Федеральное агентство морского и речного транспорта

Федеральное государственное бюджетное образовательное учреждение высшего образования

«Государственный университет морского и речного флота имени адмирала С.О. Макарова»

Положение по организации внутреннего контроля соответствия обработки персональных данных

Санкт-Петербург
2023

СТРАНИЦА СТАТУСА ДОКУМЕНТА

Приложение № 3

к приказу ФГБОУ ВО «ГУМРФ имени адмирала С.О. Макарова»
от 29.05. 2023 № 601

Система менеджмента качества **Положение по организации внутреннего контроля соответствия обработки персональных данных**	Новая редакция

Настоящее Положение разработано согласно требованиям Международного Стандарта ИСО 9001:2015 и является документом системы менеджмента качества ФГБОУ ВО «ГУМРФ имени адмирала С.О. Макарова».

Положение разработано в соответствии с действующим законодательством и нормативными правовыми актами Российской Федерации.

Положение устанавливает порядок организации контроля соответствия обработки персональных данных ФГБОУ ВО «ГУМРФ имени адмирала С.О. Макарова» требованиям законодательства в области защиты информации и персональных данных.

Контроль документа	Первый проректор
Руководитель разработки	Директор департамента цифрового развития и информатизации Кислов Р.И.
Исполнитель	Кислов Р.И.

Оглавление

Лист ознакомления

№	Должность	Ф.И.О.	Дата	Подпись
1				
2				
3				
4				
5				
6				

Лист учета экземпляров

Место хранения корректируемых экземпляров	№ экземпляра
Департамент цифрового развития и информатизации	2

Место хранения некорректируемого экземпляра	№ экземпляра
Общий отдел	1
Служба качества	3
Корпоративный портал	

Лист учета корректуры

№	Номер страницы	Номер пункта	Изменение (проверка)	Дата внесения корректуры (проверки)	Утверждение корректуры (Ф.И.О. / Подпись)

I. Общие положения

1.1. Настоящее положение по организации контроля соответствия обработки персональных данных, разработано в соответствии со следующими нормативно- правовыми актами:

– Федеральный закон РФ № 149-ФЗ от 27 июля 2006 г. «Об информации, информационных технологиях и о защите информации»;

– Федеральный закон от 27 июля 2006 № 152-ФЗ «О персональных данных»;

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

– Приказ ФСТЭК России № 17 от 11 февраля 2013 г. «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

– Приказ ФСТЭК России № 21 от 18 февраля 2013 г. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.2. Периодический внутренний контроль и (или) аудит соответствия обработки персональных данных Федеральному закону «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, Положению о персональных данных ФГБОУ ВО «ГУМРФ имени адмирала С.О. Макарова» (далее - университет) должен проводиться не реже одного раза в три года.

1.3. Ответственным за проведение мероприятий по внутреннему контролю обработки персональных данных является ответственный за организацию обработки персональных данных университета, назначенный приказом ректора университета.

1.4. Действие данного положения распространяется на университет и его филиалы.

II. Контроль соответствия обработки персональных данных

2.1. Внутренний аудит соответствия обработки персональных данных Федеральному закону «О персональных данных» и принятым в соответствии с ним нормативным правовым актам проводится компетентными лицами (группа аудита), назначаемыми приказом ректора

либо распоряжением ответственного за обработку персональных данных университета из числа работников университета.

2.2. В состав группы аудита должен быть включен директор департамента цифрового развития и информатизации.

2.3. Уведомление ответственных должностных лиц университета о предстоящем аудите соответствия обработки персональных данных осуществляет ответственный за обработку персональных данных в ходе проведения постановочного совещания.

2.4. Аудиторы, проводящие контроль соответствия обработки персональных данных, должны использовать имеющуюся информацию о предыдущих проверках, что необходимо для повышения эффективности контроля.

2.5. Отчет о проведении контроля соответствия обработки персональных данных университета (неизменную копию отчета) руководитель группы аудита передает непосредственно ответственному за организацию обработки персональных данных университета.

2.6. Отчет о проведении контроля соответствия обработки персональных данных университета является информацией ограниченного доступа и не подлежит ознакомлению должностными лицами университета, не допущенными к обработке персональных данных.

2.7. Группе аудита должны быть предоставлены возможности для беспрепятственного выполнения контроля соответствия обработки персональных данных.

2.8. Методы аудита соответствия обработки персональных данных включают: сбор предварительной информации, планирование объема и содержания работ, анализ локальных нормативных актов университета, установление связи с ответственными должностными лицами (в том числе интервьюирование), обследование конкретных информационных систем персональных данных (далее - ИСПДн), технический контроль эффективности защиты персональных данных.

2.9. Методы проведения аудита соответствия обработки персональных данных в филиалах университета могут быть скорректированы ввиду недостаточности визуального контроля соответствия мер и средств обработки персональных данных.

2.10. Собранные в ходе аудита соответствия обработки персональных данных свидетельства должны вноситься в список рабочих документов проверки. Свидетельства аудита наряду с отчетом по аудиту должны быть надлежащим образом защищены группой аудита путем использования мер и средств контроля и управления доступом.

2.11. Обо всех несоответствиях обработки персональных данных, выявленных в ходе аудита, руководитель группы аудита обязан немедленно известить ответственных должностных лиц университета для принятия мер по устранению выявленных нарушений обработки

персональных данных.

2.12. Руководитель группы аудита проводит выборочную проверку знаний работниками локальных нормативных актов университета по вопросам обработки персональных данных, по вопросам защиты персональных данных.

2.13. Результаты аудита соответствия обработки персональных данных заносятся в «Журнал учета мероприятий по контролю соответствия обработки персональных данных» (Приложение).

2.14. Время для проведения аудита соответствия обработки персональных данных определяет ответственный за обработку персональных данных исходя из понимания затрат и полезности результатов аудита.

III. Контроль эффективности защиты персональных данных в информационной системе университета

3.1. Меры по контролю защищенности персональных данных, содержащихся в информационных системах персональных данных, должны реализовываться путем проведения анализа защищенности и тестирования ее системы защиты информации (далее – СЗИ). На основе данных анализа и тестирования СЗИ осуществляется выбор и внедрение (при необходимости) средств защиты информации, сертифицированных на соответствие требованиям по безопасности информации.

3.2. Ответственность за анализ защищенности и тестирование системы защиты информации ИСПДн возлагается на начальника отдела сетевого и системного администрирования департамента цифрового развития и информатизации. В случае необходимости углубленного анализа защищенности информации могут привлекаться сторонние организации, имеющие лицензию ФСТЭК России на оказание услуг по технической защите информации.

3.3. Контроль эффективности защиты персональных данных осуществляется путем проведения периодических плановых и внеплановых проверок СЗИ. Проверке подвергаются функции СЗИ, состав которых определяется в соответствии с установленным для ИСПДн уровнем защищенности персональных данных.

3.4. Обследование ИСПДн проводится с целью определения соответствия помещений, технических и программных средств, организационной, эксплуатационной и проектной документации требованиям по защите персональных данных. В ходе обследования проверяется эффективность применения организационных и технических мероприятий по следующим направлениям защиты информации:

– соблюдение организационно-технических требований к помещениям, в которых располагаются компоненты ИСПДн;

– сохранность печатей, пломб на технических средствах передачи и обработки информации, а также на устройствах их защиты;

– контроль парольной защиты согласно «Инструкции по организации парольной защиты»;

– контроль выполнения требований по защите ИСПДн от несанкционированного доступа;

– выявления попыток несанкционированного доступа;

– тестирование конфигурации средств защиты информации;

– выполнение требований по защите информации при внешних взаимодействиях (передача персональных данных за пределы контролируемой зоны);

– выполнение требований по криптографической защите информации;

– выполнение требований по трансграничной передаче персональных данных;

– выполнение требований по антивирусной защите информации, согласно «Инструкции по организации антивирусной защиты».

3.4. Результаты, полученные в ходе ведения контроля, обрабатываются и анализируются в целях определения достаточности и эффективности предписанных мер защиты информации и выявления нарушений. При обнаружении нарушений требований по защите информации, выявленных в ходе проведения внеплановой проверки, директор департамента цифрового развития и информатизации докладывает ответственному за обработку персональных данных для принятия им решения по устранению выявленного нарушения.

3.5. Результаты контроля эффективности защиты персональных данных заносятся в «Журнал учета мероприятий по контролю соответствия обработки персональных данных».

Приложение

Журнал учета мероприятий по защите персональных данных

Журнал начат «__»_____20__г. Должность_____ (ФИО должностного лица)	Журнал завершен «__»_____20__г. Должность_____ (ФИО должностного лица)

№ п/п	Наименование мероприятия	Краткое описание мероприятия	Дата проведения	ФИО проводившего мероприятие	Подпись	Примечание