Приложение 3
к приказу директора
ГБПОУ КК УТМиПТ
от 25.03.2024 г. № 64/1

ПРАВИЛА
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в государственном бюджетном профессиональном образовательном учреждении Краснодарского края «Успенский техникум механизации и профессиональных технологий»

1. Общие положения

1.1. Настоящие правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в государственном бюджетном профессиональном образовательном учреждении Краснодарского края «Успенский техникум механизации и профессиональных технологий» (далее – Правила) определяют порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным законодательством Российской Федерации и принятыми в соответствии с ним нормативными правовыми актами.

1.2. Настоящие Правила разработаны в соответствии с:

1.2.1 Федеральным законом от 27 июня 2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»);

1.2.2 постановлением Правительства Российской Федерации от 15 августа 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

1.2.3 постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке информационных системах персональных данных».

1.3. Настоящими Правилами в своей работе должны руководствоваться:

Работники государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий» (далее – образовательная организация), осуществляющие внутренний контроль соответствия обработки персональных данных требованиям к защите персональных данных.

2. Структура процессов по внутреннему контролю

2.1. Контроль выполнения требований по защите персональных данных в образовательной организации осуществляется с целью определения наличия

несоответствий между требуемым уровнем защиты персональных данных и его фактическим состоянием, а также выработки мер по их устранению и недопущению в дальнейшем.

2.2. Контроль выполнения требований по защите персональных данных в образовательной организации осуществляет ответственный за организацию обработки персональных данных и администратор информационной безопасности образовательной организации.

2.3. Контроль проводится в форме плановых и внеплановых проверок. Внеплановые проверки могут быть контрольными и по частным вопросам.

2.4. Контрольные проверки проводятся для установления полноты выполнения рекомендаций плановых проверок.

2.5. Проверки по частным вопросам охватывают отдельные направления по защите персональных данных и могут проводиться в случаях, когда стали известны факты несанкционированного доступа, утечки либо утраты персональных данных субъектов персональных данных или нарушения требований по защите персональных данных.

2.6. Сроки проведения контрольных проверок доводятся руководителям проверяемых структурных подразделений образовательной организации не позднее, чем за 24 часа до начала проверки.

2.7. Проверки по частным вопросам могут проводиться без уведомления руководителей структурных подразделений образовательной организации.

2.8. Периодичность и сроки проведения плановых проверок структурных подразделений Техникума устанавливаются планом проверок на календарный год. Сроки проведения плановых проверок доводятся руководителям проверяемых подразделений не позднее, чем за 10 суток до начала проверки.

3. Порядок подготовки к проверке

3.1. Общий контроль выполнения требований по обеспечению безопасности персональных данных в структурных подразделениях образовательной организации осуществляется в соответствии с Планом проведения внутренних проверок соответствия обработки персональных данных требованиям к защите персональных данных образовательной организации (форма представлена в приложении 1), утвержденным директором образовательной организации.

3.2. Ответственный за организацию обработки персональных данных подготавливает предложения по составу комиссии или группы проверяющих лиц.

3.3. Контроль в структурных подразделениях образовательной организации, осуществляется в соответствии с Планом проведения внутренних проверок соответствия обработки персональных данных требованиям к защите персональных данных структурных подразделений образовательной организации а (форма представлена в приложении 2). Данные Планы утверждаются руководителями структурных подразделений образовательной организации и согласовываются с ответственным за выполнение мероприятий по контролю

исполнения структурных подразделений Техникума, требований документов по обеспечению безопасности персональных данных.

3.4. Проверяющие лица обязаны получить у руководителей проверяемых структурных подразделений Техникума информацию об условиях обработки персональных данных, необходимую для достижения целей проверки. Перед началом проверки они должны изучить материалы предыдущих проверок данного структурного подразделения образовательной организации.

4. Порядок проведения проверки

4.1. Руководитель проверяемого структурного подразделения образовательной организации обязан оказывать содействие комиссии по проверке или группе проверяющих лиц и в случае необходимости определяет должностное лицо, ответственное за сопровождение проверки.

4.2. Допуск проверяющих лиц к конкретным информационным ресурсам, защищаемым сведениям и техническим средствам должен исключать ознакомление проверяющих лиц с конкретными персональными данными.

4.3. Должны быть согласованы конкретные вопросы по объему, содержанию, срокам проведения проверки, а также каких работников структурных подразделений образовательной организации необходимо привлечь к проверке и какие помещения следует посетить.

4.4. Общий порядок проведения проверки включает:

4.4.1 выявление работников, задействованных в обработке персональных данных;

4.4.2 проверка факта ознакомления работников проверяемого структурного подразделения образовательной организации с нормативными документами, регламентирующими вопросы обработки и защиты персональных данных;

4.4.3 получение при содействии работников проверяемого структурного подразделения образовательной организации документов, касающихся обработки и защиты персональных данных в данном структурном подразделении и анализ полученной документации;

4.4.4 непосредственная проверка выполнения установленного порядка обработки и защиты персональных данных и требований законодательства Российской Федерации в области защиты персональных данных.

4.5. В ходе осуществления контроля выполнения требований по защите персональных данных в структурном подразделении образовательной организации рассматриваются следующие показатели работ по защите персональных данных:

4.5.1 наличие согласий на обработку персональных данных субъектов персональных данных, в случаях, предусмотренных законодательствам Российской Федерации;

4.5.2 соответствие состава и сроков обработки целям обработки персональных данных;

4.5.3 соответствие Перечня должностей работников, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным реальному составу работников;

4.5.4 соответствие Перечня лиц, имеющих доступ в помещения, в которых ведется обработка персональных данных реальному составу работников;

4.5.5 наличие нормативных документов по защите персональных данных;

4.5.6 знание нормативных документов и уровень подготовки работников, имеющих доступ к персональным данным;

4.5.7 полнота и правильность выполнения требований нормативных документов работниками, имеющими доступ к персональным данным;

4.5.8 наличие документов, подтверждающих учет и сохранность материальных носителей персональных данных.

4.6. В ходе осуществления контроля выполнения требований по защите персональных данных в структурном подразделении образовательной организации дополнительно рассматриваются следующие показатели работ по защите персональных данных:

4.6.1 соответствие информации, указанной в уведомлении об обработке персональных данных, реальному положению дел;

4.6.2 наличие и корректность перечня информационных систем;

4.6.3 наличие документа, подтверждающего:

4.6.3.1 правильность определения уровня защищенности персональных данных, обрабатываемых в информационных системах, а также классов защищенности информационных систем;

4.6.3.2 наличие документа, подтверждающего факт определения угроз безопасности персональных данных, а также его актуальность (срок актуальности документа не может превышать 3 года);

4.6.3.3 соответствие состава средств вычислительной техники информационных систем указанному в документации на информационную систему;

4.6.3.4 соответствие требованиям по организации разграничения доступа пользователей к информационным ресурсам (в том числе сетевым);

4.6.3.5 порядок защиты персональных данных при передаче по сети;

4.6.3.6 применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

4.6.3.7 оценка эффективности принимаемых мер по обеспечению безопасности персональных данных.

4.7. Во время проведения проверки, выявленные нарушения требований по обработке и защите персональных данных должны быть по возможности устранены. Проверяющие лица могут дать рекомендации по устранению на месте отмечаемых нарушений и недостатков.

4.8. Недостатки, которые не могут быть устранены на месте, включаются в итоговый документ по результатам проверки.

5. Оформление результатов проверки

5.1. Результаты проверки оформляются актом.

5.2. Акт составляется в одном экземпляре и подписывается членами комиссии. Оригинал документа с результатами проверки хранится (передается) у ответственного за выполнение мероприятий по контролю исполнения структурными подразделениями образовательной организации требований документов по обеспечению безопасности персональных данных. Копия документа о проверке передается в проверяемое структурное подразделение образовательной организации.

5.3. Результаты проверок подразделений периодически обобщаются ответственным за выполнение мероприятий по контролю исполнения структурными подразделениями образовательной организации доводятся до сведения ответственного за организацию обработки и обеспечение безопасности персональных данных образовательной организации.

5.4. При необходимости принятия решений по результатам проверки структурного подразделения образовательной организации – ответственному за организацию обработки и обеспечение безопасности персональных данных образовательной организации готовится соответствующая служебная записка.

6. Корректирующие мероприятия и контроль за их исполнением

6.1. Руководитель структурного подразделения образовательной организации анализирует акт о результатах внутренней проверки и в пятидневный срок определяет перечень мероприятий, необходимых для устранения нарушений и их причин.

6.2. Перечень мероприятий согласуется с ответственным за организацию обработки и обеспечение безопасности персональных данных образовательной организации.

6.3. Если корректирующие мероприятия касаются других структурных подразделений образовательной организации, то к анализу привлекаются специалисты соответствующих структурных подразделений.

6.4. Выполнение корректирующих мероприятий и их достаточность определяется ответственным за организацию обработки и обеспечение безопасности персональных данных образовательной организации.

6.5. Внутренняя проверка считается оконченной после выполнения всех корректирующих мероприятий и устранения выявленных нарушений.

Приложение 1
к Правилам осуществления
внутреннего контроля соответствия
обработки персональных данных
требованиям к защите
персональных данных

ПЛАН
проведения внутренних проверок соответствия обработки персональных данных требованиям к защите персональных данных государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий»

№ п/п	Наименование структурного подразделения государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий»	Наименование мероприятия	Период проведения проверки	Отметка о выполнении (№ акта проверки)	Отметка о выполнении корректирующих мероприятий	Примечание
1	2	3	4	5	6	7

Приложение 2
к Правилам осуществления
внутреннего контроля соответствия
обработки персональных
данных требованиям к защите
персональных данных

ПЛАН
проведения внутренних проверок соответствия обработки персональных данных требованиям к защите персональных данных структурных подразделений государственного бюджетного профессионального образовательного учреждения Краснодарского края «Успенский техникум механизации и профессиональных технологий»

№ п/п	Наименование мероприятия	Период проведения проверки	Отметка о выполнении (№ акта проверки)	Отметка о выполнении корректирующих мероприятий	Примечание
1	2	3	4	5	6