Приложение 3

к приказу от 29.12.2018 № 474

«Об утверждении полного

пакета документов,

регламентирующих обработку

персональных данных»

**Правила**

**осуществления внутреннего контроля соответствия обработки персональных данных в информационной системе персональных данных Государственного областного бюджетного профессионального образовательного учреждения «Елецкий колледж экономики, промышленности и отраслевых технологий»**

**Общие положения**

Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее - Правила) в информационной системе персональных данных Государственного областного бюджетного профессионального образовательного учреждения «Елецкий колледж экономики, промышленности и отраслевых технологий» (далее Учреждение) разработаны в соответствии с законодательством Российской Федерации и законодательством Липецкой области и определяют порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

1. **Тематика внутреннего контроля.**

1.1. Тематика проверок обработки персональных данных с использованием средств автоматизации:

а) соответствие полномочий пользователя матрице доступа;

б) соблюдение пользователями информационной системы персональных данных (далее ИСПДн) Учреждения требований инструкции по организации парольной защиты в информационных системах персональных данных Учреждения;

в) соблюдение пользователями ИСПДн требований инструкции по организации антивирусной защиты в информационных системах персональных данных Учреждения;

г) соблюдение порядка доступа в помещения Учреждения, в которых ведется обработка персональных данных работников;

д) знание пользователями ИСПДн порядка своих действий во внештатных ситуациях.

1.2. Тематика проверок обработки персональных данных без использования средств автоматизации:

а) соблюдение правил хранения бумажных носителей с персональными данными;

б) соблюдение порядка доступа к бумажным носителям с персональными данными;

в) соблюдение порядка доступа в помещения, где обрабатываются и хранятся бумажные носители с персональными данными.

1. **Порядок проведения внутренних проверок.**

2.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям в Учреждении организуется проведение периодических проверок условий обработки персональных данных в соответствии с планом проверок (Приложение 1 к Правилам).

2.2. Проверки осуществляются комиссией, создаваемой приказом директора Учреждения.

2.3. Внутренние проверки проводятся по необходимости, в соответствии с поручением директора Учреждения, но не реже одного раза в год.

2.4. Внутренние проверки осуществляются непосредственно на месте обработки персональных данных путем опроса, либо, при необходимости, путем осмотра рабочих мест работников, участвующих в процессе обработки персональных данных.

2.5. По результатам каждой проверки составляется Акт проведения внутренней проверки (Приложение 2 к Правилам).

2.6. При выявлении в ходе проверки нарушений председателем комиссии в акте делается запись о мероприятиях по устранению нарушений и сроках исполнения.

2.7. Акты хранятся у Ответственного в течение текущего года. Уничтожение актов проводится Ответственным самостоятельно в первом квартале года, следующего за отчетным.

2.8. О результатах проверки и мерах, необходимых для устранения нарушений, директору Учреждения докладывает председатель комиссии.

Приложение 1

к Правилам осуществления внутреннего контроля соответствия обработки персональных данных в информационной системе персональных даных требованиям к защите персональных данных

УТВЕРЖДАЮ:

Директор ГОБПОУ «Елецкий колледж

экономики, промышленности и

отраслевых технологий»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Р.Ю.Евсеев

Приказ от 29 декабря 2018 г № 474

**План**

**внутренних проверок условий обработки персональных данных**

**Государственного областного бюджетного профессионального образовательного учреждения «Елецкий колледж экономики, промышленности и отраслевых технологий»**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Тема проверки | Нормативный документ, предъявляющий требования | Срок проведения | Исполнитель |
|  | Соответствие полномочий пользователя требованиям к защите персональных данных | Перечень ИСПД;  Перечень должностей сотрудников Центра;  Порядок доступа сотрудников Центра в помещения, в которых ведется обработка персональных данных;  Правила обработки персональных данных. | 1 раз в год | Провоторова С.В.  Алексеев А.И. |
|  | Соблюдение пользователями ИСПД парольной политики | Политика информационной безопасности | 1 раз в год | Алексеев А.И. |
|  | Соблюдение пользователями ИСПД антивирусной политики | Политика информационной безопасности | 1 раз в год | Алексеев А.И. |
|  | Соблюдение пользователями ИСПД правил работы со съемными носителями персональных данных | Политика информационной безопасности | 1 раз в год | Алексеев А.И. |
|  | Соблюдение пользователями правил работы с криптографическими средствами защиты информации | Политика информационной безопасности | 1 раз в год | Черепников К.А.  Алексеев А.И. |
|  | Соблюдение порядка доступа в помещения, где расположены элементы ИСПД | Порядок доступа служащих в помещения, где ведется обработка персональных данных | 1 раз в год | Алексеев А.И. |
|  | Соблюдение порядка резервирования баз данных и хранения резервных копий | Политика информационной безопасности | 1 раз в год | Алексеев А.И. |
|  | Соблюдение порядка работы со средствами защиты информации | Политика информационной безопасности | 1 раз в год | Алексеев А.И. |
|  | Знание пользователями ИСПД своих действий во внештатных ситуациях | Политика информационной безопасности | 1 раз в год | Алексеев А.И. |
|  | Хранение бумажных носителей с персональными данными | Законодательство Российской Федерации | 1 раз в год | Веретенникова М.А. |
|  | Доступ к бумажным носителям с персональными данными | Законодательство Российской Федерации | 1 раз в год | Родионова Т.В. |
|  | Доступ в помещения, где обрабатываются и хранятся бумажные носители с персональными данными | Порядок доступа служащих в помещения, где ведется обработка персональных данных | 1 раз в год | Теплякова Е.И. |

Ответственный за организацию

обработки персональных данных \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Алексеев А.И.

“\_\_\_\_” \_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

Приложение 2

к правилам осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

УТВЕРЖДАЮ:

Директор ГОБПОУ «Елецкий колледж

экономики, промышленности и

отраслевых технологий»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Р.Ю.Евсеев

Приказ от 29 декабря 2018 г № 474

**Акт**

**проведения внутренней проверки условий обработки**

**персональных данных** **в информационной системе персональных данных Государственного областного бюджетного профессионального образовательного учреждения «Елецкий колледж экономики, промышленности и отраслевых технологий»**

Настоящий Акт составлен в том, что «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_20\_\_\_\_\_ г. лицом, 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: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Председатель комиссии:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Ф.И.О.) (подпись)

Члены комиссии:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Ф.И.О.) (подпись)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Ф.И.О.) (подпись)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(Ф.И.О.) (подпись)

«\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_\_ г.