Приложение № 3
к приказу директора
от 01.06.2015 № 1160

ПРАВИЛА ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ СООТВЕТСТВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕБОВАНИЯМ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ОБУ «ЦСЗН ЛИПЕЦКОЙ ОБЛАСТИ»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее - Правила) в областном бюджетном учреждении «Центр социальной защиты населения Липецкой области» (далее - Учреждение), определяют процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных (далее - ПДн); основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки ПДн, необходимой для предоставления государственных и муниципальных услуг, требованиям к защите ПДн.

1.2. Настоящие Правила разработаны на основании Федерального закона РФ от 27.07.2006 № 152-ФЗ «О персональных данных», Федерального закона РФ от 27.07.2010 №210-ФЗ «Об организации предоставления государственных и муниципальных услуг» и в соответствии с частью 1 «Перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», утвержденных постановлением Правительства РФ от 2.03.2012 №211.

1.3. Для обработки ПДн, необходимых для предоставления государственных и муниципальных услуг Учреждением используется информационная система персональных данных (далее - ИСПДн) «Адресная социальная помощь»», предназначенная для осуществления деятельности Учреждения, согласно федеральному и областному законодательству.

1.4. Для обработки ПДн сотрудников, необходимых для обеспечения кадровой и бухгалтерской деятельности в Учреждении в соответствии с Трудовым кодексом Российской Федерации, используется ИСПДн «1С: Бухгалтерия и кадры».

1.5. Пользователем ИСПДн (далее - Пользователь) является сотрудник Учреждения, участвующий в рамках выполнения своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ к аппаратным средствам, ПО, данным и средствам защиты информации (далее - СЗИ) ИСПДн.

1.6. Контрольные мероприятия за обеспечением уровня защищенности персональных данных и соблюдений условий использования средств защиты информации, а также соблюдением требований законодательства Российской Федерации по обработке персональных данных в ИСПДн Учреждения проводятся в следующих целях:

- проверка выполнения требований организационно-распорядительной документации по защите информации в Учреждении и действующего законодательства Российской Федерации в области обработки и защиты персональных данных;
- оценка уровня осведомленности и знаний работников Учреждения в области обработки и защиты персональных данных;
- оценка обоснованности и эффективности применяемых мер и средств защиты.

2. ТЕМАТИКА ВНУТРЕННЕГО КОНТРОЛЯ

Тематика внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн:

2.1. Проверки соответствия обработки ПДн установленным требованиям в Учреждении разделяются на следующие виды:

- регулярные;
- плановые;
- внеплановые.

2.2. Регулярные контрольные мероприятия проводятся администратором безопасности ИСПДн (далее - администратор АИС) периодически в соответствии с утвержденным Планом проведения контрольных мероприятий (далее - План, приложение № 1) и предназначены для осуществления контроля выполнения требований в области защиты информации в Учреждении.

2.3. Плановые контрольные мероприятия проводятся постоянной комиссией периодически в соответствии с утвержденным Планом проведения контрольных мероприятий и направлены на постоянное совершенствование системы защиты персональных данных ИСПДн Учреждения.

2.4. Внеплановые контрольные мероприятия проводятся на основании решения комиссии по информационной безопасности (создается на период проведения мероприятий). Решение о проведении внеплановых контрольных мероприятий и созданию комиссии по информационной безопасности может быть принято в следующих случаях:

- по результатам расследования инцидента информационной безопасности; - по результатам внешних контрольных мероприятий, проводимых регулирующими органами;
- по решению руководителя Учреждения.

3. ПЛАНИРОВАНИЕ КОНТРОЛЬНЫХ МЕРОПРИЯТИЙ

3.1. Для проведения плановых внутренних контрольных мероприятий лицо, ответственное за обеспечение безопасности персональных данных, разрабатывает План внутренних контрольных мероприятий на текущий год.

3.2. План проведения внутренних контрольных мероприятий включает следующие сведения по каждому из мероприятий:

- цели проведения контрольных мероприятий;
- задачи проведения контрольных мероприятий;
- объекты контроля (процессы, подразделения, информационные системы т.п.);
- состав участников, привлекаемых для проведения контрольных мероприятий;
- сроки и этапы проведения контрольных мероприятий.

3.3. Общий срок контрольных мероприятий не должен превышать пяти рабочих дней. При необходимости срок проведения контрольных мероприятий может быть продлен, но не более чем на десять рабочих дней, соответствующие изменения отображаются в отчете, выполняемом по результатам проведенных контрольных мероприятий.

4. ОФОРМЛЕНИЕ РЕЗУЛЬТАТОВ КОНТРОЛЬНЫХ МЕРОПРИЯТИЙ

4.1 По итогам проведения регулярных контрольных мероприятий результаты проверок фиксируется в Журнале учета событий информационной безопасности.

4.2. По итогам проведения плановых и внеплановых контрольных мероприятий лицо, комиссия, разрабатывает отчет, в котором указывается:

- описание проведенных мероприятий по каждому из этапов;
- перечень и описание выявленных нарушений;
- рекомендации по устранению выявленных нарушений;

- заключение по итогам проведения внутреннего контрольного мероприятия.

4.3. Отчет передается на рассмотрение руководству Учреждения.

4.4. Общая информация о проведенном контрольном мероприятии фиксируется в Журнале учета событий информационной безопасности.

4.5. Результаты проведения мероприятий по внеплановому контролю заносятся в протокол проведения внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных Учреждения (приложение № 2).

5. ПОРЯДОК ПРОВЕДЕНИЯ ПЛАНОВЫХ И ВНЕПЛАНОВЫХ КОНТРОЛЬНЫХ МЕРОПРИЯТИЙ

5.1. Плановые и внеплановые контрольные мероприятия проводятся при обязательном участии лица, ответственного за обеспечение безопасности ПДн ИСПДн, также по его ходатайству к проведению контрольных мероприятий могут привлекаться администраторы АИС и ответственный за обеспечение безопасности ПДн, обрабатываемых без использования средств автоматизации, Учреждения.

5.2. Лицо, ответственное за обеспечение безопасности ПДн ИСПДн, не позднее, чем за три рабочих дня до начала проведения контрольных мероприятий уведомляет всех руководителей подразделений, в которых планируется проведение контрольных мероприятий, и направляет им для ознакомления План проведения контрольных мероприятий. При проведении внеплановых контрольных мероприятий уведомление не требуется.

5.3. Во время проведения контрольных мероприятий, в зависимости от целей мероприятий, могут выполняться следующие проверки:

- соответствие полномочий пользователя правилам доступа;
- соблюдение пользователями требований инструкций по организации антивирусной и парольной политики, инструкции по обеспечению безопасности ПДн;
- соблюдение администраторами АИС инструкций и регламентов по обеспечению безопасности информации в Учреждении;
- соблюдение Порядка доступа в помещения Учреждения, где ведется обработка персональных данных;
- знание пользователями положений Инструкции пользователя по обеспечению безопасности обработки ПДн при возникновении нештатных ситуаций;
- порядок и условия применения средств защиты информации;
- состояние учета машинных носителей персональных данных;
- наличие (отсутствие) фактов несанкционированного доступа к ПДн и принятие необходимых мер;
- проведенные мероприятия по восстановлению ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- технические мероприятия, связанные со штатным и нештатным функционированием средств защиты;
- технические мероприятия, связанные со штатным и нештатным функционированием подсистем системы защиты информации.

Приложение № 1
к Правилам осуществления внутреннего контроля
соответствия обработки персональных данных
требованиям к защите персональных данных

ПЛАН
внутренних проверок контроля соответствия обработки персональных данных требованиям к защите персональных данных

Мероприятие	Периодичность регулярных мероприятий	Периодичность плановых мероприятий	Исполнитель
Контроль соблюдения правил доступа к ПДн	Еженедельно	Ежемесячно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных
Контроль соблюдения режима защиты	Еженедельно	Ежемесячно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных
Контроль выполнения антивирусной политики	Еженедельно	Ежемесячно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных
Контроль выполнения парольной политики	Еженедельно	Ежемесячно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных
Контроль соблюдения режима защиты при подключении к сетям общего пользования и (или) международного обмена	Еженедельно	Ежемесячно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных
Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн		Ежемесячно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных
Контроль обновления ПО и единообразия применяемого ПО на всех элементах АИС	Еженедельно	Ежемесячно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных
Контроль обеспечения резервного копирования		Ежемесячно	Ответственный за обеспечение безопасности персональных данных информационных систем персо-

			нальных данных _____
Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а также предсказание появления новых, еще неизвестных, угроз		Ежегодно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных _____
Поддержание в актуальном состоянии нормативно-организационных документов		Ежемесячно	Ответственный за организацию обработки ПДн **Антонова А.Г.**
Контроль запрета на использование беспроводных соединений	Еженедельно	Ежемесячно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных _____