Приложение № 15
к приказу руководителя комитета
физической культуры и спорта
администрации города Ставрополя
от «28» 12 2018 г. № 265-ОД

ИНСТРУКЦИЯ

по порядку проведения проверок состояния защиты персональных данных комитета физической культуры и спорта администрации города Ставрополя

г. Ставрополь
2018 г.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий документ определяет порядок проведения проверок состояния защиты персональных данных (ПДн) комитета физической культуры и спорта администрации города Ставрополя (далее – Комитет).

1.2. Проведение проверок состояния защиты ПДн осуществляется в целях выявления нарушений требований нормативной документации, установление причин нарушений, разработка плана корректирующих действий направленных на устранение и предотвращение нарушений.

1.3. Проверки осуществляются администратором информационной безопасности (ИБ) информационных систем персональных данных (ИСПДн), ответственным за обеспечение безопасности ПДн, а также руководителями отделов Управления в непосредственно подчиненных им отделов.

1.4. Должностные лица Комитета знакомятся с основными положениями и приложениями Инструкции в части, их касающейся, по мере необходимости.

2. ПОРЯДОК ПРОВЕДЕНИЯ ВНУТРЕНИХ ПРОВЕРОК

2.1. При проведении внутренней проверки производиться:
- проверка соблюдения требований по обработке и защите персональных данных;
- проверка соблюдения условий использования средств защиты ПДн, предусмотренных эксплуатационной и технической документацией;
- проверка эффективности средств защиты ПДн.

2.2. Приказом назначается рабочая группа (комиссия) по проведению проверок состояния защиты ПДн.

2.3. Внутренние проверки проводятся в соответствии с планом внутренних проверок состояния защиты ПДн (далее - План). План формируется в конце текущего года на последующий. Форма Плана представлена в Приложении 1.

2.4. План составляется администратором информационной безопасности (ИБ) ИСПДн Комитета в соответствии с положениями данной Инструкции.

2.5. План должен содержать перечень мероприятий по проверке, перечень проверяемых подразделений и сроки проведения проверок, составленные с учетом требований руководителей отделов, ответственного за обеспечение безопасности ПДн и администратора ИБ ИСПДн.

2.6. Внеплановые проверки могут проводиться в случаях получения жалоб, выявления нарушений системы защиты и подготовки к контролю со стороны уполномоченных федеральных органов, регулирующих деятельность в сфере обработки персональных данных.

2.7. На основании утвержденного Плана внутренних проверок администратором ИБ ИСПДн составляет приказ о проведении проверки деятельности отдела Комитета. Приказ издается не позднее, чем за десять дней до даты проверки.

2.8. В ходе работы в проверяемых отделах должна быть получена объективная и полная информация по состоянию защиты ПДн.

2.9. Проверяющие имеют право, осматривать помещения, где производится обработка ПДн, получать доступ к техническим средствам, участвующим в обработке ПДн, просматривать настройки СЗИ, а также проводить беседы и консультации с работниками отделов.

2.10. При проведении проверок в общем случае должно проверяться:

- наличие установленных средств защиты информации;
- корректность настроек средств защиты информации;
- выполнение пользователями и администраторами требований инструктивных материалов по защите ПДн;
- исполнение требований к процедурам обработки ПДн (уничтожению ПДн, сбору согласий, допуску персонала к ПДн и т.п.);
- правильность организации работы с носителями ПДн;
- соответствие системы защиты ПДн реальному положению дел в Комитете и т.п.

Для проверки эффективности системы защиты персональных данных должны использоваться средства выявления уязвимостей информационной безопасности.

2.11. По результатам проверок составляется акт о результатах внутренней проверки (Приложение 2), выявленных недостатков и нарушений, предложений по их устранению. Руководитель проверяемого отдела должен быть поставлен в известность о выявленных несоответствиях в течение трех дней после проведенной проверки.

3. КОРРЕКТИРУЮЩИЕ МЕРОПРИЯТИЯ И КОНТРОЛЬ ЗА ИХ ИСПОЛНЕНИЕМ

3.1. Руководитель проверяемого отдела анализирует акт о результатах внутренней проверки и в трехдневный срок определяет перечень мероприятий, необходимых для устранения нарушений и их причин.

3.2. Если корректирующие мероприятия касаются других отделов, то к анализу привлекаются специалисты соответствующих подразделений.

3.3. Выполнение корректирующих мероприятий и их достаточность определяется ответственным за обеспечение безопасности ПДн и администратором ИБ ИСПДн.

3.4. Внутренняя проверка считается оконченной после выполнения всех корректирующих мероприятий и устранения выявленных нарушений.

4. ПОРЯДОК ПЕРЕСМОТРА ИНСТРУКЦИИ

4.1. Полный плановый пересмотр данного документа также проводится регулярно, раз в год, с целью проверки соответствия положений данного документа реальным условиям применения их в ИСПДн Комитета.

4.2. Частичный пересмотр данного документа проводится по письменному предложению администратора ИБ ИСПДн. Форма регистрации изменений в Инструкцию представлена в Приложении 3.

4.3. Вносимые изменения не должны противоречить другим положениям Инструкции.

5. ОТВЕТСТВЕННЫЕ ЗА ВЫПОЛНЕНИЕ ИНСТРУКЦИИ

Ответственным за выполнения требований данной Инструкции является:

- администратор ИБ ИСПДн в части задач, возложенных на него настоящей инструкцией.
- ответственный за обеспечение безопасности ПДн в части общего контроля информационной безопасности.

УТВЕРЖДАЮ

Руководитель комитета

_____ А.Е. Середа

«29» декабря 2017 г.

План внутренних проверок состояния защиты персональных данных на 2018 год

№ п/п	Наименование мероприятия	Наименование отдела	Период проведения проверки	Отметка о выполнении (№ акта проверки)	Отметка о выполнении корректирующих мероприятий	Примечание
1	Правильность обработки персональных данных информационных систем	Общий отдел	01.08.2018			
2	Правильность обработки персональных данных информационных систем	Отдел по физической культуре и спорту	02.08.2018			

ПРИЛОЖЕНИЕ 2 ФОРМА АКТА ВНУТРЕННЕЙ ПРОВЕРКИ

АКТ

о результатах внутренней проверки _____
наименование структурного подразделения

№_____ от _____

1. Цель проверки_____
2. Основание: _____
3. Время проведения проверки_____
4. Результаты проверки_____

   _____

   _____

   _____
5. Рекомендации по устранению нарушений_____

   _____

   _____

   _____

Члены рабочей группы:

_____

_____

_____

Лист ознакомления с «Инструкцией по порядку проведения проверок состояния защиты персональных данных комитета физической культуры и спорта администрации города Ставрополя»

№ п/п	Фамилия И.О. сотрудника	Дата ознакомления	Расписка сотрудника в ознакомлении