих мероприятий.

2.2 Формирование рабочей группы

2.2.1 С целью внедрения организационно-распорядительной документации в ООО «Сатурн» должна быть сформирована рабочая группа. В состав рабочей группы рекомендуется включить работников следующих структурных подразделений:

- подразделение, ответственное за управление персоналом;
- подразделение, ответственное за обеспечение информационной безопасности;
- подразделение, ответственное за правовое сопровождение деятельности ООО «Сатурн»;
- подразделение, ответственное за сопровождение ИТ-инфраструктуры и информационных систем ООО «Сатурн»;
- подразделение, ответственное за документооборот в ООО «Сатурн».

2.3 Назначение ответственных лиц

2.3.1 Рабочая группа определяет работников ООО «Сатурн», которые будут назначены ответственными в части обработки и обеспечения безопасности персональных данных. Действующим законодательством предусмотрены две роли в указанной области:

- Ответственный за организацию обработки персональных данных;
- Ответственный за обеспечение безопасности персональных данных.

2.3.2 Рабочая группа формирует состав Комиссии по обеспечению безопасности персональных данных в ООО «Сатурн». Рекомендуется включить в Комиссию тех же работников, которые входят в рабочую группу.

2.3.3 После определения ответственных лиц рабочая группа должна распределить функции по организации обработки и обеспечения безопасности персональных данных между ответственными лицами. Рекомендуемая матрица ролей приведена в разделе 4.1.

2.4 Адаптация организационно-распорядительных документов в области обработки и обеспечения безопасности персональных данных

2.4.1 Рабочая группа осуществляет доработку типовых проектов организационно-распорядительных документов, исходя из фактических процессов обработки и обеспечения безопасности персональных данных в ООО «Сатурн»и ролевой модели, определенной на предыдущем этапе.

2.4.2 Доработка проводится согласно методике адаптации, приведенной в разделе 4.

2.4.3 Доработанные организационно-распорядительные документы должны быть введены в действие.

2.5 Проведение организационных мероприятий по приведению процессов обработки персональных данных в соответствие

2.5.1 Лица, назначенные Ответственными за организацию обработки и обеспечение безопасности персональных данных, проводят следующие первоочередные мероприятия по приведению процессов обработки в соответствие:

а) ознакомление работников с внутренними организационно-распорядительными документами согласно матрице ознакомления, приведенной в разделе 4.2;

б) размещение публичной политики обработки персональных данных в открытом доступе;

в) проведение инструктажа работникам, допущенным к обработке персональных данных, и взятие с них обязательства о неразглашении, согласно регламенту предоставления доступа к персональным данным;

г) получение письменного согласия субъектов персональных данных согласно регламенту взаимодействия с субъектами персональных данных;

д) оснащение помещений, в которых хранятся материальные носители персональных данных, запирающимися шкафами (сейфами), исходя из требований регламента обработки персональных данных без использования средств автоматизации;

е) проведение учета машинных носителей персональных данных согласно регламенту обращения с машинными носителями персональных данных.

2.6 Создание системы защиты персональных данных

2.6.1 Члены Комиссии по обеспечению безопасности персональных данных участвуют в приемки системы защиты персональных данных, разработка и внедрение которой включает следующие этапы:

- разработка технического задания на систему защиты персональных данных;
- разработка технического проекта системы защиты персональных данных
- внедрение технических средств защиты информации;
- опытная эксплуатация системы защиты персональных данных;

– введение системы защиты персональных данных в промышленную эксплуатацию.

2.7 Проведение контролирующих мероприятий

2.7.1 Члены Комиссии по обеспечению безопасности персональных данных проводят внутренние проверки процессов обработки и обеспечения безопасности персональных данных в ООО «Сатурн»согласно регламенту проведения периодических проверок в области обработки и обеспечения безопасности персональных данных.

3 Методика адаптации типовых проектов организационно-распорядительных документов

3.1 Политика в отношении обработки персональных данных

3.1.1 Основание для разработки документа:

– ФЗ-152;

3.1.2 Документ должен быть размещен в открытом доступе (на доске информации рядом с отделом кадров, на корпоративном портале).

3.1.3 Целевая аудитория документа:

– все субъекты персональных данных;
– все работники ООО «Сатурн»;
– Ответственный за организацию обработки персональных данных;
– Ответственный за обеспечение безопасности персональных данных.

3.2 Публичная политика обработки персональных данных

3.2.1 Основание для разработки документа:

– п.2 ч.1 ст.18.1 ФЗ-152;
– ч.2 ст.18.1 ФЗ-152.

3.2.2 Документ должен быть размещен в открытом доступе (на доске информации рядом с отделом кадров, на корпоративном портале).

3.2.3 Целевая аудитория документа:

– все субъекты персональных данных;
– все работники ООО «Сатурн»;
– Ответственный за организацию обработки персональных данных;
– Ответственный за обеспечение безопасности персональных данных.

3.2.4 Порядок адаптации документа:

– в пункте 2.6 необходимо проверить и уточнить перечень персональных данных работников, которые включают в общедоступные источники персональных данных;
– в пункте 4.2 необходимо привести актуальный перечень лиц, которым ООО «Сатурн» поручает обработку персональных данных, с указанием целей поручения обработки и юридических адресов;

3.3 Положение об организации обработки персональных данных

3.3.1 Основание для разработки документа:

– п.2, 6 ч.1 ст.18.1 ФЗ-152;
– ст.8, 10, 11, 12, 16 ФЗ-152;
– п.4-5, 8 ст.86 ТК РФ.

3.3.2 Целевая аудитория документа:

– все работники ООО «Сатурн»;
– Ответственный за организацию обработки персональных данных;
– Ответственный за обеспечение безопасности персональных данных.

3.3.3 Порядок адаптации документа:

– в пункте 2.1.6 необходимо уточнить перечень персональных данных работников, которые включают в общедоступные источники персональных данных;

3.4 Перечень персональных данных, обрабатываемых в ООО «Сатурн»

3.4.1 Основание для разработки документа:

– ст.5 ФЗ-152;
– п.2 ч.1 ст.18.1 ФЗ-152.

3.4.2 Целевая аудитория документа:

– все работники ООО «Сатурн»;
– Ответственный за организацию обработки персональных данных;
– Ответственный за обеспечение безопасности персональных данных;

3.5 Регламент взаимодействия с субъектами персональных данных

3.5.1 Основание для разработки документа:

– п.2 ч.1 ст.18.1 ФЗ-152;
– п.6 ч.1 ст.18.1 ФЗ-152;
– ч.4 ст.9 ФЗ-152;
– п.8 ст.86 ТК РФ.

3.5.2 Целевая аудитория документа:

– все работники ООО «Сатурн»;
– Ответственный за организацию обработки персональных данных;
– Ответственный за обеспечение безопасности персональных данных.

3.6 Регламент предоставления доступа к персональным данным

3.6.1 Основание для разработки документа:

– п.2 ч.1 ст.18.1 ФЗ-152;
– пп. в) п. 13 ПП-1119;
– пп. в) п. 5 П-378.

3.6.2 Целевая аудитория документа:

– работники ООО «Сатурн», допущенные к обработке персональных данных;
– Ответственный за организацию обработки персональных данных;

– Ответственный за обеспечение безопасности персональных данных.

3.6.3 Порядок адаптации документа:

– в разделе 3.4 необходимо уточнить последовательность прохождения и согласования заявки на доступ к ИСПДн исходя из общего порядка предоставления доступа к информационным системам, принятого в ООО «Сатурн».

3.7 Перечень структурных подразделений и должностей, допущенных к обработке персональных данных

3.7.1 Основание для разработки документа:

– пп. в) п. 13 ПП-1119;

– пп. в) п. 5 П-378.

3.7.2 Целевая аудитория документа:

– работники ООО «Сатурн», допущенные к обработке персональных данных;

– Ответственный за организацию обработки персональных данных;

– Ответственный за обеспечение безопасности персональных данных.

3.7.3 Порядок адаптации документа:

– в колонках «Наименование структурного подразделения» и «Должность» необходимо указать все подразделения и должности, предполагающие обработку персональных данных;

– в колонке «ИСПДн», к которой предоставлен доступ, указываются все ИСПДн, к которым должен быть допущен работник, занимающий соответствующую должность.

3.8 Регламент обмена персональными данными с третьими лицами

3.8.1 Основание для разработки документа:

– ч.3 ст.6 ФЗ-152;

– п.3 ПП-1119.

3.8.2 Целевая аудитория документа:

– работники ООО «Сатурн», допущенные к обработке персональных данных;

– Ответственный за организацию обработки персональных данных;

– Ответственный за обеспечение безопасности персональных данных.

3.9 Перечень мест хранения бумажных носителей персональных данных в ООО «Сатурн»

3.9.1 Основание для разработки документа:

– ПП-687.

3.9.2 Целевая аудитория документа:

– работники ООО «Сатурн», допущенные к обработке персональных данных;

– Ответственный за организацию обработки персональных данных;
– Ответственный за обеспечение безопасности персональных данных.

3.9.3 Порядок адаптации документа:

– необходимо проверить и уточнить места хранения бумажных носителей и срок их хранения, исходя из фактических процессов хранения бумажных носителей персональных данных

3.10 Регламент обработки персональных данных без использования средств автоматизации

3.10.1 Основание для разработки документа:

– ПП-687.

3.10.2 Целевая аудитория документа:

– работники ООО «Сатурн», допущенные к обработке персональных данных;
– Ответственный за организацию обработки персональных данных;
– Ответственный за обеспечение безопасности персональных данных.

3.11 Регламент обращения с машинными носителями персональных данных

3.11.1 Основание для разработки документа:

– п. 5 ч. 2 ст. 19 ФЗ-152;
– пп. б) п. 13 ПП-1119;
– пп. б) п. 5 П-378.

3.11.2 Целевая аудитория документа:

– работники ООО «Сатурн», допущенные к обработке персональных данных;
– Ответственный за организацию обработки персональных данных;
– Ответственный за обеспечение безопасности персональных данных.

3.12 Регламент обезличивания персональных данных

3.12.1 Основание для разработки документа:

– Приказ Роскомнадзора от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных».

3.12.2 Целевая аудитория документа:

– работники ООО «Сатурн», допущенные к обработке персональных данных;
– Ответственный за организацию обработки персональных данных;
– Ответственный за обеспечение безопасности персональных данных.

3.13 Регламент уничтожения персональных данных

3.13.1 Основание для разработки документа:

– ч.7 ст.5 ФЗ-152.

3.13.2 Целевая аудитория документа:

– работники ООО «Сатурн», допущенные к обработке персональных данных;
– Ответственный за организацию обработки персональных данных;
– Ответственный за обеспечение безопасности персональных данных.

3.14 Регламент доступа в помещения, в которых ведется обработка персональных данных

3.14.1 Основание для разработки документа:

– пп. а) п. 13 ПП-1119;
– пп. а) п. 5 П-378.

3.14.2 Целевая аудитория документа:

– работники ООО «Сатурн», допущенные к обработке персональных данных;
– Ответственный за организацию обработки персональных данных;
– Ответственный за обеспечение безопасности персональных данных.
– в разделе 2.1.4 необходимо уточнить название документа (документов), определяющего порядок осуществления пропускного и внутриобъектового режима в ООО «Сатурн».

3.15 Регламент взаимодействия с уполномоченными органами в сфере обработки и обеспечения безопасности персональных данных

3.15.1 Основание для разработки документа:

– ст. 20-22 ФЗ-152.

3.15.2 Целевая аудитория документа:

– Ответственный за организацию обработки персональных данных;
– Ответственный за обеспечение безопасности персональных данных.

3.16 Регламент ответственного за организацию обработки персональных данных

3.16.1 Основание для разработки документа:

– п.1 ч.1 ст.18.1 ФЗ-152;
– ст.22.1 ФЗ-152.

3.16.2 Целевая аудитория документа:

– Ответственный за организацию обработки персональных данных.

3.16.3 Порядок адаптации документа:

– часть обязанностей ответственного за организацию обработки персональных данных, указанных в разделе 2.1, может быть перераспределена между ответственным за обеспечение безопасности персональных данных и членами

комиссии по обеспечению безопасности персональных данных исходя из существующего распределения обязанностей в ООО «Сатурн».

3.17 Положение об обеспечении безопасности персональных данных

3.17.1 Основание для разработки документа:

– ст.18.1, 19 ФЗ-152;
– ПП-1119;
– П-378.

3.17.2 Целевая аудитория документа:

– Ответственный за обеспечение безопасности персональных данных.

3.17.3 Порядок адаптации документа:

– в пункте 3.5 необходимо уточнить перечень технических подсистем защиты, которые реализованы (планируются к реализации) в ООО «Сатурн»;
– в пункте 5.2 необходимо уточнить перечень лиц, входящих в состав Комиссии по обеспечению безопасности персональных данных;
– в пункте 5.3 необходимо уточнить порядок утверждения состава Комиссии по обеспечению безопасности персональных данных;
– часть обязанностей Комиссии по обеспечению безопасности персональных данных, указанных в разделе 5.4, может быть перераспределена между ответственным за организацию обработки персональных данных и ответственным за обеспечение безопасности персональных данных исходя из существующего распределения обязанностей в ООО «Сатурн».

3.18 Регламент ответственного за обеспечение безопасности персональных данных

3.18.1 Основание для разработки документа:

– п. 14 ПП-1119.

3.18.2 Целевая аудитория документа:

– Ответственный за обеспечение безопасности персональных данных.

3.18.3 Порядок адаптации документа:

– часть обязанностей ответственного за обеспечение безопасности персональных данных, указанных в разделе 2.1, может быть перераспределена между ответственным за организацию обработки персональных данных и членами комиссии по обеспечению безопасности персональных данных исходя из существующего распределения обязанностей в ООО «Сатурн».

3.19 Регламент оценки возможного вреда субъектам персональных данных

3.19.1 Основание для разработки документа:

– п.5 ч.1 ст.18.1 ФЗ-152;
– п. 7 ПП-1119.

3.19.2 Целевая аудитория документа:

– члены комиссии по обеспечению безопасности ПДн.

3.20 Регламент выделения информационных систем персональных данных и определения необходимого уровня защищенности персональных данных

3.20.1 Основание для разработки документа:

– ПП-1119.

3.20.2 Целевая аудитория документа:

– члены комиссии по обеспечению безопасности ПДн.

3.21 Перечень информационных систем персональных данных

3.21.1 Основание для разработки документа:

– ПП-1119.

3.21.2 Целевая аудитория документа:

– члены комиссии по обеспечению безопасности ПДн.

3.21.3 Порядок адаптации документа:

– в соответствующих колонках таблицы проверить и уточнить наименование, назначение и основные характеристики ИСПДн, информационные системы, входящие в состав ИСПДн, а также категории субъектов персональных данных и сроки их хранения.

3.22 Регламент выбора мер по обеспечению безопасности персональных данных

3.22.1 Основание для разработки документа:

– п. 9 П-21.

3.22.2 Целевая аудитория документа:

– члены комиссии по обеспечению безопасности ПДн.

3.23 Регламент управления инцидентами информационной безопасности

3.23.1 Основание для разработки документа:

– п. 6 ч. 2 ст. 19 ФЗ-152.

3.23.2 Целевая аудитория документа:

– члены комиссии по обеспечению безопасности ПДн.

3.23.3 Порядок адаптации документа:

– в таблице 5 в колонке «Длительность и начало выполнения» необходимо уточнить сроки выполнения этапов, исходя из фактических бизнес-процессов компании. Аналогичные изменения необходимо внести в соответствующих абзацах разделов 2.2 и 2.3;
– в таблице 5 в колонке «Подразделение / Должность» необходимо уточнить соответствующие названия подразделений и должностей ООО «Сатурн».

3.24 Регламент проведения периодических проверок в области обработки и обеспечения безопасности персональных данных

3.24.1 Основание для разработки документа:

– п. 4, 9 ч. 2 ст. 19 ФЗ-152;
– п. 17 ПП-1119;
– п. 6 П-21.

3.24.2 Целевая аудитория документа:

– члены комиссии по обеспечению безопасности ПДн.

3.25 Приказ о порядке обработки персональных данных

3.25.1 Порядок адаптации документа:

– документ необходимо оформить на бланке ООО «Сатурн»;
– необходимо указать должность и ФИО лица, ответственного за исполнение приказа, а также лица, подписывающего приказ.

3.26 Приказ о назначении ответственного за организацию обработки персональных данных

3.26.1 Порядок адаптации документа:

– документ необходимо оформить на бланке ООО «Сатурн»;
– необходимо указать должность и ФИО лица, ответственного за организацию обработки персональных данных, ответственного за исполнение приказа, а также лица, подписывающего приказ.

3.27 Приказ о назначении ответственного за обеспечение безопасности персональных данных

3.27.1 Порядок адаптации документа:

– документ необходимо оформить на бланке ООО «Сатурн»;
– необходимо указать должность и ФИО лица, ответственного за обеспечение безопасности персональных данных, ответственного за исполнение приказа, а также лица, подписывающего приказ.

3.28 Приказ о создании комиссии по обеспечению безопасности персональных данных

3.28.1 Основание для разработки документа:

– п.4, 5 ч.1 ст.18.1 ФЗ-152;
– ПП-1119;
– п. 9 П-21.

3.28.2 Целевая аудитория документа:

– члены комиссии по обеспечению безопасности ПДн.

3.28.3 Порядок адаптации документа:

– документ необходимо оформить на бланке ООО «Сатурн»;
– необходимо указать должность и ФИО членов комиссии по обеспечению безопасности персональных данных, ответственного за исполнение приказа, а также лица, подписывающего приказ.

3.29 Приказ об организации режима обеспечения безопасности помещений, в которых осуществляется обработка персональных данных

3.29.1 Порядок адаптации документа:

– документ необходимо оформить на бланке ООО «Сатурн»;
– необходимо указать подразделение и должность лиц, допущенных в серверные помещения; указать ФИО и должность ответственного за исполнение приказа, а также лица, подписывающего приказ.

3.30 Приказ о создании системы защиты персональных данных

3.30.1 Порядок адаптации документа:

– документ необходимо оформить на бланке ООО «Сатурн»;
– необходимо указать ФИО и должности лиц, ответственных за эксплуатацию средств защиты информации, ответственного за исполнение приказа, а также лица, подписывающего приказ.

4 Методика внедрения типовых проектов организационно-распорядительных документов

4.1 Ролевая модель

В ходе внедрения организационно-распорядительной документации необходимо распределить функции по организации обработки и обеспечения безопасности персональных данных между ответственными лицами. Рекомендуемая модель распределения функций (ролевая модель) приведена в таблице 4.

Таблица 4 — Ролевая модель

№ п/п	Функция	Ответственный за исполнение	Документ, в котором описана реализация функции
1	Взаимодействие с субъектами персональных данных	Ответственный за организацию обработки ПДн	Регламент взаимодействия с субъектами персональных данных
2	Взаимодействие с Роскомнадзором	Ответственный за организацию обработки ПДн	Регламент взаимодействия с уполномоченными органами
3	Взаимодействие с ФСТЭК России и ФСБ России	Ответственный за обеспечение безопасности ПДн	Регламент взаимодействия с уполномоченными органами
4	Актуализация внутренних организационно-распорядительных документов в области обработки персональных данных	Ответственный за организацию обработки ПДн	Процедура внедрения организационно-распорядительной документации в сфере обработки и обеспечения безопасности персональных данных
5	Актуализация внутренних организационно-распорядительных документов в области обеспечения безопасности персональных данных	Ответственный за обеспечение безопасности ПДн	Процедура внедрения организационно-распорядительной документации в сфере обработки и обеспечения безопасности персональных данных
6	Предоставление допуска к обработке персональных данных и доступа в информационные системы персональных данных	Ответственный за организацию обработки ПДн Ответственный за обеспечение безопасности ПДн	Регламент предоставления доступа к персональным данным
7	Проведение инструктажей по порядку обработки персональных данных	Ответственный за организацию обработки ПДн	Регламент предоставления доступа к персональным данным

№ п/п	Функция	Ответственный за исполнение	Документ, в котором описана реализация функции
8	Проведение инструктажей по порядку обеспечения безопасности ПДн	Ответственный за обеспечение безопасности ПДн	Регламент предоставления доступа к персональным данным
9	Обеспечению учета и сохранности бумажных и машинных носителей персональных данных	Ответственный за обеспечение безопасности ПДн	Регламент обработки персональных данных без использования средств автоматизации Регламент обращения с машинными носителями персональных данных
10	Обеспечение режима безопасности помещений, в которых размещены компоненты ИСПДн	Ответственный за обеспечение безопасности ПДн	Регламент доступа в помещения, в которых ведется обработка персональных данных
11	Оценка вреда, который может быть причинен субъекту персональных данных	Члены Комиссии по обеспечению безопасности ПДн	Регламент оценки возможного вреда субъектам персональных данных
12	Выделение информационных систем персональных данных	Члены Комиссии по обеспечению безопасности ПДн	Регламент выделения информационных систем персональных данных и определения необходимого уровня защищенности персональных данных
13	Разработка модели угроз и нарушителя безопасности ПДн для каждой ИСПДн	Члены Комиссии по обеспечению безопасности ПДн	Регламент выделения информационных систем персональных данных и определения необходимого уровня защищенности персональных данных
14	Определение необходимого уровня защищенности ПДн при их обработке в ИСПДн	Члены Комиссии по обеспечению безопасности ПДн	Регламент выделения информационных систем персональных данных и определения необходимого уровня защищенности персональных данных
15	Выбор мер по обеспечению безопасности персональных данных	Члены Комиссии по обеспечению безопасности ПДн	Регламент выбора мер по обеспечению безопасности персональных данных
16	Реагирование на инциденты информационной безопасности	Члены Комиссии по обеспечению безопасности ПДн	Регламент управления инцидентами информационной безопасности
17	Внутренний контроль за соблюдением законодательства РФ о персональных данных	Члены Комиссии по обеспечению безопасности ПДн	Регламент проведения периодических проверок в области обработки и обеспечения безопасности персональных данных
18	Обеспечение функционирования системы защиты персональных данных	Ответственный за обеспечение безопасности ПДн	Приказ о создании системы защиты персональных данных

4.2 Целевая аудитория документов

4.2.1 Ознакомление работников ООО «Сатурн» с внутренними организационно-распорядительными документами в области обработки и обеспечения безопасности персональных данных проводится согласно матрице ознакомления (таблица 5).

Таблица 5 — Матрица ознакомления с документами

№ п/п	Наименование документа	Все субъекты ПДн	Все работники	Работники, допущенные к обработке ПДн	Ответственный за организацию обработки ПДн	Ответственный за обеспечение безопасности ПДн	Члены комиссии по обеспечению безопасности ПДн
1	Политика в отношении обработки персональных данных						
2	Публичная политика обработки персональных данных						
3	Положение об организации обработки персональных данных						
4	Перечень персональных данных, обрабатываемых						
5	Регламент взаимодействия с субъектами персональных данных						
6	Регламент предоставления доступа к персональным данным						
7	Перечень структурных подразделений и должностей, допущенных к обработке персональных данных						
8	Регламент обмена персональными данными с третьими лицами						
9	Регламент обработки персональных данных без использования средств автоматизации						
10	Перечень мест хранения бумажных носителей персональных данных						
11	Регламент обращения с машинными носителями персональных данных						
12	Регламент обезличивания персональных данных						
13	Регламент уничтожения персональных данных						
14	Регламент доступа в помещения, в которых ведется обработка персональных данных						
15	Регламент взаимодействия с уполномоченными органами						
16	Регламент ответственного за организацию обработки персональных данных						
17	Положение об обеспечении безопасности персональных данных						
18	Регламент ответственного за обеспечение безопасности персональных данных						
19	Регламент оценки возможного вреда субъектам персональных данных						
20	Регламент выделения информационных систем персональных данных и определения необходимого уровня защищенности персональных данных						
21	Регламент выбора мер по обеспечению безопасности персональных данных						
22	Регламент управления инцидентами информационной безопасности						
23	Регламент проведения периодических проверок в области обработки и обеспечения безопасности персональных данных						