АДМИНИСТРАЦИЯ ГОРОДСКОГО ОКРУГА ШАТУРА МОСКОВСКОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ

07.07.2021 № 1367

О создании комиссии по защите информации

Во исполнение Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных, Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»,

ПОСТАНОВЛЯЮ:

1. Создать комиссию по защите информации при администрации Городского округа Шатура.
2. Утвердить положение о комиссии по защите информации согласно Приложению № 1 к настоящему постановлению.
3. Утвердить типовую форму Протокола заседания комиссии по защите информации согласно Приложению № 2 к настоящему постановлению.
4. Утвердить типовую форму Акта определения уровня защищенности персональных данных при их обработке в информационной системе персональных данных и класса защищенности информационной системы согласно Приложению № 3 к настоящему постановлению.
5. Утвердить типовую форму Акта по результатам приемочных испытаний вновь вводимого сегмента на соответствие типовому сегменту согласно Приложению № 4 к настоящему постановлению.
6. Управлению делами администрации Городского округа Шатура (Трубачева И.В.) обеспечить размещение настоящего постановления на официальном сайте Городского округа Шатура.
7. Контроль за выполнением настоящего постановления возложить на заместителя главы администрации Городского округа Давыдова В.Ю.

Администрация Городского округа Шатура Московской области

Глава Городского округа А.В. Артюхин

Приложение №1
к постановлению администрации
Городского округа Шатура
Московской области
от «07» 07 2021 г. № 1367

ПОЛОЖЕНИЕ
о комиссии по защите информации

1. Общие положения

1.1. Настоящее Положение определяет основные задачи, порядок формирования, полномочия и ответственность комиссии по защите информации (далее - Комиссия).

2. Основные задачи Комиссии

2.1. Основными задачами комиссии являются:

2.1.1. Сбор и анализ исходных данных по информационным системам персональных данных администрации Городского округа Шатура (далее - Администрация).

2.1.2. Определение значений параметров для проведения классификации информационных систем в соответствии с Приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

2.1.3. Определение значений параметров для установления уровня защищенности персональных данных в соответствии с постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

2.1.4. Определение класса защищенности информационных систем персональных данных Администрации на основании собранных данных.

2.1.5. Определение уровня защищенности персональных данных при их обработке в информационных системах персональных данных.

2.1.6. Определение соответствия автоматизированных рабочих мест сотрудников, подключаемых к государственным информационным системам Московской области (далее – ГИС МО) требованиям по обеспечению информационной безопасности согласно Техническим требованиям для

защищенного подключения рабочих мест соответствующих типовых сегментов к ГИС МО.

3. Порядок формирования Комиссии

3.1. Комиссия формируется из числа штатных сотрудников администрации Городского округа Шатура и подведомственных учреждений, участвующих в процессе обработки информации.

3.2. В состав Комиссии входит не менее четырех человек – членов Комиссии, в их числе – председатель Комиссии.

3.3. Члены комиссии назначаются распорядительным актом администрации Городского округа Шатура.

3.4. В случае изменения состава Комиссии, в распорядительный акт вносятся соответствующие изменения.

4. Полномочия Комиссии

4.1. Для осуществления задач, указанных в разделе 2 настоящего Положения, Комиссия имеет право:

4.1.1. Получать необходимые сведения у всех работников Администрации, участвующих в обработке персональных данных.

4.1.2. Просматривать электронные базы данных и бумажные носители, содержащие персональные данные, с целью выявления состава обрабатываемых персональных данных.

4.1.3. Отслеживать технологический процесс обработки персональных данных.

4.1.4. Выявлять или получать готовые сведения о структуре локальной вычислительной сети Администрации.

4.1.5. Определять или получать готовые сведения о наличии и способах доступа к сетям общего пользования.

4.1.6. Определять или получать готовые сведения о технических и программных средствах обработки данных.

4.1.7. Определять или получать готовые сведения об условиях, местах и способах передачи данных в сторонние организации.

4.1.8. Получать необходимую информацию у администратора корпоративной сети.

5. Отчетность Комиссии

5.1. Комиссия при выполнении своих задач должна составить протокол заседания комиссии.

5.2. В результате своей деятельности Комиссия должна составить Акт(ы) определения уровня защищенности персональных данных, класса защищенности информационных систем персональных данных, а также акты соответствия автоматизированных рабочих мест, подключаемых к ГИС МО, требованиям по обеспечению информационной безопасности.

Приложение №2
к постановлению администрации
Городского округа Шатура
Московской области
от «07» 07 2021 г. № 1367

ПРОТОКОЛ № __
заседания комиссии по защите информации

Дата и время проведения _____
Место проведения _____

Председатель комиссии _____ ФИО
Члены комиссии _____ ФИО
_____ ФИО
_____ ФИО

Повестка дня

Определение информационных систем персональных данных (далее - ИСПДн), принадлежащих_____.
(Наименование организации)

1. Слушали: _____
доложил(а) исходные данные об ИСПДн «Наименование».

Выступил(а): _____
предложил(а) утвердить акт определения уровня защищенности персональных данных и класса защищённости ИСПДн «Наименование».

Постановили:

Утвердить акт определения уровня защищенности персональных данных и класса защищённости ИС «Наименование».

2. Слушали: _____
доложил(а) исходные данные об ИСПДн «Наименование».

Выступил(а): _____
предложил(а) утвердить акт определения уровня защищенности персональных данных и класса защищённости ИСПДн «Наименование».

Постановили:

Утвердить акт определения уровня защищенности персональных данных и класса защищённости ИС «Наименование».

Председатель комиссии	_____	ФИО
Члены комиссии	_____	ФИО
	_____	ФИО
	_____	ФИО

Приложение №3
к постановлению администрации
Городского округа Шатура
Московской области
от «07» 07 2021 г. № 1367

АКТ
определения уровня защищенности ПДн при их обработке в ИСПДн «Наименование» и класса защищенности ИС «Наименование»

Председатель комиссии _____ ФИО
Члены комиссии _____ ФИО
_____ ФИО
_____ ФИО

Рассмотрев исходные данные об информационной системе персональных данных (далее - ИСПДн), комиссия определила:

– Категории персональных данных обрабатываемых в ИСПДн: в информационной системе обрабатываются _____ категории персональных данных;

– Категории субъектов: персональные данные субъектов персональных данных, не являющихся сотрудниками оператора;

– Объем обрабатываемых персональных данных: менее _____;

– Тип актуальных угроз: для информационной системы актуальны угрозы _____ типа;

– Уровень значимости информации: информация имеет _____ уровень значимости _____;

– Масштаб информационной системы: информационная система имеет _____масштаб.

Комиссия решила, в соответствии с Постановлением Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а так же в соответствии с приказом ФСТЭК Российской Федерации от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и на основании анализа исходных данных, необходимо обеспечить _____ уровень защищенности (___) персональных данных и установить _____ класс защищенности информационной системы (__).

Результат оценки вреда:

Для информационной системы актуальны угрозы 3-го типа.

Уровень значимости информации определен степенью возможного ущерба для обладателя информации от нарушения конфиденциальности (неправомерные доступ, копирование, предоставление или распространение), целостности (неправомерные уничтожение или модифицирование) или доступности (неправомерное блокирование) информации, руководствуясь следующей формулой:

УЗ = [(конфиденциальность, степень ущерба) (целостность, степень ущерба) (доступность, степень ущерба)], где степень возможного ущерба определяется обладателем информации.

Комиссия утвердила следующее:

УЗ = [(конфиденциальность, _____ степень ущерба) (целостность, _____ степень ущерба) (доступность, _____ степень ущерба)] – таким образом, комиссия установила _____ уровень значимости (___) (возможны незначительные негативные последствия).

Председатель комиссии	_____	ФИО
Члены комиссии	_____	ФИО
	_____	ФИО
	_____	ФИО

«__»_____20__ г.

Приложение №4
к постановлению администрации
Городского округа Шатура
Московской области
от «07» 07 2021 г. № 1367

АКТ
по результатам приемочных испытаний
вновь вводимого сегмента
«Наименование сегмента»
на соответствие типовому сегменту «Наименование типового сегмента»

Председатель комиссии _____ ФИО
Члены комиссии _____ ФИО
_____ ФИО
_____ ФИО

Комиссия провела оценку соответствия вновь вводимого сегмента «Наименование сегмента», расположенному по адресу:_____, типовому сегменту «Наименование сегмента», прошедшему аттестационные испытания.

КОМИССИЯ УСТАНОВИЛА:

Основываясь на документально подтверждённых сведениях, что для вновь вводимого сегмента «Наименование сегмента»:

- в соответствии с актом классификации установлен ____класс защищенности – «__», соответствующий классу защищенности типового сегмента «Наименование типового сегмента», прошедшего аттестационные испытания;
- перечень угроз безопасности информации, актуальных для вновь вводимого сегмента, соответствует перечню угроз безопасности информации типового сегмента «Наименование типового сегмента», прошедшего аттестационные испытания;
- в соответствии с техническим паспортом вновь вводимого сегмента состав технических средств, программного обеспечения и средств защиты информации идентичен составу типового сегмента «Наименование типового сегмента», прошедшего аттестационные испытания;
- для вновь вводимого сегмента имеется наличии необходимая организационно- распорядительная документация и эксплуатационная документация на систему защиты информации, соответствующая документации типового сегмента «Наименование типового сегмента», прошедшего аттестационные испытания.

Руководствуясь «Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (утверждены приказом ФСТЭК России от 11.02.2013 № 17),

КОМИССИЯ РЕШИЛА:

1. Признать вновь вводимый сегмент «Наименование сегмента» соответствующим типовому сегменту 2.6.3 «АРМ пользователя информационной системы», указанной информационной системы, прошедшему аттестационные испытания.

2. Признать возможным распространение действия аттестата соответствия ГИС МО «Наименование ГИС» от _____ г. № _____требованиям безопасности информации на вновь вводимый сегмент.

Председатель комиссии	_____	ФИО
Члены комиссии	_____	ФИО
	_____	ФИО
	_____	ФИО

«__»_____20__ г.