УТВЕРЖДЕНЫ
приказом № 332 от 04.06. 2024
Директор ГАПОУ СО «ТМК»

И.А.Мочалов _____

П 372-2024

ПРАВИЛА
ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ В СООТВЕТСТВИИ С ОБРАБОТКОЙ ПЕРСОНАЛЬНЫХ ДАННЫХ В ГОСУДАРСТВЕННОМ АВТОНОМНОМ ПРОФЕССИОНАЛЬНОМ ОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ САМАРСКОЙ ОБЛАСТИ «ТОЛЬЯТТИНСКИЙ МАШИНОСТРОИТЕЛЬНЫЙ КОЛЛЕДЖ»

(взамен П 350-2023)

г.Тольятти, 2024

1. Общие положения

1.1. Настоящие Правила определяют процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере защиты персональных данных (далее – ПДн); основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки информации в государственном автономном профессиональном образовательном учреждении Самарской области «Тольяттинский машиностроительный колледж» (далее – Учреждение) требованиям к защите персональных данных.

1.2. Настоящие Правила разработаны в соответствии с руководящими и нормативными документами регуляторов Российской Федерации в области защиты персональных данных.

1.3. Контрольные мероприятия за обеспечением состояния обеспечения безопасности информации, и соблюдений условий использования средств защиты ПДн, а также соблюдением требований законодательства Российской Федерации по обработке персональных данных в Учреждении проводятся в следующих целях:

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

2. Тематика внутреннего контроля

2.1. Тематика внутреннего контроля соответствия обработки информации требованиям к защите персональных данных:

2.1.1. Проверки соответствия обработки информации в Учреждении установленным требованиям разделяются на следующие виды:

- регулярные;
- плановые;
- внеплановые.

2.1.2. Регулярные контрольные мероприятия проводятся Администратором информационной безопасности периодически в соответствии с утвержденным Планом проведения контрольных мероприятий (далее – План) Приложение № 1 и предназначены для осуществления контроля выполнения требований в области защиты информации ограниченного доступа, не составляющей государственную тайну, в т.ч. персональных данных.

2.1.3. Плановые контрольные мероприятия проводятся постоянной комиссией периодически в соответствии с утвержденным Планом (Приложение № 1) и направлены на постоянное совершенствование системы защиты информации в Учреждении.

2.1.4. 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 ГАПОУ СО «ТМК».

3. Планирование контрольных мероприятий

3.1. Для проведения плановых внутренних контрольных мероприятий Администратор информационной безопасности разрабатывает План внутренних контрольных мероприятий на текущий год.

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

4. Оформление результатов контрольных мероприятий

4.1. Информация о проведенном контрольном мероприятии фиксируется в Журнале учета внутренних мероприятий по контролю за обеспечением безопасности информации (далее – Журнал) Приложение № 2.

4.2. В Журнале фиксируется следующая информация:

- наименование мероприятия;
- дата проведения мероприятия;
- исполнитель;
- результат.

5. Порядок проведения плановых и внеплановых проверок

5.1. Плановые и внеплановые контрольные мероприятия проводятся при обязательном участии лица, ответственного за организацию обработки ПДн в ГАПОУ СО «ТМК», совместно с Администратором информационной безопасности (далее - Комиссия).

5.2. Проверки проводятся на основании Плана проведения контрольных мероприятий.

5.3. Проведение внеплановой проверки организуется в течение пяти рабочих дней с момента поступления соответствующего заявления.

5.4. При проведении проверки должны быть полностью, объективно и всесторонне установлены:

- порядок и условия применения организационных и технических мер по обеспечению защиты ПДн, исполнение которых в том числе обеспечивает установленные уровень/класс защищенности информационной системы уровень защищенности ПДн (если такие ПДн обрабатываются в информационной системе);
- порядок и условия применения средств защиты информации;
- эффективность принимаемых мер по обеспечению безопасности информации в Учреждении;
- состояние учета машинных носителей информации;
- соблюдение правил доступа к ПДн;
- наличие (отсутствие) фактов несанкционированного доступа к информации и принятие необходимых мер.

5.5. При проведении внутренней проверки комиссия имеет право:

- запрашивать у работников ГАПОУ СО «ТМК», допущенных к обработке информации ограниченного доступа в Учреждении, сведения, необходимые для реализации полномочий;

- требовать от уполномоченных на обработку информации ограниченного доступа должностных лиц уточнения, блокирования или уничтожения недостоверных, или полученных незаконным путем ПДн;

- принимать меры по приостановлению или прекращению обработки ПДн, осуществляемой с нарушением требований законодательства Российской Федерации;

- вносить руководителю ГАПОУ СО «ТМК» предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности информации предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки ПДн.

5.6. В отношении информации ограниченного доступа, ставшей известной комиссии в ходе проведения мероприятий по внутреннему контролю, должна обеспечиваться ее конфиденциальность.

5.7. Проверка должна быть завершена не позднее, чем через пять рабочих дней со дня принятия решения о её проведении. Все проводимые мероприятия по контролю за обеспечением безопасности информации должны быть зафиксированы в Журнале (Приложение № 2). Ответственность за ведение Журнала возлагается на Администратора информационной безопасности.

РАЗРАБОТАНО:

Ведущий специалист по кадрам Т.О.Медяшкина

СОГЛАСОВАНО:

Заместитель директора по учебно – производственной работе С.А. Крюков

Юрисконсульт Э.Н. Зайкова

ПРИЛОЖЕНИЕ № 1

№ п/п	Мероприятие	Периодич-ность	Ответственный
1	Поддержание журнала учета проверок в актуальном состоянии	Еженедельно	
2	Контроль над соблюдением режима обработки персональных данных	Еженедельно	
3	Контроль над соблюдением режима защиты информации ограниченного доступа	Ежедневно	
4	Анализ журнала учета событий, регистрируемых средствами защиты, с целью контроля действий пользователей и выявления возможных нарушений	Ежемесячно	
5	Проверка соответствия состава и структуры программно-технических средств Учреждении документированному составу и структуре средств, представленному в техническом паспорте Учреждении	Ежеквартально	
6	Проверка выполнения требований по условиям расположения АРМ в помещениях, в которых размещены элементы Учреждении	Ежемесячно	
7	Проверка неизменности настроенных параметров средств защиты информации, используемых в Учреждении	Ежеквартально	
8	Проверка соблюдения правил соблюдения парольной защиты	Ежемесячно	
9	Проверка знаний персоналом базы нормативно-методических документов в области обеспечения безопасности ПДн	Ежеквартально	
10	Контроль над выполнением антивирусной защиты,	Еженедельно	

	обновлением антивирусных баз и версий средств антивирусной защиты		
11	Контроль над соблюдением режима защиты при подключении к сетям общего пользования и (или) международного обмена	Еженедельно	
12	Тестирование функций средств защиты информации с помощью тест-программ, имитирующих попытки несанкционированного доступа	Ежемесячно	
13	Контроль над соблюдением безопасности передачи информации ограниченного доступа по каналам связи	Еженедельно	
14	Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты информации ограниченного доступа	Ежегодно	
15	Контроль над обновлением программного обеспечения и единообразия применяемого программного обеспечения	Еженедельно	
16	Контроль над обеспечением резервного копирования информации ограниченного доступа и программных средств	Ежемесячно	
17	Организация анализа и пересмотра имеющихся угроз безопасности информации ограниченного доступа, а также прогнозирование появления новых угроз безопасности	Ежегодно	
18	Поддержание в актуальном состоянии нормативно-организационных документов	Ежемесячно	

19	Контроль над разработкой и внесением изменений в программное обеспечение собственной разработки или штатное программное обеспечение, специально дорабатываемое собственными разработчиками или сторонними организациями	Ежемесячно	

ПРИЛОЖЕНИЕ 2

ЖУРНАЛ

учета внутренних мероприятий по контролю за обеспечением безопасности информации, в т.ч. ПДн, в государственном автономном профессиональном образовательном учреждении Самарской области «Тольяттинский машиностроительный колледж»

Журнал начат «____» _____ 202_ г.

_____
/Должность/

_____
/ФИО должностного лица/

Журнал завершен «____» _____ 202_ г.

_____
/Должность/

_____
/ФИО должностного лица/

На _____ листах

№ п/п	Мероприятие	Дата	Исполнитель	Результат

ЛИСТ ОЗНАКОМЛЕНИЯ

с Правилами осуществления внутреннего контроля в соответствии с обработкой персональных данных в ГАПОУ СО «ТМК»

№	ФИО (должность)	Дата	Подпись