МИНИСТЕРСТВО ПРИРОДНЫХ РЕСУРСОВ И ЭКОЛОГИИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ГИДРОМЕТЕОРОЛОГИИ И МОНИТОРИНГУ
ОКРУЖАЮЩЕЙ СРЕДЫ
(РОСГИДРОМЕТ)

Федеральное государственное бюджетное учреждение

«СИБИРСКИЙ РЕГИОНАЛЬНЫЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ ИНСТИТУТ»
(ФГБУ «СибНИГМИ»)

630099, г. Новосибирск, ул.Советская,30
Тел. (383) 222-25-30, 222-41-39
НОВОСИБИРСК ГИМЕТ
Факс (383) 222-25-30 e-mail adm@sibnigmi.ru

П Р И К А З

25.12.2024 № 243/ОД

О назначении должностного лица, ответственного за организацию защиты персональных данных в информационных системах

В целях обеспечения защиты персональных данных работников и безопасности в информационных системах ФГБУ «СибНИГМИ», руководствуясь Федеральным законом от 27.07.2006 N 152-ФЗ «О персональных данных» ,

ПРИКАЗЫВАЮ:

1. Назначить специалиста по закупкам Воложанинова К.А. ответственным за организацию защиты персональных данных в информационных системах ФГБУ «СибНИГМИ».

2. Разрешить доступ специалисту по закупкам Воложанинову К.А к персональным данным, необходимым для выполнения служебных (трудовых) обязанностей.

3. Утвердить Инструкцию ответственного за организацию защиты персональных данных в информационных системах ФГБУ «СибНИГМИ» (Приложение 1).

4. Ответственному за организацию защиты персональных данных в информационных системах в своей работе руководствоваться требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», руководящих и нормативных документов ФСТЭК, Федеральной службы по надзору в сфере связи,

информационных технологий и массовых коммуникаций, Инструкцией ответственного за организацию защиты персональных данных в информационных системах, а также принятыми в ФГБУ «СибНИГМИ» локальными нормативными актами и организационно-распорядительными документами.

5. В случае отсутствия Воложанинова К.А. его полномочия, как ответственного за организацию защиты персональных данных в информационных системах, могут быть переданы иному должностному лицу в соответствии с приказом директора.

Основания: Дополнительное соглашение от 25.12.2024 к трудовому договору от 11.03.2024 № 7/24 со специалистом по закупкам Воложаниновым К.А.

Врио директора В.Н.Копылов

С приказом ознакомлен: Воложанинов К.А

Специалист по кадрам
Т.А.Пустовалова

Приложение №1
к приказу № 243/ОД
от 25.12.2024г.

ИНСТРУКЦИЯ
ответственного за организацию защиты персональных данных в информационных системах ФГБУ «СибНИГМИ»

1. Общие положения

1.1 Настоящая Инструкция разработана в соответствии с требованиями законодательства Российской Федерации в сфере защиты персональных данных и определяет задачи, функции, обязанности, права и ответственность сотрудника ответственного за организацию защиты персональных данных в информационных системах ФГБУ «СибНИГМИ». Кроме того, в настоящей Инструкции определена технология выполнения функций и обязанностей, а также решения задач сотрудником, ответственным за организацию защиты персональных данных в информационных системах.

1.2 Сотрудник, ответственный за организацию защиты персональных данных в информационных системах назначается приказом директора.

1.3 Сотрудник, ответственный за организацию защиты персональных данных в информационных системах, в пределах своих функциональных обязанностей организует обеспечение безопасности персональных данных, обрабатываемых в информационной системе персональных данных с использованием средств автоматизации.

1.4 Сотрудник, ответственный за организацию защиты персональных данных в информационных системах, руководствуется положениями настоящей Инструкции, Приказа ФСТЭК России от 18 февраля 2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при обработке в информационных системах персональных данных», требованиями других нормативных правовых и нормативно-методических документов, регламентирующих защиту персональных данных, при их автоматизированной обработке в информационной системе персональных данных, а также требованиями эксплуатационной документации на эксплуатируемые средства защиты информации, технические и программные средства, используемые в информационной системе персональных данных, имеющие встроенные механизмы защиты.

Данная Инструкция является руководящим документом ответственного за организацию защиты персональных данных в информационных системах в ФГБУ «СибНИГМИ» (далее - Оператор). Требования ответственного за организацию защиты персональных данных в информационных системах, связанные с выполнением им своих функций, обязательны для исполнения всеми сотрудниками Оператора.

Ответственный за организацию защиты персональных данных в информационных системах подчиняется руководителю Организации, получает указания непосредственно от него и подотчетен только руководителю Организации.
Ответственный за организацию защиты персональных данных в информационных системах в своей деятельности руководствуется:

- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 01.11.2012 № 1119;
- Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным постановлением Правительства Российской Федерации от 15.09.2008 № 687;

- Приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Приказом Федеральной службы по техническому и экспортному контролю от 11.02.2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»; 11.02.2014
- настоящей Инструкцией.

2. Задачи и обязанности

2.1. Основными задачами сотрудника ответственного за организацию защиты персональных данных являются:
- организация функционирования системы защиты информации информационной системы персональных данных, включая организацию эксплуатации технических и программных средств защиты информации, в соответствии с установленными требованиями, по защите персональных данных и конфиденциальной информации в целом;
- текущий контроль работы средств и систем защиты информации;
- контроль за работой пользователей информационной системы персональных данных, выявление и регистрация попыток несанкционированного доступа к защищаемым информационным ресурсам.

2.2. Основными функциями сотрудника ответственного за организацию защиты персональных данных являются:

- организация установки, сопровождения, администрирования и обеспечения функционирования средств и систем защиты информации в пределах возложенных на него обязанностей;
- обучение персонала и пользователей информационной системы персональных данных правилам работы со средствами защиты информации;
- организация определения и назначения прав пользователям информационной системы защиты персональных данных на доступ к защищаемым информационным ресурсам информационной системы персональных данных в соответствии с Матрицей доступа, а также требованиями руководящих и нормативно-методических документов по защите персональных данных;
- организация защиты всех критичных средств и информации, используемых для доступа в систему (паролей и идентификаторов);
- организация осуществления периодического контроля программной среды информационной системы персональных данных на отсутствие компьютерных вирусов;
- проведение периодического контроля состава штатного программного обеспечения информационной системы персональных данных и их целостности;
- анализ журналов регистрации событий средств защиты от несанкционированного доступа;
- участие в проведении расследований фактов нарушения или угрозы нарушения безопасности защищаемой информации в информационной системе персональных данных;
- текущий контроль технологического процесса обработки защищаемой информации в информационной системе персональных данных.
- обеспечение непрерывного функционирования системы защиты персональных данных (далее - СЗПДн) в целом, ее программных и технических компонентов;
- настройка прав доступа сотрудников к персональным данным (далее - ПДн) и средствам их обработки согласно требованиям по информационной безопасности ПДн Оператора;
- разработка для пользователей информационных систем персональных данных инструкций по работе со средствами защиты информации;
- ведение журналов учета, входящих в состав организационно-распорядительной документации у Оператора;

- предоставление экспертных консультаций и рекомендаций сотрудникам, участвующим в обработке и обеспечении безопасности персональных данных (далее - ПДн) у Оператора, по вопросам использования средств защиты информации;
- хранение эталонного программного обеспечения средств защиты информации;
- ведение учета носителей ПДн и обеспечение их безопасного уничтожения согласно принятым у Оператора Регламентом по учёту, хранению и уничтожению носителей персональных данных;
- контроль обслуживания, настройки и ремонта средств обработки и средств защиты ПДн;
- сопровождение и контроль сторонних организаций (подрядчиков) в случае привлечения их для обслуживания, настройки и ремонта средств обработки и средств защиты ПДн;
- настройка конфигураций средств защиты информации, используемых для обеспечения безопасности ПДн;
- предоставление необходимой информации при проведении проверок уполномоченными органами и при проведении контрольных мероприятий по защите ПДн;
- реагирование на инциденты информационной безопасности, связанные с обработкой и обеспечением безопасности ПДн;
- участие во взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;
- информирование в порядке, определенном федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных;
- уведомление уполномоченного органа по защите прав субъектов персональных данных о факте неправомерной или случайной передаче (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных;
- в случае нарушения требований к защите персональных данных принимать необходимые меры по восстановлению нарушенных прав субъектов персональных данных.

3. Должен знать

Ответственный за обеспечение безопасности персональных данных должен знать:
- нормативно-правовые акты, регламентирующие вопросы обработки и защиты персональных данных;
- локальные нормативные акты и организационно-распорядительные документы по вопросам обработки и защиты персональных данных;
- особенности обработки и защиты персональных данных в Организации.

4. Технология решения основных задач и выполнения своих функций и обязанностей сотрудника, ответственного за организацию защиты персональных данных

4.1. В процессе эксплуатации информационной системы персональных данных сотрудник, ответственный за систему защиты информации в информационной системе персональных данных, обеспечивает выполнение всех установленных требований по защите персональных данных, применительно к установленному классу информационной системы персональных данных.

4.2. Сотрудник, ответственный за систему защиты информации в информационной системе персональных данных, контролирует порядок ведения, смены и хранения паролей доступа в информационную систему персональных данных.

4.3. При проверке правильности ведения паролей сотрудник, ответственный за систему защиты информации в информационной системе персональных данных, устанавливает соответствие всех используемых паролей доступа в информационной системе персональных данных в соответствии с требованиями инструкции по организации парольной защиты.

4.4. Сотрудник ответственный за систему защиты информации в информационной системе персональных данных контролирует работу пользователей и осуществляет выявление фактов несанкционированного доступа к персональным данным.

4.5. Сотрудник ответственный за систему защиты информации в информационной системе персональных данных организует установление прав пользователям информационной системы персональных данных по доступу к защищаемым информационным ресурсам в соответствии с Матрицей доступа.

5. Права сотрудника, ответственного за организацию защиты персональных данных

5.1. Требовать от пользователей информационной системы персональных данных и обслуживающего персонала информационной системы персональных данных соблюдения установленных правил обработки персональных данных и выполнения требований законодательства РФ и внутренних нормативных документов.

5.2. Выдвигать требование о прекращении доступа пользователя к работам в информационную систему персональных данных в случае грубых нарушений требований законодательства РФ и внутренних нормативных документов, порядка и правил обработки персональных данных или нарушения функционирования средств и систем защиты информации.

5.3. Требовать объяснительных документов и назначения служебного расследования в отношении пользователя информационной системы персональных данных и обслуживающего персонала информационной системы персональных данных по фактам нарушения безопасности информации и несанкционированного доступа к защищаемой информации.

5.4. Вносить директору предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке.

6. Ответственность сотрудника, ответственного за средства защиты информации в информационной системе персональных данных

Сотрудник ответственный за средства защиты информации в информационной системе персональных данных несет ответственность в полном объеме по действующему законодательству за разглашение сведений, составляющих служебную тайну, ставших известными ему в соответствии с родом работы, а также утрату конфиденциальных и выходных документов, содержащих персональные данные.

Согласовано:
Специалист по кадрам Т.А.Пустовалова

С настоящей инструкцией ответственного за организацию защиты персональных данных в информационных системах ознакомлен(а)

№ п/п	Фамилия, имя, отчество работника	Дата ознакомления	Подпись работника
1	Волошанинов К.А	25.12.2024	

ДОПОЛНИТЕЛЬНОЕ СОГЛАШЕНИЕ
К ТРУДОВОМУ ДОГОВОРУ 07/24 от 11.03.2024 г.

Город Новосибирск

25 декабря 2024 г.

Федеральное государственное бюджетное учреждение «Сибирский региональный научно-исследовательский гидрометеорологический институт» (ФГБУ «СибНИГМИ») в лице врио директора ***Копылова Василия Николаевича*** (приказ Росгидромета № 496 /лс от 25.09.2023), действующего на основании Устава от 26.10.2015, с изменениями от 09.11.2020г , именуемый в дальнейшем Работодатель, с одной стороны,

и _____ ***Воложанинов Константин Анатольевич*** _____
(Ф.И.О. Работника полностью)

именуемый в дальнейшем Работник, с другой стороны, вместе в тексте именуемые Стороны, заключили настоящее соглашение о нижеследующем:

1. Внести изменения в Трудовой договор № 07/24 от 11.03.2024 г.:

1.1. добавить в раздел 1.1 следующего содержания:

«Работник назначается ответственным за организацию защиты персональных данных в информационных системах ФГБУ «СибНИГМИ». Работник обязуется выполнять следующую работу:

- организация установки, сопровождения, администрирования и обеспечения функционирования средств и систем защиты информации в пределах возложенных на него обязанностей;
- обучение персонала и пользователей информационной системы персональных данных правилам работы со средствами защиты информации;
- организация определения и назначения прав пользователям информационной системы защиты персональных данных на доступ к защищаемым информационным ресурсам информационной системы персональных данных в соответствии с Матрицей доступа, а также требованиями руководящих и нормативно-методических документов по защите персональных данных;
- организация защиты всех критичных средств и информации, используемых для доступа в систему (паролей и идентификаторов);
- организация осуществления периодического контроля программной среды информационной системы персональных данных на отсутствие компьютерных вирусов;
- проведение периодического контроля состава штатного программного обеспечения информационной системы персональных данных и их целостности;
- анализ журналов регистрации событий средств защиты от несанкционированного доступа;
- участие в проведении расследований фактов нарушения или угрозы нарушения безопасности защищаемой информации в информационной системе персональных данных;
- текущий контроль технологического процесса обработки защищаемой информации в информационной системе персональных данных.
- обеспечение непрерывного функционирования системы защиты персональных данных (далее - СЗПДн) в целом, ее программных и технических компонентов;
- настройка прав доступа сотрудников к персональным данным (далее - ПДн) и средствам их обработки согласно требованиям по информационной безопасности ПДн Оператора;

- разработка для пользователей информационных систем персональных данных инструкций по работе со средствами защиты информации;
- ведение журналов учета, входящих в состав организационно-распорядительной документации у Оператора;
- предоставление экспертных консультаций и рекомендаций сотрудникам, участвующим в обработке и обеспечении безопасности персональных данных (далее - ПДн) у Оператора, по вопросам использования средств защиты информации;
- хранение эталонного программного обеспечения средств защиты информации;
- ведение учета носителей ПДн и обеспечение их безопасного уничтожения согласно принятым у Оператора Регламентом по учёту, хранению и уничтожению носителей персональных данных;
- контроль обслуживания, настройки и ремонта средств обработки и средств защиты ПДн;
- сопровождение и контроль сторонних организаций (подрядчиков) в случае привлечения их для обслуживания, настройки и ремонта средств обработки и средств защиты ПДн;
- настройка конфигураций средств защиты информации, используемых для обеспечения безопасности ПДн;
- предоставление необходимой информации при проведении проверок уполномоченными органами и при проведении контрольных мероприятий по защите ПДн;
- реагирование на инциденты информационной безопасности, связанные с обработкой и обеспечением безопасности ПДн;
- участие во взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;
- информирование в порядке, определенном федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, о компьютерных инцидентах, повлекших неправомерную передачу (предоставление, распространение, доступ) персональных данных;
- уведомление уполномоченного органа по защите прав субъектов персональных данных о факте неправомерной или случайной передаче (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных;
- в случае нарушения требований к защите персональных данных принимать необходимые меры по восстановлению нарушенных прав субъектов персональных данных.»

1.2. добавить в раздел 3.2 следующего содержания:

«Работник, имеющий доступ к персональным данным Работников, обязан:
- соблюдать и исполнять требования Положения о порядке хранения и защиты персональных данных работников и законодательства РФ в области персональных данных, в том числе, относящиеся к обязанностям Работодателя, действуя от его имени;
- сохранять конфиденциальность персональных данных, полученных в связи с исполнением своих трудовых обязанностей;
- не отвечать на вопросы, связанные с передачей персональных данных других Работников третьим лицам, по телефону или электронной почте, если это не связано с исполнением трудовых обязанностей;
- незамедлительно сообщать своему непосредственному руководителю или лицу, ответственному за организацию обработки персональных данных у Работодателя, обо всех фактах нарушения конфиденциальности персональных данных или об

обстоятельствах, создающих угрозу их разглашения, в том числе, об утрате (хищении) материальных носителей персональных данных (бумажных документов, дисков, флэш-накопителей и др.)».

2. Изменения в трудовой договор, определенные настоящим дополнительным соглашением, вступают в силу с 25 декабря 2024 года.

3. Настоящее дополнительное соглашение является неотъемлемой частью трудового договора, составлено в двух экземплярах, имеющих одинаковую юридическую силу. Один экземпляр хранится у Работодателя, второй - у Работника.

Работодатель врио директора

Копылов В.Н.

М.П.

Работник

Воложанинов К.А.

подпись

Расшифровка подписи

Оформленный экземпляр дополнительного соглашения к договору получил:

«25» 12 2024г.