РЕГЛАМЕНТ
выбора мер по обеспечению безопасности персональных данных в ООО «Сатурн»

Москва 2018

Содержание

1 Информация о документе....3
1.1 Назначение документа....3
1.2 Цель принятия документа....3
1.3 Область применения документа....3
1.4 Вводимые сокращения и термины....3
1.5 Внешние нормативные и распорядительные документы....4
1.6 Внутренние нормативные и распорядительные документы....4
1.7 Пересмотр документа....5
2 Порядок выбора мер по обеспечению безопасности персональных данных....6
2.1 Методика выбора мер по обеспечению безопасности персональных данных....6
2.2 Определение базового набора мер по обеспечению безопасности персональных данных....6
2.3 Адаптация базового набора мер по обеспечению безопасности персональных данных....7
2.4 Уточнение адаптированного базового набора мер по обеспечению безопасности персональных данных....8
2.5 Дополнение уточненного адаптированного базового набора мер по обеспечению безопасности персональных данных....8
2.6 Результаты определения состава и содержания мер по обеспечению безопасности персональных данных....8

1 Информация о документе

1.1 Назначение документа

1.1.1 Настоящий Регламент выбора мер по обеспечению безопасности персональных данных в ООО «Сатурн» (далее – Регламент) определяет порядок выбора мер по обеспечению безопасности персональных данных в ООО «Сатурн» (далее – Общество).

1.2 Цель принятия документа

1.2.1 Настоящий Регламент принят в целях обеспечения соответствия требованиям Федерального закона «О персональных данных».

1.3 Область применения документа

1.3.1 Настоящий документ обязан знать и использовать в работе Ответственный за обеспечение безопасности персональных данных.

1.4 Вводимые сокращения и термины

Таблица 1 — Перечень сокращений

Сокращение	Расшифровка сокращения
ПДн	персональные данные
ИСПДн	информационная система персональных данных
Приказ № 21	Приказ ФСТЭК России от 18.02.2014 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

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

Термин	Определение термина
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. № 152-ФЗ (ред. от 24.07.2014) «О персональных данных»
2	Постановление Правительства РФ от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
3	Приказ ФСТЭК России от 18.02.2014 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»
4	«Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (Выписка) (утв. ФСТЭК России 16.02.2008)
5	«Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. ФСТЭК России 14.02.2008)

1.6 Внутренние нормативные и распорядительные документы

Таблица 4 — Внутренние нормативные и распорядительные документы

№ п/п	Наименование документа
1	Положение об организации обработки персональных данных
2	Публичная политика обработки персональных данных

№ п/п	Наименование документа
3	Регламент взаимодействия с уполномоченными органами в сфере обработки и обеспечения безопасности персональных данных

1.7 Пересмотр документа

1.7.1 Пересмотр настоящего Регламента должен осуществляться в следующих случаях:

– при изменении действующих нормативных правовых актов в области обеспечения безопасности персональных данных;

– при существенном изменении процессов обработки персональных данных Общества.

2 Порядок выбора мер по обеспечению безопасности персональных данных

2.1 Методика выбора мер по обеспечению безопасности персональных данных

2.1.1 Выбор мер по обеспечению безопасности персональных данных, подлежащих реализации в информационной системе персональных данных Общества в рамках обеспечения безопасности персональных данных, включает:

а) **определение базового набора мер по обеспечению безопасности персональных данных** для установленного уровня защищенности персональных данных при их обработке в ИСПДн в соответствии с базовыми наборами мер по обеспечению безопасности персональных данных, приведенными в Приказе № 21;

б) **адаптацию базового набора мер по обеспечению безопасности персональных данных** с учетом структурно-функциональных характеристик информационной системы персональных данных, информационных технологий, особенностей функционирования информационной системы персональных данных (в том числе исключение из базового набора мер, непосредственно связанных с информационными технологиями, не используемыми в информационной системе персональных данных, или структурно-функциональными характеристиками, не свойственными информационной системе персональных данных);

в) **уточнение адаптированного базового набора мер по обеспечению безопасности персональных данных** с учетом не выбранных ранее мер, приведенных в Приказе № 21, в результате чего определяются меры по обеспечению безопасности персональных данных, обеспечивающие блокирование (нейтрализацию) всех актуальных угроз безопасности персональных данных;

г) **дополнение уточненного адаптированного базового набора мер по обеспечению безопасности персональных данных** мерами, обеспечивающими выполнение требований нормативных правовых актов в области обеспечения безопасности персональных данных (за исключением требований Приказа №21, уже учтенных в базовом наборе).

2.2 Определение базового набора мер по обеспечению безопасности персональных данных

2.2.1 Определение базового набора мер по обеспечению безопасности персональных данных основывается на уровне защищенности персональных данных, установленном в соответствии с Регламентом выделения ИСПДн и определения необходимого уровня защищенности персональных данных.

2.2.2 Базовый набор мер по обеспечению безопасности персональных данных установлен Приказом ФСТЭК России от 18.02.2014 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности

персональных данных при их обработке в информационных системах персональных данных».

2.2.3 В качестве начального выбирается один из четырех базовых наборов мер по обеспечению безопасности персональных данных, соответствующий установленному уровню защищенности.

2.2.4 Пример выбора базового набора мер по обеспечению безопасности персональных данных (идентификации и аутентификации субъектов доступа и объектов) для 1 уровня защищенности приведен в таблице 6.

Таблица 6 – Базовый набор мер идентификации и аутентификации субъектов доступа и объектов доступа для 1 уровня защищенности персональных данных

Индекс меры	Наименование меры
Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)	
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации
ИАФ.5	Защита обратной связи при вводе аутентификационной информации
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)

2.3 Адаптация базового набора мер по обеспечению безопасности персональных данных

2.3.1 По результатам рассмотрения структурно-функциональных характеристик информационной системы персональных данных, применяемых информационных технологий и особенностей функционирования информационной системы персональных данных вносятся изменения в базовый набор мер по обеспечению безопасности персональных данных. Пример внесенных изменений с указанием обоснования приведен в таблице 6.

Таблица 6 – Изменение базового набора мер по результатам его адаптации

Индекс меры	Наименование меры	Изменение (добавлена/ исключена)	Обоснование
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	исключена	В ИСПДн Общества не предоставляется доступ внешних пользователей

Индекс меры	Наименование меры	Изменение (добавлена/ исключена)	Обоснование
УПД.14	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	исключена	В ИСПДн Общества не предоставляется удаленный доступ через внешние информационно-телекоммуникационные сети

2.4 Уточнение адаптированного базового набора мер по обеспечению безопасности персональных данных

2.4.1 По результатам рассмотрения актуальных угроз безопасности персональных данных вносятся изменения в адаптированный базовый набор мер по обеспечению безопасности персональных данных. Пример внесенных изменений с указанием обоснования приведен в таблице 7.

Таблица 7 – Изменения базового набора мер по результатам его адаптации

Индекс меры	Наименование меры	Изменение (добавлена/ исключена)	Обоснование
ЗНИ.7	Контроль подключения машинных носителей информации	добавлена	В ИСПДн Общества актуальны угрозы разглашения ПДн, в том числе несанкционированное копирование на съемные носители

2.5 Дополнение уточненного адаптированного базового набора мер по обеспечению безопасности персональных данных

2.5.1 По результатам рассмотрения требований к защите персональных данных, установленными иными нормативными правовыми актами в области обеспечения безопасности персональных данных и защиты информации вносятся изменения в уточненный адаптированный базовый набор мер по обеспечению безопасности персональных данных.

2.6 Результаты определения состава и содержания мер по обеспечению безопасности персональных данных

2.6.1 Результаты определения состава и содержания мер по обеспечению безопасности персональных данных, подлежащих реализации в ИСПДн Общества, приводятся в сводной таблице. Пример результатов определения состава и содержания мер по обеспечению безопасности персональных данных приведен в Таблице 8.

Таблица 8 – Результаты определения состава и содержания мер по обеспечению безопасности персональных данных

Индекс меры	Наименование меры	Вывод о необходимости реализации	Обоснование	Реализуется техническими мерами	Реализуется организационными мерами
ЗНИ.1	Учет машинных носителей персональных данных	Требуется	Мера содержится в базовом наборе	-	+
ЗНИ.2	Управление доступом к машинным носителям персональных данных	Требуется	Мера содержится в базовом наборе	-	+
ЗНИ.6	Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации	Требуется	Мера содержится в базовом наборе	+	+
ЗНИ.7	Контроль подключения машинных носителей информации	Требуется	Дополнение уточненного адаптированного базового набора	+	+