Государственное профессиональное образовательное учреждение
Тульской области «Алексинский химико-технологический техникум»

СОГЛАСОВАНО
на Совете техникума
протокол № от 15.02.2022г.

УТВЕРЖДАЮ
Директор ГПОУ ТО «АХТТ»
Приказ № от 15.02.2022г.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП

Сертификат: 00 bd 35 07 6f f6 ed 19 23
Владелец: Анохина Ольга Николаевна
Действителен с 22.03.2022 по 21.03.2027

ПРАВИЛА

осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в ГПОУ ТО «Алексинский химико-технологический техникум»

Общие положения

1.1. Настоящие правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее – Правила) в ГПОУ ТО «Алексинский химико-технологический техникум» (далее – ГПОУ ТО «АХТТ»), определяют процедуры, направленные на соблюдение или выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных (далее – ПДн); основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки ПДн, требованиям к защите ПДн.

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

1.3. 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 информационной системе ПДн (ИСПДн) ГПОУ ТО «АХТТ» проводятся в следующих целях:

1.3.1. проверка выполнения требований организационно-распорядительной документации по защите информации в ГПОУ ТО «АХТТ» и действующего законодательства Российской Федерации в области обработки и защиты персональных данных;

1.3.2. оценка уровня осведомленности и знаний работников ГПОУ ТО «АХТТ» в области обработки и защиты персональных данных;

1.3.3. 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 ГПОУ ТО «АХТТ» разделяются на следующие виды:

- регулярные;
- плановые;
- внеплановые.

2.2. Регулярные внутренние контрольные мероприятия проводятся периодически в соответствии с утвержденным Планом внутреннего контроля условий обработки персональных данных (далее – План) и предназначены для осуществления контроля выполнения требований в области защиты информации в ГПОУ ТО «АХТТ».

2.3. Плановые внутренние контрольные мероприятия проводятся периодически в соответствии с утвержденным Планом и направлены на постоянное совершенствование системы защиты персональных данных ИСПДн и на бумажных носителях в ГПОУ ТО «АХТТ».

2.4. Внеплановые внутренние 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 директора ГПОУ ТО «АХТТ».

3. Планирование внутренних контрольных мероприятий

3.1. Для проведения регулярных, 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:

3.2.1. тема мероприятий;

3.2.2. сроки проведения контрольных мероприятий;

3.2.3. состав участников, привлекаемых для проведения контрольных мероприятий (исполнители).

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 журнале, заполняемом по результатам проведенных контрольных мероприятий.

4. Оформление результатов контрольных мероприятий

4.1. По итогам проведения контрольных мероприятий результаты проверок фиксируются в Журнале учета мероприятий внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее - Журнал).

В Журнале отмечаются мероприятия в соответствии с Планом, носящие регулярный и плановый характер.

В Журнал заносится следующая информация:

- название проведенного мероприятия;
- дата проведенного мероприятия;
- исполнитель мероприятия;
- результат (отчет, действия) мероприятия (при необходимости).

4.2. По итогам проведения плановых и внеплановых контрольных мероприятий, в случае выявления нарушений ответственное лицо за организацию обработки ПДн/ комиссия, составляет Акт (приложение), в котором указывается:

- описание проведенных мероприятий;
- перечень и описание выявленных нарушений;
- рекомендации по устранению выявленных нарушений;
- заключение по итогам проведения внутреннего контрольного мероприятия.
- акт передается директору ГПОУ ТО «АХТТ» для ознакомления.

5. Порядок проведения плановых и внеплановых контрольных мероприятий

5.1. В отношении персональных данных, ставших известными лицу, ответственному за организацию обработки персональных данных, или членам комиссии в ходе проведения внутреннего контроля, соблюдается конфиденциальность и обеспечивается безопасность при их обработке.

5.2. Регулярные, плановые и внеплановые контрольные мероприятия проводятся при обязательном участии лица, ответственного за обеспечение безопасности ПДн, также к проведению контрольных мероприятий могут привлекаться сотрудники, ответственные за осуществление обработки персональных данных в рамках своих функциональных обязанностей.

5.3. Лицо, ответственное за организацию обработки ПДн, не позднее, чем за три рабочих дня до начала проведения контрольных мероприятий уведомляет всех руководителей подразделений, в которых планируется проведение контрольных мероприятий. При проведении внеплановых контрольных мероприятий уведомление не требуется.

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

- Соответствие полномочий Пользователя правилам доступа.
- Соответствие сбора ПДн целям обработки ПДн.
- Соблюдение Пользователями требований инструкций по организации антивирусной и парольной политики, инструкции по обеспечению безопасности ПДн.
- Соблюдение сотрудниками инструкций и регламентов по обеспечению безопасности информации в ГПОУ ТО «АХТТ».
- Выполнение требований безопасности ПДн исполняются и удовлетворяют поставленным целям
- Знание Пользователей положений Инструкции пользователя информационных систем.
- 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 с штатным и нештатным функционированием средств защиты.

Приложение
к Правилам осуществления внутреннего контроля соответствия
обработки персональных данных требованиям к
защите персональных данных в ГПОУ ТО «АХТТ»

УТВЕРЖДАЮ
Директор ГПОУ ТО «АХТТ»
_____ О.Н.Анохина
«_____» _____20___ г.

АКТ
проведения внутренних контрольных мероприятий по соблюдению условий обработки персональных данных в ГПОУ ТО «АХТТ»

Настоящий АКТ составлен в том, что «_____» _____20__ г. ответственным за организацию обработки персональных данных/ комиссией по внутреннему контролю в составе:

проведена проверка_____.
(тема проверки)

Проверка осуществлялась в соответствии с требованиями
_____
_____.
(название документа)

В ходе проверки проверено:
_____
_____.

Выявленные нарушения:
_____
_____.

Меры по устранению нарушений:
_____
_____.

Срок устранения нарушений: _____.

_____ _____
(Ф.И.О.) (подпись)

Члены комиссии:

_____ _____
(Ф.И.О.) (подпись)

_____ _____
(Ф.И.О.) (подпись)

_____ _____
(Ф.И.О.) (подпись)

«_____» _____ 20_____ г.