РЕГЛАМЕНТ
выделения информационных систем персональных данных и определения необходимого уровня защищенности персональных данных в ООО «Сатурн»

Москва 2018

Содержание

1 Информация о документе

1.1 Назначение документа

1.1.1 Настоящий Регламент выделения информационных систем персональных данных и определение необходимого уровня защищенности персональных данных в ООО «Сатурн» (далее – Регламент) определяет порядок выделения информационных систем персональных данных и порядок определения необходимого уровня защищенности персональных данных в ООО «Сатурн» (далее – Общество).

1.2 Цель принятия документа

1.2.1 Настоящий Регламент принят в целях обеспечения соответствия требованиям постановления Правительства РФ от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.3 Область применения документа

1.3.1 Настоящий документ обязаны знать и использовать в работе члены Комиссии по обеспечению безопасности персональных данных.

1.4 Вводимые сокращения и термины

Таблица 1 — Перечень сокращений

Сокращение	Расшифровка сокращения
ИС	информационная система
ИСПДн	информационная система персональных данных
НДВ	недокументированные (недекларированные) возможности
ПДн	персональные данные
УЗ	уровень 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

Термин	Определение термина
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
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. № 162-ФЗ (ред. от 24.07.2014) «О персональных данных»
2	Постановление Правительства РФ от 16 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

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
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, 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 Общества.

2 Порядок выделения информационных систем персональных данных

2.1 Выявление информационных систем, в которых осуществляется обработка персональных данных

2.1.1 Выявление информационных систем, в которых осуществляется обработка персональные данных, проводит Комиссия по обеспечению безопасности персональных данных путем анализа бизнес-процессов Общества.

2.1.2 Для каждой информационной системы, в которой осуществляется обработка персональных данных, необходимо определить:

– цели обработки персональных данных (назначение ИС);

– категории субъектов персональных данных, обрабатываемых в ИС (работники, клиенты и т.п.)

– объем обрабатываемых персональных данных;

– тип информационной системы;

– тип актуальных угроз безопасности персональных данных (предварительный);

– требуемый уровень защищенности персональных данных (предварительный).

2.2 Выделение информационных систем персональных данных

2.2.1 После выявления информационных систем, в которых осуществляется обработка персональных данных, Комиссия принимает решение о выделении информационных систем персональных данных.

2.2.2 В одну ИСПДн может быть включена одна или несколько информационных систем, в которых осуществляется обработка ПДн.

2.2.3 В целях оптимизации процессов управления системой защиты персональных данных возможно объединение однотипных информационных систем в состав одной ИСПДн. Основанием для объединения может являться: обработка одних и тех же категорий субъектов персональных данных, схожие цели обработки, общий круг пользователей системы и т.д.

2.2.4 Для каждой выделенной ИСПДн должна быть разработана Модель угроз и нарушителя безопасности персональных данных в соответствии с разделом 3.1, а также определен необходимый уровень защищенности персональных данных в соответствии с разделом 3.3

2.2.5 По результатом выделения ИСПДн формируется документ «Перечень информационных систем персональных данных», содержащий сведения обо всех ИСПДн Общества.

2.2.6 В Обществе должна проводиться периодическая проверка процессов обработки персональных данных на предмет выявления новых ИСПДн.

3 Определение необходимого уровня защищенности персональных данных (классификация ИСПДн)

3.1 Разработка модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных

3.1.1 Разработка модели угроз безопасности персональных данных при их обработке в ИСПДн проводится в целях определения актуальных угроз безопасности, в том числе угроз, связанных с наличием НДВ, и их последующей нейтрализации.

3.1.2 Модель угроз должна быть разработана для каждой ИСПДн Общества, при этом допускается разработка общей модели угроз для нескольких однотипных ИСПДн.

3.1.3 Разработка модели угроз включает следующие этапы:

– определение актуальных категорий нарушителей;

– оценку возможностей актуальных категорий нарушителей;

– перечень типовых актуальных угроз для ИСПДн;

– оценку актуальности угроз безопасности персональных данных, в том числе угроз, связанных с наличием НДВ в системном и прикладном программном обеспечении ИСПДн;

– определение необходимого уровня криптографической защиты персональных данных.

3.2 Методика определения необходимого уровня защищенности персональных данных

3.2.1 Определение необходимого уровня защищенности производится исходя из следующих параметров ИСПДн:

– тип ИСПДн;

– категории субъектов персональных данных, обрабатываемых в ИСПДн;

– тип актуальных угроз безопасности персональных данных;

– объем обрабатываемых персональных данных.

3.2.2 Тип ИСПДн определяется исходя из категорий персональных данных, обрабатываемых в системе. Выделяются следующие типы ИСПДн:

– специальные ИСПДн (в ИСПДн обрабатываются персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных);

– биометрические ИСПДн (в ИСПДн обрабатываются сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются Обществом для установления личности субъекта персональных данных, и не обрабатываются сведения, относящиеся к специальным категориям персональных данных);

– общедоступные ИСПДн (в ИСПДн обрабатываются персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей 8 Федерального закона «О персональных данных»);

– иные ИСПДн.

3.2.3 Выделяются следующие типы категории субъектов персональных данных, обрабатываемых в ИСПДн:

– в ИСПДн обрабатываются персональные данные сотрудников Общества;

– в ИСПДн обрабатываются персональные данные субъектов, не являющихся сотрудниками Общества;

– в ИСПДн обрабатываются персональные данные сотрудников и субъектов, не являющихся сотрудниками Общества.

3.2.4 Тип актуальных угроз безопасности персональных данных определяется согласно Модели угроз соответствующей ИСПДн. Выделяются следующие типы угроз безопасности:

– угрозы, связанные с наличием НДВ в системном программном обеспечении ИСПДн (угрозы 1-го типа);

– угрозы, связанные с наличием НДВ в прикладном программном обеспечении ИСПДн (угрозы 2-го типа);

– угрозы, не связанные с наличием НДВ в системном и прикладном программном обеспечении (угрозы 4-го типа).

3.2.5 Выделяются следующие значения объема персональных данных, обрабатываемых в ИСПДн:

– менее 100 000 субъектов;

– более 100 000 субъектов.

3.2.6 Таблица сопоставления параметров ИСПДн необходимым уровням защищенности персональных данных приведена в Приложении № 1.

3.3 Порядок определения необходимого уровня защищённости персональных данных (порядок классификации ИСПДн)

3.3.1 Определение необходимого уровня защищенности персональных данных (классификацию ИСПДн) осуществляет Комиссия по обеспечению безопасности персональных данных согласно методике, указанной в разделе 4.2.

3.3.2 По результатам определения необходимого уровня защищенности персональных данных для каждой ИСПДн оформляется Акт классификации. типовая форма Акта классификации ИСПДн приведена в Приложении № 2.

3.3.3 На основании утвержденных актов классификации в документе «Перечень информационных систем персональных данных» указывается необходимый уровень защищенности персональных данных.

Приложение № 1. Таблица для определения уровня защищенности персональных данных

Объем обрабатываемых данных	Тип информационной системы	Категория субъектов персональных данных	Тип актуальных угроз безопасности персональных данных	УЗ
более 100 000	Специальная	Сотрудников	Угрозы 1-го типа	1
			Угрозы 2-го типа	2
			Угрозы 3-го типа	3
		Не сотрудников	Угрозы 1-го типа	1
			Угрозы 2-го типа	1
			Угрозы 3-го типа	2
	Биометрическая	Сотрудников и не сотрудников	Угрозы 1-го типа	1
			Угрозы 2-го типа	2
			Угрозы 3-го типа	3
	Иная	Сотрудников	Угрозы 1-го типа	1
			Угрозы 2-го типа	3
			Угрозы 3-го типа	3
		Не сотрудников	Угрозы 1-го типа	1
			Угрозы 2-го типа	2
			Угрозы 3-го типа	3
	Общедоступная	Сотрудников	Угрозы 1-го типа	2
			Угрозы 2-го типа	3
			Угрозы 3-го типа	3
		Не сотрудников	Угрозы 1-го типа	2
			Угрозы 2-го типа	2
			Угрозы 3-го типа	3
менее 100 000	Специальная	Сотрудников и не сотрудников	Угрозы 1-го типа	1
			Угрозы 2-го типа	2
			Угрозы 3-го типа	3
	Биометрическая	Сотрудников и не сотрудников	Угрозы 1-го типа	1
			Угрозы 2-го типа	2
			Угрозы 3-го типа	3
	Иная	Сотрудников и не сотрудников	Угрозы 1-го типа	1
			Угрозы 2-го типа	3
			Угрозы 3-го типа	3
	Общедоступная	Сотрудников и не сотрудников	Угрозы 1-го типа	2
			Угрозы 2-го типа	3
			Угрозы 3-го типа	3

Приложение № 2. Типовая форма акта классификации ИСПДн

УТВЕРЖДАЮ
Должность
ООО «Сатурн»

_____ / *И.О. Фамилия* /
«___» _____ 20__ г

АКТ №___
классификации ИСПДн «*Наименование системы*»
ООО «Сатурн»
(Проект)

1 Настоящий Акт составлен Комиссией по обеспечению безопасности персональных данных *ООО «Сатурн»*, назначенной приказом от «___» _____ 20__ г. № ___ в составе:

Члены комиссии: *И.О. Фамилия, должность*
И.О. Фамилия, должность
И.О. Фамилия, должность

с целью определения необходимого уровня защищенности персональных данных при их обработке в информационной системе персональных данных *«Наименование системы».*

2 При определении необходимого уровня защищенности персональных данных Комиссия руководствовалась следующими документами:

– Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Регламент выделения информационных систем персональных данных и определения необходимого уровня защищенности персональных данных в ООО «Сатурн», утвержден {*кем*} «___» _____ 20__ г.;

– Модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных «*Наименование системы*», утверждена {*кем*} «___» _____ 20__ г.

3 Исходные данные, представленные Комиссии для определения необходимого уровня защищенности персональных данных, при их обработке в ИСПДн «*Наименование системы*», приведены в таблице 1.

Таблица 1 — Исходные данные для определения необходимого уровня защищенности

Наименование исходных данных	**Описание**
Актуальность угроз, связанных с наличием недокументированных (недекларированных) возможностей в системном и (или) прикладном программном обеспечении, используемом в информационной системе	для системы актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе (угрозы 1-го типа)
	для системы актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе (угрозы 2-го типа)
	для системы актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе (угрозы 4-го типа)
Тип информационной системы	в системе обрабатываются персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных (специальные категории персональных данных)
	в системе обрабатываются биометрические персональные данные
	в системе обрабатываются персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных (общедоступные персональные данные)
	в системе не обрабатываются биометрические и общедоступные персональные данные, а также специальные категории персональных данных (обрабатываются иные персональные данные)
Категории субъектов персональных данных	в системе обрабатываются персональные данные сотрудников Общества
	в системе обрабатываются персональные данные сотрудников Общества и субъектов, не являющихся сотрудниками Общества
	в системе обрабатываются персональные данные субъектов, не являющихся сотрудниками Общества
Объем обрабатываемых персональных данных	в системе обрабатываются данные более чем 100 000 субъектов
	в системе обрабатываются данные менее чем 100 000 субъектов

4 На основании рассмотренных исходных данных и документов, указанных в п. 2, Комиссия установила необходимость обеспечения для персональных данных при их обработке в ИСПДн «*Наименование системы*» {*N-го*} уровня защищенности.

Члены комиссии: _____ */ И.О. Фамилия /*

_____ */ И.О. Фамилия /*