

План внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных на 2017 год администрации города Котовска принят во исполнение требований статей 18.1, 19, 22.1. Федерального закона –ФЗ 152 «О персональных данных»

ОБЩИЕ ПОЛОЖЕНИЯ

План внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных на 2017 год содержит перечень внутренних проверок, сроки их исполнения и исполнителей.

План распространяется на все информационные системы персональных данных администрации города Котовска.

Мероприятие 1	Периодичность 2	Исполнитель 3
КОНТРОЛЬ СОБЛЮДЕНИЯ ОРГАНИЗАЦИОННО-РЕЖИМНЫХ ТРЕБОВАНИЙ В ПОМЕЩЕНИЯХ, В КОТОРЫХ ОСУЩЕСТВЛЯЕТСЯ ОБРАБОТКА ПДн		
1	2	3
Проверка актуальности перечня должностных лиц, имеющих право самостоятельного доступа в помещения, где обрабатываются или хранятся ПДн	ежегодно / после каждого изменения штатного расписания	комиссия по персональным данным / ответственный за обработку ПДн
Соблюдение порядка доступа в помещения, где расположены элементы информационных систем персональных данных	ежеквартально	руководители подразделений администратор ИСПДн комиссия по персональным данным
Доступ в помещения, где обрабатываются и хранятся бумажные носители с персональными данными	ежеквартально	руководители подразделений ответственный за обработку ПДн комиссия по персональным данным
Наличие жалюзи на окнах	ежегодно	администратор ИСПДн комиссия по персональным данным

Установка дополнительных запирающих устройств на места хранения документов с ПДн	по необходимости	ответственный за обработку ПДн
Проверка исполнения режима доступа в серверное помещение	ежеквартально	администратор ИСПДн

КОНТРОЛЬ ДОСТУПА К ПРИЛОЖЕНИЯМ ИНФОРМАЦИОННЫХ СИСТЕМ, В КОТОРЫХ ОСУЩЕСТВЛЯЕТСЯ ОБРАБОТКА ПДн

1	2	3
Контроль фактов подачи заявок на блокирование доступа к ИСПДн увольняемых работников и своевременность подачи таких заявок	ежеквартально	администратор ИСПДн комиссия по персональным данным
Контроль использования предоставленных прав доступа (в том числе и право удаленного доступа)	ежеквартально	администратор ИСПДн комиссия по персональным данным
Соответствие используемых пользователями ИСПДн полномочий параметрам (матрице) доступа	ежегодно	администратор ИСПДн комиссия по персональным данным

КОНТРОЛЬ ПОРЯДКА ОБРАЩЕНИЯ С НОСИТЕЛЯМИ ПДн

1	2	3
Проверка корректности ведения журнала учета машинных носителей и соответствия записей в журнале записям в автоматизированной системе контроля съемных магнитных носителей информации	ежеквартально	администратор ИСПДн комиссия по персональным данным
Проверка наличия съемных носителей ПДн и соблюдения пользователями ИСПДн правил работы с ними	ежегодно	администратор ИСПДн комиссия по персональным данным
Своевременность проведения мероприятий по уничтожению персональных данных	ежеквартально	руководители подразделений ответственный за обработку ПДн комиссия по персональным данным администратор ИСПДн

Контроль отсутствия конфиденциальных документов, содержащих ПДн, без присмотра на рабочих столах работников	ежемесячно	руководители подразделений ответственный за обработку ПДн комиссия по персональным данным
---	------------	---

ПРОВЕРКА ВЫПОЛНЕНИЯ ЗАПРОСОВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ

1	2	3
Проверка своевременности исполнения запросов субъектов персональных данных	ежемесячно	ответственный за обработку ПДн комиссия по персональным данным
Контроль актуальности ведения журнала учета обращений субъектов ПДн по вопросам обработки их ПДн	ежемесячно	ответственный за обработку ПДн комиссия по персональным данным
Наличие необходимых согласий субъектов персональных данных, чьи ПДн обрабатываются в ИСПДн	раз в полгода	ответственный за обработку ПДн комиссия по персональным данным

КОНТРОЛЬ ВЫЯВЛЕНИЯ И НЕЙТРАЛИЗАЦИИ НАРУШЕНИЙ РЕЖИМА ОБРАБОТКИ ПДн

1	2	3
Проверка корректности ведения базы данных инцидентов информационной безопасности	ежеквартально	администратор ИСПДн уполномоченные работники информационно-технического отдела
Актуальность заполнения отчетов об инцидентах и их нейтрализации	ежемесячно	администратор ИСПДн
Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн	раз в полгода	ответственный за обработку ПДн комиссия по персональным данным
Проверка фиксации неудачных попыток входа в систему в системном журнале	ежеквартально	администратор ИСПДн администратор ИСПДн уполномоченные работники информационно-технического отдела

Выборочная проверка АРМ пользователей на предмет наличия возможных вредоносных программ и запрещенных информационных ресурсов	ежеквартально	администратор ИСПДн уполномоченные работники информационно- технического отдела
---	---------------	--

КОНТРОЛЬ СОБЛЮДЕНИЯ ТРЕБОВАНИЙ РЕЖИМА ОБРАБОТКИ ПДн

1	2	3
Соблюдение порядка работы со средствами защиты информации	ежегодно	комиссия по персональным данным администратор ИСПДн
Соблюдение пользователями ИСПДн требований антивирусной защиты	ежеквартально	администратор ИСПДн комиссия по персональным данным
Соблюдение порядка резервирования баз данных, иной защищаемой информации и хранения резервных копий	ежегодно	администратор ИСПДн комиссия по персональным данным
Контроль за внесением изменений в программное обеспечение, за обновлениями программного обеспечения и единообразия применяемого ПО на всех элементах ИСПДн	ежегодно	руководители подразделений администратор ИСПДн комиссия по персональным данным
Соблюдение режима защиты при подключении к сетям общего пользования и (или) международного обмена	ежеквартально	руководители подразделений администратор ИСПДн комиссия по персональным данным
Подготовка предложений по приобретению и установке новых лицензионных программных продуктов	ежегодно	администратор ИСПДн уполномоченные работники информационно-технического отдела
Проверка корректности расположения мониторов АРМ, исключая несанкционированный просмотр экранов	ежегодно	руководители подразделений администратор ИСПДн комиссия по персональным данным
Контроль сохранности пломб на технических средствах передачи и обработки ПДн, а также на устройствах их защиты	ежеквартально	администратор ИСПДн уполномоченные работники информационно-технического отдела

КОНТРОЛЬ СОБЛЮДЕНИЯ ПОЛЬЗОВАТЕЛЯМИ ИСПДн ПАРОЛЬНОЙ ПОЛИТИКИ

1	2	3
Проверка сроков действия паролей	ежегодно	администратор ИСПДн комиссия по персональным данным
Проверка пользовательских паролей на количество символов и очевидность с целью выявления слабых паролей	ежеквартально	администратор ИСПДн комиссия по персональным данным

АНАЛИЗ И ПЕРЕСМОТР ИМЕЮЩИХСЯ УГРОЗ БЕЗОПАСНОСТИ ПДн

1	2	3
Анализ и пересмотр имеющихся угроз безопасности ПДн, а так же предсказание появления новых, еще неизвестных, угроз	ежегодно	комиссия по персональным данным администратор ИСПДн
Корректировка Частных моделей угроз безопасности ПДн при их обработке в ИСПДн	ежегодно	комиссия по персональным данным администратор ИСПДн
Моделирование (при необходимости) новых моделей угроз безопасности ПДн в соответствии с действующими нормативными правовыми актами и методическими документами ФСТЭК и ФСБ России	ежегодно	комиссия по персональным данным администратор ИСПДн

ПРОВЕРКА КОРРЕКТНОСТИ КЛАССИФИКАЦИИ ИСПДн

1	2	3
Проверка правильности определения категорий обрабатываемых в ИСПДн ПДн	ежегодно	комиссия по персональным данным администратор ИСПДн
Корректировка объема обрабатываемых ПДн (количество субъектов ПДн, ПДн которых обрабатываются в ИСПДн)	ежегодно	комиссия по персональным данным администратор ИСПДн
Уточнение структуры ИСПДн	ежегодно	администратор ИСПДн комиссия по персональным

		данным
Анализ режимов обработки ПДн и разграничения прав доступа пользователей ИСПДн	ежегодно	администратор ИСПДн комиссия по персональным данным
Уточнение местонахождения технических средств ИСПДн	по необходимости	администратор ИСПДн комиссия по персональным данным
Проведение повторной классификации ИСПДн (в случае обнаружения изменений исходных данных об ИСПДн по сравнению с отраженными в акте классификации данной ИСПДн)	по необходимости	администратор ИСПДн комиссия по персональным данным
Проверка правильности осуществления сбора, систематизации, записи, накопления, хранения, уточнения (обновления, изменения), извлечения, использования, передачи (распространения, предоставления, доступа), обезличивания, блокирования, удаления, уничтожения ПДн в каждой из ИСПДн	ежегодно	администратор ИСПДн комиссия по персональным данным
Актуализация информации о законности целей обработки ПДн и оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения требований по обработке и обеспечению безопасности ПДн	ежегодно	комиссия по персональным данным ответственный за обработку ПДн администратор ИСПДн

ПОДДЕРЖАНИЕ В АКТУАЛЬНОМ СОСТОЯНИИ НОРМАТИВНО-ОРГАНИЗАЦИОННЫХ ДОКУМЕНТОВ ПО ВОПРОСАМ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПДн

1	2	3
Актуализация локальных нормативных актов по вопросам обеспечения безопасности ПДн	ежегодно / после каждого изменения законодательных и иных нормативных правовых актов по защите ПДн и отраслевых стандартов / по результатам проверки	комиссия по персональным данным ответственный за обработку ПДн администратор ИСПДн

	регуляторами по результатам расследований выявленных инцидентов информационной безопасности	
Проверка актуальности сведений, содержащихся в уведомлении Роскомнадзора об обработке (о намерении осуществлять обработку) персональных данных	ежегодно	администратор ИСПДн ответственный за обработку ПДн комиссия по персональным данным

ОБУЧЕНИЕ И ПРОВЕРКА РАБОТНИКОВ ПО ВОПРОСАМ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПДн

1	2	3
Контроль ознакомления вновь принимаемых работников с локальными нормативными актами, регламентирующими обработку ПДн	ежеквартально	ответственный за обработку ПДн комиссия по персональным данным
Проверка знания пользователями ИСПДн о своих действиях во внештатных ситуациях	один раз в полгода	ответственный за обработку ПДн комиссия по персональным данным
Проверка знаний и соблюдения работниками положений действующего законодательства Российской Федерации в области ПДн и локальных актов Общества	ежегодно	комиссия по персональным данным ответственный за обработку ПДн администратор ИСПДн
Обучение руководителей и работников в области обработки и защиты ПДн	ежегодно	комиссия по персональным данным ответственный за обработку ПДн