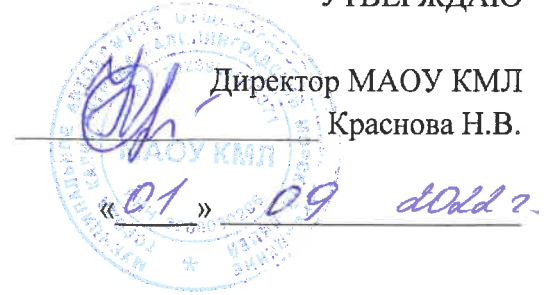


УТВЕРЖДАЮ

Директор МАОУ КМЛ
Краснова Н.В.



**Правила
внутреннего контроля соответствия обработки персональных данных
работников, обучающихся, родителей (законных представителей) обучающихся в
МАОУ КМЛ**

1. Общие положения

1.1. Настоящие Правила внутреннего контроля соответствия обработки персональных данных требованиям защиты персональных данных в муниципальном автономном общеобразовательном учреждении города Калининграда Калининградский морской лицей (далее - МАОУ КМЛ) устанавливаются основания, порядок и формы проведения внутреннего контроля соответствия обработки и защиты персональных данных требованиям, установленным в МАОУ КМЛ.

1.2. Настоящие Правила разработаны в соответствии с законодательством Российской Федерации в области обработки и защиты персональных данных (далее – ПДн) и иными правовыми актами, принимаемыми в соответствии с данным законодательством (далее – законодательство в сфере ПДн)

2. Порядок осуществления внутреннего контроля

2.1. Внутренний контроль соответствия обработки ПДн установленным требованиям (далее – внутренний контроль) осуществляется в МАОУ КМЛ путем проведения проверок соблюдения требований законодательства в сфере ПДн.

2.2. Проверки проводятся лицом, ответственным за организацию обработки ПДн.

2.3. Проверки разделяются на плановые и внеплановые

2.4. Плановые проверки проводятся в соответствии с ежегодным планом проведения проверок соответствия обработки ПДн требованиям защиты не реже 1 раза в год (приложение №1).

2.5. Ежегодный план проверок разрабатывается лицом, ответственным за организацию обработки ПДн и утверждается директором МАОУ КМЛ для осуществления внутреннего контроля соответствия обработки ПДн требованиям, предусмотренным ФЗ «О защите персональных данных».

2.6. Основанием для проведения внеплановой проверки является поступившее в МАОУ КМЛ письменное обращение субъекта персональных данных или его представителя о нарушении правил обработки персональных данных, зарегистрированное в Журнале учета обращений субъектов персональных данных (приложение №2).

2.7. Проведение внеплановой проверки организуется в течение 3 рабочих дней с момента поступления обращения.

2.8. Срок проведения проверки не может превышать месяц со дня принятия решения о ее проведении.

2.9. Лицо, ответственное за организацию обработки ПДн, получившее доступ к ПДн субъектов ПДн в ходе проведения проверки, обеспечивает конфиденциальность ПДн субъектов ПДн, не раскрывает третьим лицам и не распространяет ПДн без согласия субъекта ПДн.

2.10. При проведении проверки должны быть полностью и всесторонне установлены:

- 1) порядок и условия применения средств защиты информации;
- 2) состояние учета носителей ПДн;
- 3) соблюдение правил доступа к персональным данным;
- 4) соблюдение пользователем информационной системы ПДн парольной и антивирусной политики, правил работы с машинными носителями информации, криптографическими средствами защиты информации;
- 5) соблюдение порядка резервирования баз данных и хранения резервных копий;
- 6) соблюдение условий хранения бумажных носителей с ПДн;
- 7) соблюдение правил доступа к бумажным носителям с ПДн;
- 8) наличие (отсутствие) фактов несанкционированного доступа к ПДн и принятие необходимых мер;
- 9) мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

2.11. Лицо, ответственное за организацию обработки ПДн при проведении проверки вправе в пределах своей компетенции:

- 1) запрашивать и получать у работников необходимые документы (сведения) для достижения целей проведения внутреннего контроля;
- 2) получать доступ к информационным системам ПДн;
- 3) принимать меры по приостановлению или прекращению обработки ПДн, осуществляемой с нарушениями требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», принятых в соответствии с ним локальных нормативных актов МАОУ КМЛ;
- 4) требовать от работников, имеющих доступ к обработке ПДн, уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем ПДн;
- 5) вносить директору предложения о:
 - а) совершенствовании правового, технического и организационного обеспечения безопасности ПДн при их обработке;
 - б) приостановлении или прекращении обработки ПДн, осуществляемой с нарушением требований законодательства Российской Федерации;
 - в) привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации о ПДн.

2.12. При проведении проверки лицо, ответственное за организацию обработки ПДн не вправе:

- 1) требовать представления документов и информации, которые не относятся к предмету проверки;
- 2) распространять информацию, полученную в результате проведения проверки и составляющую государственную, служебную, иную охраняемую законом тайну, за исключением случаев, предусмотренных законодательством Российской Федерации.

2.13. Лицо, ответственное за организацию обработки ПДн при проведении проверки обязано:

1) своевременно и в полной мере исполнять предоставленные в соответствии с законодательством Российской Федерации полномочия по предупреждению, выявлению и пресечению нарушений требований;

2) соблюдать законодательство Российской Федерации, права и законные интересы работника, в отношении которого проводится проверка;

3) обеспечивать конфиденциальность ставших ему известными в ходе проведения мероприятий внутреннего контроля ПДн.

2.14. Проверки проводятся с участием проверяемого работника, имеющего доступ к обработке ПДн, непосредственно на месте обработки ПДн путем опроса либо, при необходимости, путем осмотра рабочего места работника, имеющего доступ к обработке ПДн.

2.15. Работник, имеющий доступ к обработке ПДн, при проведении проверки имеет право:

1) непосредственно присутствовать при проведении проверки;

2) давать объяснения по вопросам, относящимся к предмету проверки;

3) знакомиться с результатами проверки.

2.12. При проведении проверки работник, имеющий доступ к обработке ПДн, должен:

1) обеспечить необходимые условия для проведения проверки;

2) организовать доступ к оборудованию, в помещения, где осуществляется обработка

ПДн;

3) предоставить необходимую информацию и документацию для достижения целей проверки.

3. Порядок фиксирования результатов проверки

3.1. Факт проведения проверок и результаты проверки фиксируются в Журнале проведения проверок соответствия обработки ПДн (приложение №3).

3.2. Нарушения, выявленные в ходе проверки, подлежат исполнению в срок, установленный в Журнале проведения проверок соответствия обработки ПДн.

3.2. В целях контроля устранения выявленных нарушений лицо, ответственное за организацию обработки ПДн, может провести повторную проверку.

3.4. Журнале проведения проверок соответствия обработки ПДн, а также иные документы и информация, полученные (разработанные) в ходе проведения проверки, хранятся в течение 3-х лет.

**муниципальное автономное общеобразовательное учреждение города
Калининграда Калининградский морской лицей**

ПЛАН
проведения проверок соответствия обработки ПДн требованиям защиты

№ п/п	Мероприятие	Дата
1	Проверка полноты, качества и актуальности разработанных внутренних распорядительных и нормативно-методических документов, регламентирующих обработку и обеспечение безопасности ПДн	
2	Проверка порядка и условий применения средств защиты информации	
3	Проверка соблюдения правил доступа к персональным данным	
4	Проверка выполнения требований действующих нормативных документов по защите ПДн	
5	Проверка соблюдения пользователем информационной системы ПДн парольной и антивирусной политики, правил работы с машинными носителями информации, криптографическими средствами защиты информации	
6	Проверка соблюдения условий хранения бумажных носителей с ПДн; соблюдение правил доступа к бумажным носителям с ПДн	
7	Проверка актуальности сведений в Реестре операторов ПДн Роскомнадзора	
8	Подведение итогов	
9	Устранение недостатков	

