Приложение №4

К приказу директора №841 от 30.12.2016г.

ПРАВИЛА

осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в ОБУСО «КЦСОН Суджанского района»

1. Общие положения

1.1. Настоящие правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее – Правила) в ОБУСО «КЦСОН Суджанского района»

(далее – Учреждение), определяют процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных (далее – ПД); основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки ПД, необходимой для предоставления государственных услуг, требованиям к защите ПД.

1.2. Настоящие Правила разработаны на основании Федерального закона РФ от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Федерального закона РФ от 27 июля 2010 г. № 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 21 марта 2012 г. № 211.

1.3. Для обработки ПД, необходимых для предоставления государственных услуг Учреждения, используется информационная система персональных данных (далее – ИСПД)Учреждения (клиенская база), предназначенная для осуществления деятельности Учреждения.

1.4. Для обработки ПД сотрудников, необходимых для обеспечения кадровой и бухгалтерской деятельности в Учреждении в соответствии с Трудовым кодексом Российской Федерации, используется ИСПД «Кадры бюджетного учреждения» и ИСПД « Учет клиентов центра социального обслуживания», АСП.

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

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 ИСПД Учреждения проводятся в следующих целях:

КОПИЯ ВЕРНА
СПЕЦИАЛИСТ ПО КАДРАМ
ПОДПИСЬ НЕСМАЧНАЯ Е.В

1.6.1 проверка выполнения требований организационно-распорядительной документации по защите информации в Учреждении и действующего законодательства Российской Федерации в области обработки и защиты персональных данных;

1.6.2 оценка уровня осведомленности и знаний работников Учреждения в области обработки и защиты персональных данных;

1.6.3 оценка обоснованности и эффективности применяемых мер и средств защиты.

2. Тематика внутреннего контроля

Тематика внутреннего контроля соответствия обработки ПД требованиям к защите ПД:

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

- регулярные;
- плановые;
- внеплановые.

2.2. Регулярные контрольные мероприятия проводятся Администратором АСП 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 (далее – План, приложение 1) и направлены на постоянное совершенствование системы защиты персональных данных ИСПД _____.

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:

2.4.1 по результатам расследования инцидента информационной безопасности;

2.4.2 по результатам внешних контрольных мероприятий, проводимых регулирующими органами;

2.4.3 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:

КОПИЯ ВЕРНА
СПЕЦИАЛИСТ ПО КАДРАМ
ПОДПИСЬ ЕСМАЧНАЯ Е.В

3.2.1 цели проведения контрольных мероприятий;

3.2.2 задачи проведения контрольных мероприятий,

3.2.3 объекты контроля (процессы, подразделения, информационные системы и т.п.);

3.2.4 состав участников, привлекаемых для проведения контрольных мероприятий;

3.2.5 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:

4.2.1 описание проведенных мероприятий по каждому из этапов;

4.2.2 перечень и описание выявленных нарушений;

4.2.3 рекомендации по устранению выявленных нарушений;

4.2.4 заключение по итогам проведения внутреннего контрольного мероприятия.

4.3. отчет передается на рассмотрение руководству Учреждения.

4.4. Общая информации о проведенном контрольном мероприятий фиксируется в Журнале учета событий информационной безопасности.

5. Порядок проведения плановых и внеплановых контрольных мероприятий

5.1. Плановые и внеплановые контрольные мероприятия проводятся при обязательном участии лица, ответственному за обеспечение безопасности ПД, также по его ходатайству к проведению контрольных мероприятий могут привлекаться администраторы АСП, и ответственный за обеспечение безопасности персональных данных информационных систем персональных данных Учреждения.

5.2. Лицо, ответственное за обеспечение безопасности ПД, 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.

КОПИЯ ВЕРНА
СПЕЦИАЛИСТ ПО КАДРАМ
ПОДПИСЬ НЕСМАЧНАЯ Е.В

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

- Соответствие полномочий Пользователя правилам доступа.

- Соблюдение Пользователями требований инструкций по организации антивирусной и парольной политики, инструкции по обеспечению безопасности ПД.

- Соблюдение Администраторами инструкций и регламентов по обеспечению безопасности информации в Учреждении.

- Знание Пользователей положений Инструкции пользователя по обеспечению безопасности обработки ПД при возникновении внештатных ситуаций.

- Знание Администраторами инструкций и регламентов по обеспечению безопасности информации в Учреждении.

- Порядок и условия применения средств защиты информации.

- Состояние учета машинных носителей персональных данных.

- Наличие (отсутствие) фактов несанкционированного доступа к ПД и принятие необходимых мер.

- Проведенные мероприятия по восстановлению ПД, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

- Технические мероприятия, связанные с штатным и нештатным функционированием средств защиты.

- Технические мероприятия, связанные с штатным и нештатным функционированием подсистем системы защиты информации.

КОПИЯ ВЕРНА
СПЕЦИАЛИСТ ПО КАДРАМ
ПОДПИСЬ НЕСМАЧНАЯ Е.В

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 ПД	Ежемесячно	1 раз в квартал	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных _Программист_
Контроль соблюдения режима защиты	Ежемесячно	1 раз в квартал	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных Программист_
Контроль выполнения антивирусной политики	Ежемесячно	1 раз в квартал	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных Программист
Контроль выполнения парольной политики	Ежемесячно	1 раз в квартал	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных Программист
Контроль соблюдения режима защиты при подключении к сетям общего пользования и (или) международного обмена	Ежемесячно	1 раз в квартал	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных Программист
Проведение внутренних	Ежемесячно	1 раз в квартал	Ответственный за

КОПИЯ ВЕРНА
СПЕЦИАЛИСТ ПО КАДРАМ
ПОДПИСЬ НЕСМАЧНАЯ Е.В

проверок на предмет выявления изменений в режиме обработки и защиты ПД			обеспечение безопасности персональных данных информационных систем персональных данных Программист
Контроль обновления ПО и единообразия применяемого ПО на всех элементах	Ежемесячно	1 раз в квартал	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных Программист
Контроль обеспечения резервного копирования	Еженедельно	Ежемесячно	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных Программист
Организация анализа и пересмотра имеющихся угроз безопасности ПД, а также предсказание появления новых, еще неизвестных, угроз	Ежемесячно	1 раз в квартал	Ответственный за обеспечение безопасности персональных данных информационных систем персональных данных Программист
Поддержание в актуальном состоянии нормативно-организационных документов	Ежемесячно	1 раз в квартал	Ответственный за организацию обработки ПД в Программист

КОПИЯ ВЕРНА
СПЕЦИАЛИСТ ПО КАДРАМ
ПОДПИСЬ ЕСМАЧНАЯ Е.В