РЕГЛАМЕНТ
проведения периодических проверок в области обработки и обеспечения безопасности персональных данных в ООО «Сатурн»

Москва 2018

Содержание

1 Информация о документе

1.1 Назначение документа

1.1.1 Настоящий Регламент проведения периодических проверок в области обработки и обеспечения безопасности персональных данных в ООО «Сатурн» (далее – Регламент) определяет порядок разработки плана проверок и проведения проверок в ООО «Сатурн» (далее – Сатурн).

1.2 Цель принятия документа

1.2.1 Настоящий Регламент принят в целях выполнения требований Федерального закона «О персональных данных».

1.3 Область применения документа

1.3.1 Настоящий документ обязан знать и использовать члены Комиссии по обеспечению безопасности персональных данных.

1.4 Внешние нормативные и распорядительные документы

Таблица 1 — 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»
4	Постановление Правительства РФ от 16 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»
4	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»

1.5 Внутренние нормативные и распорядительные документы

Таблица 2 — Внутренние нормативные и распорядительные документы

№ п/п	Наименование документа
1	Положение об обеспечении безопасности персональных данных
2	Положение об организации обработки персональных данных
3	Публичная политика обработки персональных данных
4	Регламент взаимодействия с субъектами персональных данных
5	Регламент предоставления доступа к персональным данным

№ п/п	Наименование документа
6	Регламент обработки персональных данных без использования средств автоматизации
7	Регламент обращения с машинными носителями персональных данных
8	Регламент доступа в помещения, в которых ведется обработка персональных данных
9	Перечень персональных данных, обрабатываемых в ООО «Сатурн»
10	Перечень структурных подразделений и должностей, допущенных к обработке персональных данных
11	Перечень мест хранения бумажных носителей персональных данных

1.6 Пересмотр документа

1.6.1 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 проведения проверок

2.1 Порядок формирования плана внутренних проверок

2.1.1 План внутренних проверок порядка обработки и обеспечения безопасности персональных данных формируется Комиссией по обеспечению безопасности персональных данных на следующий календарный год.

2.1.2 Перечень и описание проверок, которые должны быть включены в план, приведен в разделе 4.

2.1.3 Типовая форма плана внутренних проверок приведена в Приложении № 1.

2.2 Порядок оповещения работников о проведении проверки

2.2.1 Работники Общества должны быть оповещены о проведении проверки не позднее, чем за 4 рабочих дня до ее начала.

2.3 Отчет о результатах проверки

2.3.1 По результатам проведения внутренних проверок Комиссия по обеспечению безопасности персональных данных разрабатывает и представляет руководству Общества ежегодный отчет.

3 Перечень проводимых проверок

3.1 Проверка соблюдения принципов обработки персональных данных

В ходе проверки соблюдения принципов обработки персональных данных осуществляются следующие мероприятия:

– проверка актуальности документа «Перечень персональных данных, обрабатываемых в ООО «Сатурн»;

– проверка процессов обработки персональных данных на предмет обработки избыточных персональных данных, а также на предмет превышения установленных сроков хранения персональных данных.

3.2 Проверка соблюдения регламента предоставления допуска к обработке персональных данных

В ходе проверки соблюдения регламента предоставления допуска к обработке персональных данных осуществляются следующие мероприятия:

– проверка актуальности документа «Перечень структурных подразделений и должностей, допущенных к обработке персональных данных»;

– проверка наличия заполненных листов ознакомления работников с организационно-распорядительными документами в области обработки и обеспечения безопасности персональных данных;

– проверка наличия подписанных обязательств о неразглашении персональных данных;

– проверка ведения журнала инструктажей по правилам обработки и обеспечения безопасности персональных данных;

– проверка наличия заявок на предоставление (изменение/прекращение) доступа к информационным системам персональных данных;

– проверка соответствия прав доступа пользователей в информационных системах персональных данных ранее поданным заявкам на предоставление доступа.

3.3 Проверка соблюдения регламента взаимодействия с субъектами персональных данных

В ходе проверки соблюдения регламента взаимодействия с субъектами персональных данных осуществляются следующие мероприятия:

– проверка наличия письменных согласий субъектов персональных данных;

– проверка соответствия письменной формы согласия актуальным процессам обработки персональных данных;

– проверка факта размещения публичной политики обработки персональных данных в открытом доступе;

– проверка ведения журнала учета обращений субъектов;

–проверка осведомленности работников о порядке взаимодействия с субъектами персональных данных, в том числе о правах субъектов персональных данных.

3.4 Проверка порядка обращения с машинными носителями персональных данных

В ходе проверки порядка обращения с машинными носителями персональных данных осуществляются следующие мероприятия:

– проверка ведения Журнала учета съемных носителей;

– проверка условий хранения съемных носителей, выданных работникам;

– проверка ведения электронного журнала учета несъемных машинных носителей;

– проверка порядка уничтожения машинных носителей персональных данных, в т.ч. наличие актов уничтожения;

– проверка осведомленности работников о порядке использования съемных машинных носителей персональных данных.

3.5 Проверка соблюдения регламента неавтоматизированной обработки персональных данных

В ходе проверки соблюдения регламента неавтоматизированной обработки персональных данных осуществляются следующие мероприятия:

– проверка актуальности документа «Перечень мест хранения бумажных носителей персональных данных»;

– проверка сохранности бумажных носителей персональных данных;

– проверка осведомленности работников о порядке неавтоматизированной обработки персональных данных.

3.6 Проверка условий эксплуатации средств криптографической защиты информации

В ходе проверки условий эксплуатации средств криптографической защиты информации осуществляются следующие мероприятия:

– проверка оснащения серверных помещений техническими устройствами, сигнализирующими о несанкционированном вскрытии (либо проверка опечатывания серверных помещений);

– проверка актуальности утвержденного перечня лиц, имеющих право доступа в серверные помещения.

Приложение № 1. Типовая форма плана внутренних проверок

ПЛАН
внутренних проверок порядка обработки и обеспечения безопасности персональных данных

Сроки проведения	Наименование мероприятия	Ответственный за проведение
с 01.02.2018 по 10.02.2018	Проверка соблюдения принципов обработки персональных данных	*{Фамилия И.О.}*
с 01.02.2018 по 10.02.2018	Проверка соблюдения порядка предоставления допуска к обработке персональных данных	*{Фамилия И.О.}*
с 01.02.2018 по 10.02.2018	Проверка соблюдения регламента взаимодействия с субъектами персональных данных	*{Фамилия И.О.}*
с 01.04.2018 по 10.04.2018	Проверка порядка обращения с машинными носителями персональных данных	*{Фамилия И.О.}*
с 01.04.2018 по 10.04.2018	Проверка соблюдения регламента неавтоматизированной обработки персональных данных	*{Фамилия И.О.}*
с 01.09.2018 по 10.09.2018	Проверка условий эксплуатации средств криптографической защиты информации	*{Фамилия И.О.}*
с 01.12.2018 по 10.12.2018	Подготовка ежегодного отчета по результатам внутренних проверок порядка обработки и обеспечения безопасности персональных данных	*{Фамилия И.О.}*