


УТВЕРЖДАЮ
Директор ОАУСО «Холмский КЦ»
 С. А. Сафонова
«09» декабря 2016 г.



ИНСТРУКЦИЯ
по порядку проведения проверок состояния защиты персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящий документ определяет порядок проведения проверок состояния защиты персональных данных (ПДн) в ОАУСО «Холмский КЦ».

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.

Проверки осуществляются администратором информационной безопасности (далее - АИБ) информационных систем персональных данных (далее - ИСПДн), ответственным за обеспечение безопасности и обработку ПДн (далее – Ответственный), а также руководителями структурных подразделений в непосредственно подчиненных им отделах.

Должностные лица ОАУСО «Холмский КЦ», знакомятся с основными положениями и приложениями Инструкции в части, их касающейся, по мере необходимости.

2. ПОРЯДОК ПРОВЕДЕНИЯ ВНУТРЕННИХ ПРОВЕРОК

При проведении внутренней проверки производится:

- проверка соблюдения требований по обработке и защите ПДн;
- проверка соблюдения условий использования средств защиты ПДн, предусмотренных эксплуатационной и технической документацией;
- проверка эффективности средств защиты ПДн.

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

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.

План составляется АИБ ИСПДн ОАУСО «Холмский КЦ» в соответствии с положениями данной Инструкции.

План должен содержать перечень мероприятий по проверке, перечень проверяемых отделов и сроки проведения проверок, составленные с учетом требований начальников отделов, ответственного за обеспечение безопасности и обработки ПДн и АИБ ИСПДн.

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 ПДн.

На основании утвержденного плана внутренних проверок АИБ ИСПДн составляет приказ о проведении проверки деятельности подразделений ОАУСО «Холмский КЦ». Приказ издается не позднее, чем за десять дней до даты проверки.

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

Проверяющие имеют право, осматривать помещения, где производится обработка ПДн, получать доступ к техническим средствам, участвующим в обработке ПДн, просматривать эксплуатацию средств защиты информации, а также проводить беседы и консультации с работниками подразделений ОАУСО «Холмский КЦ», требовать предоставления письменных объяснений, справок, отчетов по вопросам, относящимся к предмету проверки. 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;
- выполнение 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 ОАУСО «Холмский КЦ».

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

По результатам проверок составляется акт о результатах внутренней проверки (Приложение 2), выявленных недостатках и нарушениях, предложений по их устранению.

Руководитель проверяемого структурного подразделения должен быть поставлен в известность о выявленных несоответствиях в течение трех дней после проведенной проверки.

Корректирующие мероприятия и контроль за их исполнением

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

Если корректирующие мероприятия касаются других структурных подразделений ОАУСО «Холмский КЦ», то к анализу привлекаются специалисты соответствующих подразделений.

Выполнение корректирующих мероприятий и их достаточность определяется ответственным за обеспечение безопасности и обработки ПДн и АИБ ИСПДн.

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

Порядок пересмотра инструкции

Полный плановый пересмотр данного документа также проводится регулярно, раз в год, с целью проверки соответствия положений данного документа реальным условиям применения их в ИСПДн ОАУСО «Холмский КЦ».

Частичный пересмотр данного документа проводится по письменному предложению АИБ ИСПДн. Форма регистрации изменений в Инструкции представлена в Приложении 3.

Вносимые изменения не должны противоречить другим положениям Инструкции.

Ответственные за выполнение инструкции

Ответственным за выполнения требований данной Инструкции является:

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

Форма акта внутренней проверки

АКТ № _____ от _____

о результатах внутренней проверки _____

_____ (наименование структурного подразделения)

1. Цель проверки:

2. Основание:

3. Время проведения проверки:

4. Результаты проверки:

5. Рекомендации по устранению нарушений:

Председатель комиссии (рабочей группы):

_____/_____

Члены комиссии (рабочей группы):

_____/_____

_____/_____

_____/_____

УТВЕРЖДАЮ
Директор ОАУСО «Холмский КЦ»
А. Сафонова
«09» декабря 2016 г.



**Областное автономное учреждение социального обслуживания
«Холмский комплексный центр социального обслуживания населения»**

**ЖУРНАЛ
по экземплярного учета средств защиты персональных данных, эксплуатационной и
технической документации к ним**

На _____ листах

Начат «__» _____ 2016 г.

Окончен «__» _____ 20__ г.

