



Городской округ
«Закрытое административно – территориальное образование
Железногорск Красноярского края»

АДМИНИСТРАЦИЯ ЗАТО г.ЖЕЛЕЗНОГОРСК

РАСПОРЯЖЕНИЕ

23.12. 2022

№ 497пр

г.Железногорск

О внесении изменений в распоряжение Администрации ЗАТО г. Железногорск от 30.06.2014 № 132пр «Об утверждении документов по безопасности информационных систем персональных данных Администрации ЗАТО г. Железногорск»

Во исполнение «Требований к защите персональных данных при их обработке в информационных системах персональных данных», утвержденных постановлением Правительства Российской Федерации от 01.11.2012 г. № 1119,

1. Внести следующие изменения в распоряжение Администрации ЗАТО г. Железногорск от 30.06.2014 № 132пр «Об утверждении документов по безопасности информационных систем персональных данных Администрации ЗАТО г. Железногорск»:

1.1. Приложение № 1 «Перечень персональных данных, обрабатываемых в информационных системах персональных данных Администрации ЗАТО г. Железногорск» изложить в новой редакции (Приложение № 1);

1.2. Приложение № 2 «Перечень информационных систем персональных данных Администрации ЗАТО г. Железногорск» изложить в новой редакции (Приложение № 2);

1.3. Приложение № 3 «Акт установления уровня защищенности персональных данных при их обработке в информационных системах персональных данных Администрации ЗАТО г. Железногорска» изложить в новой редакции (Приложение № 3);

1.4. Приложение № 4 «Положение по обработке персональных данных в Администрации ЗАТО г. Железногорска» изложить в новой редакции (Приложение № 4);

1.5. Приложение № 8 «Инструкция ответственного за обработку персональных данных в информационных системах персональных данных Администрации ЗАТО г. Железногорска» изложить в новой редакции (Приложение № 5);

1.6. Приложение № 9 «Инструкция администратора безопасности информационных систем персональных данных Администрации ЗАТО г. Железногорска» изложить в новой редакции (Приложение № 6);

1.7. Приложение № 10 «Инструкция пользователя информационных систем персональных данных Администрации ЗАТО г. Железногорска» изложить в новой редакции (Приложение № 7);

1.8. Приложение № 11 «Инструкция по организации парольной защиты в информационных системах персональных данных Администрации ЗАТО г. Железногорска» изложить в новой редакции (Приложение № 8);

1.9. Приложение № 12 «Инструкция по организации антивирусного контроля в информационных системах персональных данных Администрации ЗАТО г. Железногорска» изложить в новой редакции (Приложение № 9);

1.10. Приложение № 15 «Положение о разрешительной системе доступа в информационных системах персональных данных Администрации ЗАТО г. Железногорска» изложить в новой редакции (Приложение № 10);

2. Контроль над исполнением настоящего распоряжения возложить на заместителя Главы ЗАТО г. Железногорск по общественно-политической работе А.В. Калинина.

3. Настоящее распоряжение вступает в силу с момента его подписания.

Глава ЗАТО г. Железногорск



И. Г. Куксин

Приложение № 1
к распоряжению Администрации
ЗАТО г. Железногорск
от 23.12 2022 № 497пр

Приложение № 1
к распоряжению Администрации
ЗАТО г. Железногорск
от 30.06.2014 № 132пр

ПЕРЕЧЕНЬ

персональных данных, обрабатываемых в информационных системах
персональных данных Администрации ЗАТО г. Железногорск

Персональные данные, обрабатываемые в информационной системе
персональных данных «АРМ «Общественная приемная»:

- фамилия, имя, отчество;
- почтовый адрес;
- номер телефона;
- льготный состав;
- социальное положение.

Персональные данные, обрабатываемые в информационной системе
персональных данных «Гаражи и усадьбы»:

- фамилия, имя, отчество;
- место жительства;
- адрес гаража.

Персональные данные, обрабатываемые в информационной системе
персональных данных «Кадры»:

- фамилия, имя, отчество;
- дата рождения;
- место рождения;
- пол;
- гражданство;
- знание иностранного языка;
- семейное положение;
- сведения о членах семьи (степень родства, Ф.И.О., дата рождения);

- паспортные данные (серия, номер, кем и когда выдан);
- номер телефона;
- номер мобильного телефона;
- адрес электронной почты;
- адрес места жительства по паспорту;
- адрес места жительства фактический;
- сведения об образовании;
- сведения о воинском учете;
- сведения о приеме на работу и переводе на другую работу;
- сведения об аттестации;
- сведения о повышении квалификации;
- стаж работы;
- сведения о командировках;
- классный чин;
- идентификационный номер налогоплательщика;
- свидетельство обязательного пенсионного страхования.

Персональные данные, обрабатываемые в информационной системе персональных данных «АРМ «ЖФСИ»:

- фамилия, имя, отчество;
- адрес;
- сведения о доходах;
- дата рождения;
- паспортные данные (серия, номер, кем и когда выдан);
- состав семьи;
- место работы.

Персональные данные, обрабатываемые в информационной системе персональных данных «АРМ «Договора»:

- фамилия, имя, отчество;
- адрес;
- № договора купли-продажи, аренды.

Персональные данные, обрабатываемые в информационной системе персональных данных «АРМ «Административная комиссия»:

- фамилия, имя, отчество;
- место работы;
- рабочий телефон;
- место прописки;
- адрес фактического проживания;
- дата рождения;
- место рождения;
- номер статьи.

Персональные данные, обрабатываемые в информационной системе персональных данных «Муниципальный регистр»:

- фамилия, имя, отчество;
- пол;
- дата рождения;
- национальность;
- гражданство;
- адреса (места регистрации, места рождения, места фактического проживания места временной регистрации);
- документы (основные документы, удостоверяющие личность);
- работа (сведения о различных местах работы);
- образование (сведения о типах учебных заведениях, полученных специальностях по образованию, датах поступления и окончания учебных заведений);
- сведения о родителях (привязка данных ребенка к данным о его родителях);
- дополнительная информация:
- социальный статус;
- семейное положение;
- тип образования;
- владение иностранными языками.

Персональные данные, обрабатываемые в информационной системе персональных данных «АИСТ»:

ПДн ребенка:

- фамилия, имя, отчество;
- пол;
- дата рождения;
- гражданство;
- место жительства и (или) место нахождения;
- приметы (рост, вес, цвет глаз, волос, другие приметы);
- состояние здоровья, физическое и умственное развитие;
- особенности характера (общительный, замкнутый и другие особенности);
- этническое происхождение;
- причины отсутствия родительского попечения.

ПДн родителей:

- фамилия, имя, отчество;
- дата рождения;
- гражданство;
- место жительства и (или) место нахождения;
- принадлежность к определенной религии и культуре;
- состояние здоровья.

ПДн несовершеннолетних братьев и сестер:

- фамилия, имя, отчество;
- пол;
- дата рождения;
- состояние здоровья;
- место жительства и (или) место нахождения.

ПДн совершеннолетних родственников:

- фамилия, имя, отчество;
- дата рождения;
- место жительства и (или) место нахождения;
- реквизиты документов, подтверждающих отказ принять ребенка на воспитание в свои семьи.

ПДн опекуна:

- фамилия, имя, отчество;
- пол;
- дата рождения;
- место рождения;
- гражданство;
- семейное положение;
- место жительства и (или) место нахождения;
- номер контактного телефона;
- реквизиты документа удостоверяющего личность;
- реквизиты заключения органа опеки и попечительства.

Персональные данные, обрабатываемые в информационной системе персональных данных «Личный кабинет сайта Администрации»:

- фамилия, имя, отчество;
- дата рождения
- почтовый адрес;
- номер телефона;
- реквизиты документа удостоверяющего личность;
- адрес электронной почты.

Приложение № 2
к распоряжению Администрации
ЗАТО г. Железногорск
от 23.12. 2022 № 497 пр

Приложение № 2
к распоряжению Администрации
ЗАТО г. Железногорск
от 30.06.2014 № 132 пр

ПЕРЕЧЕНЬ
информационных систем персональных данных Администрации ЗАТО г. Железногорск

№ п/п	Наименование ИСПДн	Исходные данные для установления уровня защищенности персональных данных (далее ПДн) в информационных системах персональных данных (далее ИСПДн)				Уровень защищеннос ти ПДн в ИСПДн
		Категория обрабатываемых ПДн	Принадлежность обрабатываемых ПДн	Показатель объема обрабатываемых ПДн	Тип актуальных угроз для ИСПДн	
1	«АРМ «Общественная приемная»	Иные ПДн	ПДн субъектов, не являющихся сотрудниками оператора	менее 100 000	3-й	УЗ-4
2	«Кадры»	Иные ПДн	ПДн субъектов, являющихся сотрудниками оператора	менее 100 000	3-й	УЗ-4

№ п/п	Наименование ИСПДн	Исходные данные для установления уровня защищенности персональных данных (далее ПДн) в информационных системах персональных данных (далее ИСПДн)				Уровень защищенности ПДн в ИСПДн
		Категория обрабатываемых ПДн	Принадлежность обрабатываемых ПДн	Показатель объема обрабатываемых ПДн	Тип актуальных угроз для ИСПДн	
3	«Гаражи и усадьбы»	Иные ПДн	ПДн субъектов, не являющихся сотрудниками оператора	менее 100 000	3-й	УЗ-4
4	«АРМ «Административная комиссия»	Иные ПДн	ПДн субъектов, не являющихся сотрудниками оператора	менее 100 000	3-й	УЗ-4
5	«АРМ «Договора»	Иные ПДн	ПДн субъектов, не являющихся сотрудниками оператора	менее 100 000	3-й	УЗ-4
6	«АРМ «ЖФСИ»	Иные ПДн	ПДн субъектов, не являющихся сотрудниками оператора	менее 100 000	3-й	УЗ-4
7	«Муниципальный регистр»	Иные ПДн	ПДн субъектов, не являющихся сотрудниками оператора	менее 100 000	3-й	УЗ-4
8	«АИСТ»	Специальные ПДн	ПДн субъектов, не являющихся сотрудниками оператора	менее 100 000	3-й	УЗ-3
9	«Личный кабинет сайта Администрации»	Иные ПДн	ПДн субъектов, не являющихся сотрудниками оператора	менее 100 000	3-й	УЗ-4

Приложение № 3
к распоряжению Администрации
ЗАТО г. Железногорск
от 23.12 2022 № 497 пр

Приложение № 3
к распоряжению Администрации
ЗАТО г. Железногорск
от 30.06.2014 № 132 пр

АКТ

установления уровня защищенности персональных данных при их обработке
в информационных системах персональных данных
Администрации ЗАТО г. Железногорск

Комиссия, назначенная распоряжением «Об установлении уровня защищенности персональных данных в информационных системах персональных данных Администрации ЗАТО г. Железногорск» от 27.07.2022 № 280пр, в составе:

Председатель комиссии:

Калинин А. В.

Заместитель Главы ЗАТО г. Железногорск по
общественно-политической работе

Члены комиссии:

Архипов В. А.

Заведующий отдела информационно-
технологического, организационного обеспечения
и связи

Доколин Д.В.

Системный администратор (администратор баз
данных) отдела информационно-
технологического, организационного обеспечения
и связи

Новиков А.В.

Системный администратор (администратор баз
данных) отдела информационно-
технологического, организационного обеспечения
и связи

установила, что:

1. В информационной системе персональных данных (далее – ИСПДн) «АРМ «Общественная приемная» обрабатываются следующие персональные данные:

– фамилия, имя, отчество;

- почтовый адрес;
- номер телефона;
- льготный состав;
- социальное положение.

В ИСПДн «Гаражи и усадьбы» обрабатываются следующие персональные данные:

- фамилия, имя, отчество;
- место жительства;
- адрес гаража.

В ИСПДн «Кадры» обрабатываются следующие персональные данные:

- фамилия, имя, отчество;
- дата рождения;
- место рождения;
- пол;
- гражданство;
- знание иностранного языка;
- семейное положение;
- сведения о членах семьи (степень родства, Ф.И.О., дата рождения);
- паспортные данные (серия, номер, кем и когда выдан);
- номер телефона;
- номер мобильного телефона;
- адрес электронной почты;
- адрес места жительства по паспорту;
- адрес места жительства фактический;
- сведения об образовании;
- сведения о воинском учете;
- сведения о приеме на работу и переводе на другую работу;
- сведения об аттестации;
- сведения о повышении квалификации;
- стаж работы;
- сведения о командировках;
- классный чин;
- идентификационный номер налогоплательщика;
- свидетельство обязательного пенсионного страхования.

В ИСПДн «АРМ «ЖФСИ» обрабатываются следующие персональные данные:

- фамилия, имя, отчество;
- адрес;
- сведения о доходах;
- дата рождения;

- паспортные данные (серия, номер, кем и когда выдан);
- состав семьи;
- место работы.

В ИСПДн «АРМ «Договора» обрабатываются следующие персональные данные:

- фамилия, имя, отчество;
- адрес;
- № договора купли-продажи, аренды.

В ИСПДн «АРМ «Административная комиссия» обрабатываются следующие персональные данные:

- фамилия, имя, отчество;
- место работы;
- рабочий телефон;
- место прописки;
- адрес фактического проживания;
- дата рождения;
- место рождения;
- номер статьи.

В ИСПДн «Муниципальный регистр» обрабатываются следующие персональные данные:

- фамилия, имя, отчество;
- пол;
- дата рождения;
- национальность;
- гражданство;
- адреса (места регистрации, места рождения, места фактического проживания места временной регистрации);
- документы (основные документы, удостоверяющие личность);
- работа (сведения о различных местах работы);
- образование (сведения о типах учебных заведениях, полученных специальностях по образованию, датах поступления и окончания учебных заведений);
- сведения о родителях (привязка данных ребенка к данным о его родителях);
- дополнительная информация:
- социальный статус;
- семейное положение;
- тип образования;
- владение иностранными языками.

В ИСПДн «АИСТ» обрабатываются следующие персональные данные:

ПДн ребенка:

- фамилия, имя, отчество;
- пол;
- дата рождения;
- гражданство;
- место жительства и (или) место нахождения;
- приметы (рост, вес, цвет глаз, волос, другие приметы);
- состояние здоровья, физическое и умственное развитие;
- особенности характера (общительный, замкнутый и другие особенности);
- этническое происхождение;
- причины отсутствия родительского попечения.

ПДн родителей:

- фамилия, имя, отчество;
- дата рождения;
- гражданство;
- место жительства и (или) место нахождения;
- принадлежность к определенной религии и культуре;
- состояние здоровья.

ПДн несовершеннолетних братьев и сестер:

- фамилия, имя, отчество;
- пол;
- дата рождения;
- состояние здоровья;
- место жительства и (или) место нахождения.

ПДн совершеннолетних родственников:

- фамилия, имя, отчество;
- дата рождения;
- место жительства и (или) место нахождения;
- реквизиты документов, подтверждающих отказ принять ребенка на воспитание в свои семьи.

ПДн опекуна:

- фамилия, имя, отчество;
- пол;
- дата рождения;
- место рождения;
- гражданство;
- семейное положение;
- место жительства и (или) место нахождения;
- номер контактного телефона;
- реквизиты документа удостоверяющего личность;

реквизиты заключения органа опеки и попечительства.

В ИСПДн «Личный кабинет сайта Администрации» обрабатываются следующие персональные данные:

- фамилия, имя, отчество;
- дата рождения
- почтовый адрес;
- номер телефона;
- реквизиты документа удостоверяющего личность;
- адрес электронной почты.

2. Каждая из ИСПДн «АРМ «Общественная приемная», «Гаражи и усадьбы», «Кадры», «АРМ «ЖФСИ», «АРМ «Договора», «АРМ «Административная комиссия», и «Муниципальный регистр», «Личный кабинет сайта Администрации» является информационной системой, обрабатывающей **иные категории** персональных данных, т.е. ИСПДн не осуществляет обработку специальных категорий персональных данных, а также биометрических или общедоступных персональных данных.

3. ИСПДн «АИСТ» является информационной системой, обрабатывающей **специальные категории** персональных данных, ИСПДн не осуществляет обработку биометрических или общедоступных персональных данных.

4. Каждая из ИСПДн «АРМ «Общественная приемная», «Гаражи и усадьбы», «АРМ «ЖФСИ», «АРМ «Договора», «АРМ «Административная комиссия», «Муниципальный регистр», «АИСТ» и «Личный кабинет сайта Администрации» является информационной системой, обрабатывающей **персональные данные субъектов, не являющихся сотрудниками** Администрации ЗАТО г. Железногорск.

ИСПДн «Кадры» является информационной системой, обрабатывающей **персональные данные сотрудников** Администрации ЗАТО г. Железногорск.

5. Для каждой из ИСПДн «АРМ «Общественная приемная», «Гаражи и усадьбы», «Кадры», «АРМ «ЖФСИ», «АРМ «Договора», «АРМ «Административная комиссия», «Муниципальный регистр», «АИСТ», «Личный кабинет сайта Администрации» **актуальны угрозы 3-го типа**, т.е. угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

6. Каждая из ИСПДн «АРМ «Общественная приемная», «Гаражи и усадьбы», «Кадры», «АРМ «ЖФСИ», «АРМ «Договора», «АРМ «Административная комиссия», «Муниципальный регистр», «АИСТ», «Личный кабинет сайта Администрации» обрабатывает персональные данные **менее чем 100 000 субъектов**.

Комиссия установила, что в соответствии с пунктом «б» части 12 «Требований к защите персональных данных при их обработке в информационных системах персональных данных», утвержденных Постановлением Правительства РФ от 1 ноября 2012 г. № 1119, в информационных системах персональных данных «АРМ «Общественная приемная», «Гаражи и усадьбы», «Кадры», «АРМ «ЖФСИ», «АРМ «Договора», «АРМ «Административная комиссия», «Муниципальный регистр», «Личный кабинет сайта Администрации» Администрации ЗАТО г. Железногорск должен быть обеспечен 4-й уровень защищенности (УЗ-4) персональных данных.

ИСПДн «АИСТ» Администрации ЗАТО г. Железногорск должен быть обеспечен 3-й уровень защищенности (УЗ-3) персональных данных.

Решение об установления уровня защищенности по ИСПДн «Муниципальный регистр» принято на основе «Аттестата соответствия объекта информатизации система персональных данных «Муниципальный регистр» Администрации ЗАТО г. Железногорск требованиям безопасности информации» №0557.02690.2021, выданного 13.12.2021. Аттестация произведена АО «РТК-Сибирь».

Решение об установлении уровня защищенности по ИСПДн «АИСТ» принято на основе «Аттестата соответствия информационной системы «АИСТ» требованиям безопасности информации» №8086.0-АА/21-П, выданного 06.07.2021, действительного до 06.07.2024. Аттестация произведена АО «Калуга Астрал».

Председатель комиссии:

Заместитель Главы ЗАТО г. Железногорск
по общественно-политической работе

Калинин А. В.

Члены комиссии:

Заведующий отдела информационно-технологического, организационного обеспечения и связи

Архипов В. А.

Системный администратор (администратор баз данных) отдела информационно-технологического, организационного обеспечения и связи

Доколин Д.В.

Системный администратор (администратор баз данных) отдела информационно-технологического, организационного обеспечения и связи

Новиков А.В.

Приложение № 4
к распоряжению Администрации
ЗАТО г. Железногорск
от 23.12. 2022 № 497 пр

Приложение № 4
к распоряжению Администрации
ЗАТО г. Железногорск
от 30.06.2014 № 132 пр

Положение по обработке персональных данных в Администрации ЗАТО г. Железногорск

1 Общие положения

Настоящее положение разработано в соответствии с Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» (далее Федеральный закон), Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и приказом ФСТЭК России 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».

Под информационной системой персональных данных (ИСПДн) понимается совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Под персональными данными (ПДн) понимается любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Под оператором понимается муниципальный орган самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Под обработкой ПДн понимается любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение,

предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Настоящее положение определяет состав, цели и порядок обработки ПДн, права субъектов ПДн, обязанности и ответственность оператора, перечень структурных подразделений организации, обрабатывающих ПДн, порядок реагирования на инциденты, связанные с нарушением правил обработки ПДн, и порядок взаимодействия с контролирующими органами.

2 Цели обработки ПДн

Целями обработки ПДн в ИСПДн Администрации ЗАТО г. Железногорск является: обеспечение органов государственной власти, органов местного самоуправления, физических и юридических лиц достоверными сведениями, необходимыми для осуществления, градостроительной, инвестиционной и иной хозяйственной деятельности; проведения землеустройства; учета поступления средств в бюджет ЗАТО Железногорск по возмездным договорам; начисление и выплата заработной платы сотрудникам, исчисление и уплата страховых взносов в пенсионный фонд Российской Федерации на обязательное пенсионное страхование, в фонд социального страхования Российской Федерации на случай временной нетрудоспособности в связи с материнством в Федеральный фонд обязательного медицинского страхования и территориальные фонды обязательного медицинского страхования; учет поступивших обращений, предложений, заявлений, жалоб граждан; организации работы по ведению государственного банка данных о детях, оставшихся без попечения родителей, а также тех, кто желает принять детей на воспитание в свои семьи и передаче этих сведений на региональный уровень; обеспечение функционирования Государственной системы регистрации (учета) избирателей, участников референдума; обеспечение соблюдения законных прав и интересов Администрации ЗАТО г. Железногорск и ее работников в связи с необходимостью получения (сбора), систематизации (комбинирования), хранения и передачи сведений, составляющих персональные данные.

3 Состав ПДн

В информационных системах персональных данных Администрации ЗАТО г. Железногорск обрабатываются следующие ПДн:

- фамилия;
- имя;
- отчество;
- почтовый адрес;
- номер телефона;
- номер мобильного телефона;
- льготный состав;
- социальное положение (статус);
- дата рождения;
- идентификационный номер налогоплательщика;

- свидетельство обязательного пенсионного страхования;
- номер лицевого счета в банке;
- паспортные данные (серия, номер, кем и когда выдан);
- наличие детей;
- адрес гаража;
- пол;
- гражданство;
- знание иностранного языка;
- национальность;
- семейное положение;
- сведения о членах семьи (степень родства, Ф.И.О., дата рождения);
- адрес электронной почты;
- адрес места жительства по паспорту;
- адрес места жительства фактический;
- сведения об образовании;
- сведения о воинском учете;
- сведения о приеме на работу и переводе на другую работу;
- сведения об аттестации;
- сведения о повышении квалификации;
- стаж работы;
- сведения о командировках;
- классный чин;
- сведения о доходах;
- номер договора купли-продажи, аренды жилья.
- номер статьи административного правонарушения;
- приметы (рост, вес, цвет глаз, волос и другие);
- состояние здоровья, физическое и умственное развитие;
- особенности характера (общительный, замкнутый и другие);
- этническое происхождение;
- причины отсутствия родительского попечения;
- принадлежность к определенной религии и культуре;
- состояние здоровья;
- реквизиты документов, подтверждающих отказ принять ребенка на воспитание;
- реквизиты заключения органа опеки и попечительства.

4 Обработка ПДн

4.1 Порядок обработки ПДн

Получение ПДн может осуществляться как путем их представления Оператору самим субъектом, так и путем получения персональных данных Оператором из иных источников, в том случае, если ПДн представляется возможным получить только у третьей стороны. Если персональные данные

субъекта получены не от субъекта персональных данных и такое получение не предусмотрено в пункте 4 статьи 18 Федерального закона, то субъекту направляется соответствующее уведомление, согласно пункту 3 статьи 18 Федерального закона.

Оператор не имеет права получать и обрабатывать ПДн субъекта не связанные с целями обработки ПДн. В случаях, непосредственно связанных с вопросами трудовых отношений данные о частной жизни субъекта (информация о жизнедеятельности в сфере семейных бытовых, личных отношений) могут быть получены и обработаны оператором только с письменного согласия субъекта.

Сроки обработки персональных данных должны ограничиваться достижением конкретных, заранее определенных и законных целей.

4.2 Хранение ПДн

После достижения цели обработки персональных данных, если это предусмотрено федеральными законами, нормативными актами или в письменном согласии субъекта персональных данных, персональные данные помещаются в архив и хранятся в течение срока, установленного законодательством РФ. На хранение персональных данных в электронном архиве должно быть получено согласие субъекта.

Если в течение срока архивного хранения, субъект персональных данных направил в адрес оператора заявление об отзыве согласия на обработку персональных данных, оператор обязан по истечении срока архивного хранения уничтожить персональные данные субъекта с составлением соответствующего акта.

4.3 Передача ПДн

Передача ПДн субъекта любым физическим или юридическим лицам может быть осуществлена только с письменного согласия субъекта ПДн, если иное не предусмотрено законодательством РФ.

4.4 Уничтожение ПДн

Уничтожение ПДн осуществляется по истечении соответствующего срока хранения. Для уничтожения персональных данных создается комиссия, которая проводит уничтожение ПДн и составляет соответствующие акты.

Носители, содержащие ПДн, уничтожаются путем сдачи предприятию по утилизации вторичного сырья (на основании договора) или таким способом, что после процедуры уничтожения не представится возможным восстановить данные. По результатам уничтожения составляется акт об уничтожении ПДн, который подписывается комиссией, созданной для уничтожения ПДн. После уничтожения оператор уведомляет об этом субъекта ПДн.

5 Права субъекта ПДн

Субъект ПДн имеет право на получение информации, касающейся обработки его ПДн, в том числе содержащей:

- подтверждение факта обработки ПДн оператором;
- правовые основания и цели обработки ПДн;
- цели и применяемые оператором способы обработки ПДн;
- наименование и место нахождения оператора, сведения о лицах, которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с оператором или на основании федерального закона;
- обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;
- сроки обработки ПДн, в том числе сроки их хранения;
- порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом;
- информацию об осуществленной или о предполагаемой передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению оператора, если обработка поручена или будет поручена такому лицу.

6 Обязанности оператора

Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных законодательством РФ и принятыми в соответствии с ним нормативными правовыми актами. К таким мерам относятся:

- назначение оператором ответственного за обработку ПДн;
- издание оператором документов, определяющих политику оператора в отношении обработки ПДн, локальных актов по вопросам обработки ПДн, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;
- применение правовых, организационных и технических мер по обеспечению безопасности ПДн;
- осуществление внутреннего контроля и (или) аудита соответствия обработки ПДн законодательству Российской Федерации и принятым в соответствии с ним нормативным правовым актам, требованиям к защите ПДн, политике оператора в отношении обработки ПДн, локальным актам оператора;
- ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства РФ о ПДн, в том числе требованиями к защите ПДн, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки ПДн, и (или) обучение указанных работников.

В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных или его представителя либо по запросу субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки. В случае выявления неточных персональных данных при обращении субъекта персональных данных или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных оператор обязан осуществить блокирование персональных данных, относящихся к этому субъекту персональных данных, или обеспечить их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

В случае подтверждения факта неточности персональных данных оператор на основании сведений, представленных субъектом персональных данных или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов обязан уточнить персональные данные либо обеспечить их уточнение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

В случае выявления неправомерной обработки ПДн, осуществляемой оператором или лицом, действующим по поручению оператора, оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку ПДн или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора. В случае, если обеспечить правомерность обработки ПДн невозможно, оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки ПДн, обязан уничтожить такие ПДн или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта ПДн или его представителя, а в случае, если обращение субъекта ПДн или его представителя либо запрос уполномоченного органа по защите прав субъектов ПДн были направлены уполномоченным органом по защите прав субъектов ПДн, также указанный орган.

В случае достижения цели обработки ПДн оператор обязан прекратить обработку ПДн или обеспечить ее прекращение (если обработка ПДн осуществляется другим лицом, действующим по поручению оператора) и уничтожить ПДн или обеспечить их уничтожение (если обработка ПДн

осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки ПДн, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн, иным соглашением между оператором и субъектом ПДн, либо если оператор не вправе осуществлять обработку ПДн без согласия субъекта ПДн на основаниях, предусмотренных законодательством Российской Федерации.

В случае отзыва субъектом персональных данных согласия на обработку его персональных данных оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами.

В случае обращения субъекта персональных данных к оператору с требованием о прекращении обработки персональных данных оператор обязан в срок, не превышающий десяти рабочих дней с даты получения оператором соответствующего требования, прекратить их обработку или обеспечить прекращение такой обработки (если такая обработка осуществляется лицом, осуществляющим обработку персональных данных), за исключением случаев, предусмотренных пунктами 2 - 11 части 1 статьи 6, частью 2 статьи 10 и частью 2 статьи 11 Федерального закона. Указанный срок может быть продлен, но не более чем на пять рабочих дней в случае направления оператором в адрес субъекта персональных данных мотивированного уведомления с указанием причин продления срока предоставления запрашиваемой информации.

В случае отсутствия возможности уничтожения персональных данных в течение срока, в частях 3-5 пункта 7 статьи 21 Федерального закона, оператор осуществляет блокирование таких персональных данных или обеспечивает их блокирование (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

7 Перечень ИСПДн Администрации ЗАТО г. Железногорск, обрабатывающих ПДн

Обработка ПДн осуществляется в следующих ИСПДн:

- «АРМ «Общественная приемная»;
- «Гаражи и усадьбы»;
- «Кадры»;
- «АРМ «ЖФСИ»;
- «АРМ «Договора»;
- «АРМ «Административная комиссия»;
- «Муниципальный регистр»;
- «АИСТ»;
- «Личный кабинет сайта Администрации».

8 Порядок реагирования на инциденты, связанные с нарушением правил обработки ПДн

Под инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а так же потерей защищаемой информации.

Происшествие, вызывающее инцидент, может произойти:

- в результате непреднамеренных действий сотрудников организации - оператора;
- в результате преднамеренных действий пользователей и третьих лиц;
- в результате нарушения правил эксплуатации технических средств ИСПДн;
- в результате возникновения нештатных ситуаций и обстоятельств непреодолимой силы.

По каждому инциденту проводится расследование.

Для проведения расследования назначается комиссия. Комиссия обязана установить, имела ли место утечка сведений, и обстоятельства ей сопутствующие, установить лиц, виновных в нарушении предписанных мероприятий по защите информации, установить причины и условия, способствовавшие нарушению, и выработать рекомендации по их устранению. После окончания расследования председатель комиссии выносит на рассмотрение решение о наказании виновных лиц и необходимых мероприятиях по устранению выявленных недостатков.

9 Порядок взаимодействия с контролирующими органами

Периодический контроль состояния защиты информации осуществляется Федеральной службой по техническому и экспортному контролю России в соответствии с действующим законодательством Российской Федерации. Доступ представителя указанного федерального органа исполнительной власти на объекты для проведения проверки, а также к работам и документам в объеме, необходимом для осуществления контроля, обеспечивается в установленном порядке по предъявлении служебного удостоверения сотрудника, а также предписания установленной формы на право проведения проверки.

10 Ответственность

Персональные данные не подлежат разглашению (распространению). Прекращение доступа к такой информации не освобождает сотрудника Оператора от взятых им обязательств по неразглашению сведений ограниченного распространения. За разглашение информации ограниченного распространения, нарушение порядка работы с документами или машинными носителями, содержащими такую информацию, сотрудник Оператора может быть привлечен к дисциплинарной, административной или иной, предусмотренной законодательством Российской Федерации ответственности.

Приложение № 5
к распоряжению Администрации
ЗАТО г. Железнодорожск
от 23.12. 2022 № 497пр

Приложение № 8
к распоряжению Администрации
ЗАТО г. Железнодорожск
от 30.06.2014 № 132 пр

ИНСТРУКЦИЯ

ответственного за обработку персональных данных в информационных системах
персональных данных Администрации ЗАТО г. Железнодорожск

1. Общие положения

Настоящая инструкция является руководящим документом ответственного за обработку персональных данных (ПДн) в информационных системах персональных данных (ИСПДн) «Гаражи и усадьбы», «Кадры», «АРМ «Административная комиссия», «АРМ «Договора», «АРМ «ЖФСИ», «АРМ «Общественная приемная», «Муниципальный регистр», «АИСТ», «Личный кабинет сайта Администрации» Администрации ЗАТО г. Железногорск.

Требования ответственного за обработку ПДн, связанные с выполнением им своих функций, обязательны для исполнения всеми пользователями ИСПДн и администратором безопасности.

Ответственный за обработку ПДн назначается распоряжением руководства из числа сотрудников, профессиональные навыки и знание нормативной базы по защите информации которых, позволяют выполнять возложенные на него обязанности.

Ответственный за обработку ПДн отвечает за обеспечение устойчивой работоспособности и информационной безопасности объектов вычислительной техники (ОВТ), входящих в состав ИСПДн при обработке персональных данных.

Ответственный за обработку ПДн должен быть ознакомлен под личную подпись с настоящей инструкцией (лист ознакомления) и предупрежден о возможной ответственности за ее нарушение.

2. Функции ответственного за обработку ПДн

В своей деятельности ответственный за обработку ПДн руководствуется данной инструкцией и другими документами, регламентирующими защиту ПДн в организации.

Ответственный за обработку ПДн:

2.1. Контролирует работу администратора безопасности.

2.2. Доводит до сотрудников организации, имеющих доступ к персональным данным, положения и требования нормативных и правовых актов по обработке персональных данных, в частности:

2.2.1. Федеральный закон № 152-ФЗ от 27.07.2006 «О персональных данных»,

2.2.2. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»,

2.2.3. Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

2.3. Обеспечивает выполнение сотрудниками принятых в организации инструкций, распоряжений, положений и других документов по защите ПДн.

2.4. Контролирует доступ пользователей к работе в ИСПДн в соответствии со списком работников, допущенных к работе с персональными данными ИСПДн (постоянно или временно).

3. Права и обязанности ответственного за обработку ПДн

На ответственного за обработку ПДн возлагаются следующие обязанности:

- следить за действиями специалистов организаций, оказывающих услуги аутсорсинга, при их работе в ИСПДн (включая монтажные и пусконаладочные работы оборудования или средств защиты информации);
- принимать решение о прекращении обработки ПДн в ИСПДн при несанкционированном доступе (попытках) к ним или возникновении ситуаций, послуживших причиной возможной утраты ПДн;
- информировать Главу ЗАТО г. Железногорск обо всех попытках несанкционированного доступа к ПДн, нарушения персоналом соответствующих распоряжений и инструкций, несвоевременного проведения (или не проведения вообще) пользователями и администратором безопасности разработанных мероприятий и вести работы по служебным расследованиям в случае их возникновения;
- контролировать, а в случае необходимости, корректировать работы по выбору, закупке и приемке нового программного обеспечения, средств защиты информации, технического оснащения, а также руководить работами при подборе кадрового обеспечения организации в области защиты информации;
- следить за неизменностью условий функционирования и эксплуатации ИСПДн с последующим информированием руководства в случае каких-либо изменений, руководствуясь настоящей инструкцией и другими нормативными документами по защите ПДн в организации;
- вести учет всех защищаемых носителей информации;
- подчиняться непосредственно Главе ЗАТО г. Железногорск;
- совместно с администратором безопасности доводить под личную подпись до сотрудников организации и пользователей ИСПДн содержание соответствующих инструкций, распоряжений, положений и других документов по защите ПДн;
- следить за своевременным проведением администратором безопасности необходимых регламентных работ по обеспечению безопасности ПДн при их обработке в ИСПДн с целью поддержания системы защиты информации в актуальном состоянии;
- следить за поддержанием применяемой в организации системы защиты информации в актуальном состоянии (своевременная разработка, корректировка и переиздание документов, изучение и мониторинг нормативной базы по защите ПДн) и подготавливать предложения по ее совершенствованию;

- организовывать проведение периодических проверок по соблюдению условий обработки персональных данных в Администрации ЗАТО г. Железногорск;
- проводить внутренний контроль соблюдения порядка доступа в помещения, в которых ведется обработка персональных данных;
- приостанавливать работу с информацией ограниченного распространения на ИСПДн в случае окончания срока действия сертификатов соответствия ФСТЭК России на любое СЗИ, из используемых в составе ИСПДн, до момента его продления. В случае не продления сертификата соответствия, ответственный за обеспечение безопасности ИСПДн обязан поставить в известность орган по аттестации, проводивший создание системы защиты (аттестацию) ИСПДн, для принятия совместного решения;
- вести журнал учета своей работы по обеспечению безопасности ПДн при их обработке в ИСПДн (формы журнала учета работ ответственного за обработку ПДн, журнала учета съемных носителей, журнала учета выдачи копий документов субъектам ПДн, журнала обучения и инструктажа пользователей, журнала учета проведения периодического тестирования функций системы защиты, журнала учета нештатных ситуаций, профилактических работ, установки и модификации ПО на ПЭВМ, а также бланк согласия субъекта ПДн на обработку ПДн, бланк заявления о прекращении обработки ПДн, бланк отзыва согласия обработки ПДн, бланки согласия на обработку ПДн Муниципальным казенным учреждением «Централизованная бухгалтерия», бланки поручения на обработку ПДн Муниципальным казенным учреждением «Централизованная бухгалтерия» приведены в приложении № 1).

4. Порядок действий в случае выявления нарушения информационной безопасности

В случае выявления фактов нарушений информационной безопасности ответственный за обработку ПДн принимает меры, необходимые для предотвращения негативных последствий нарушения безопасности информации при обработке информации, содержащей персональные данные и информирует непосредственное руководство о факте нарушения и принятых мерах.

Анализирует и устанавливает причины возникшего нарушения и принимает меры по предотвращению подобных нарушений в дальнейшем.

По факту нарушения составляет служебную записку на имя Главы ЗАТО г. Железногорск с указанием причин нарушения и принятых мер.

В случае создания комиссии по расследованиям причин нарушения, принимает участие в ее работе.

5. Ответственность ответственного за обработку ПДн

Ответственный за обработку ПДн несет всю полноту ответственности за качество и своевременность выполнения задач и функций, возложенных на него в соответствии с настоящей инструкцией и другими нормативными документами по защите ПДн в организации.

Ответственный за обработку ПДн, получивший доступ к ПДн, обязан хранить в тайне сведения ограниченного распространения, полученные им во время работы или иным путем и пресекать действия других лиц, которые могут привести к разглашению такой информации.

В случае оставления занимаемой должности ответственный за обработку ПДн обязан вернуть все документы и материалы, относящиеся к деятельности подразделения, организации, Главе ЗАТО г. Железногорск.

СОГЛАСИЕ
на обработку персональных данных

« ____ » _____ 20__ г.

Я, _____,

(Ф.И.О.)

_____ года рождения, документ, удостоверяющий личность
_____, серия _____ номер _____, выданный

(число, месяц, год выдачи, наименование органа, выдавшего документ)

зарегистрированный по адресу: _____,

(адрес регистрации)

в соответствии со статьей 9 Федерального закона от 27.06.2006 N 152-ФЗ «О персональных данных», (далее 152-ФЗ), Федерального закона от 02.05.2006 N 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации» даю свое согласие на обработку Администрации ЗАТО г.Железногорск, ИНН 2452012069 адрес: 662971, Красноярский край, ЗАТО Железногорск, город Железногорск, ул. «22» Партсъезда д.21 (далее – Администрация) моих персональных данных, относящихся исключительно к перечисленным ниже категориям персональных данных: фамилия; имя; отчество; пол; год, месяц дата и место рождения; адрес места жительства (регистрации), семейное положение, образование, профессия, тип документа, удостоверяющего личность; данные документа, удостоверяющего личность; гражданство; мобильный телефон; адрес электронной почты (иное) с целью:

_____ посредством использования информационного ресурса оператора по адресу: _____, с

использованием которого будут осуществляться действия с персональными данными, либо без использования такого ресурса (нужное подчеркнуть).

Настоящее согласие предоставляется мной Администрации на осуществление действий в отношении моих персональных данных, которые необходимы для достижения указанных выше целей, включая (без ограничения), сбор, обработку, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение, передачу третьим лицам для осуществления действий по обмену информацией, обезличивание, блокирование персональных данных, а также осуществление любых иных действий, предусмотренных действующим законодательством Российской Федерации. Я также даю согласие на поручение обработки персональных данных другому лицу (подведомственной организации) с соблюдением требований, установленных п. 3 ст. 6 152-ФЗ.

Источник получения персональных данных _____

Я проинформирован, что Администрация гарантирует обработку моих персональных данных в соответствии с действующим законодательством Российской Федерации:

неавтоматизированным способом _____,

автоматизированным способом _____.

Дата начала обработки персональных данных _____

Данное согласие вступает в силу со дня подписания и действует до достижения целей обработки персональных данных.

Согласие может быть отозвано на основании письменного заявления об отзыве согласия.

Основанием для прекращения обработки персональных данных является письменное требование о прекращении обработки направленное Администрации.

« ____ » _____ 20__ г.

_____/_____/

Подпись

Расшифровка подписи

СОГЛАСИЕ
на обработку персональных данных Муниципальным казенным учреждением
«Централизованная бухгалтерия»

г. Железногорск Красноярского края

« ____ » _____ 20__ года

Я, _____, зарегистрированный (ая) по адресу:

(Фамилия, Имя, Отчество)

(край, город, улица, дом, кв.)

имеющий паспорт:

(паспорт (другой документ, удостоверяющий личность) №, когда и кем выдан)

свободно, своей волей и в своем интересе даю согласие на обработку (любое действие (операцию) или совокупность действий (операций), совершаемых с использованием средств автоматизации и/или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение) Муниципальным казенным учреждением «Централизованная бухгалтерия» (ИНН 2452036006, адрес: 662972, Россия, Красноярский край, ЗАТО Железногорск, г. Железногорск, ул. Свердлова, зд. 47, помещение 4) в соответствии с «Соглашением о передаче полномочий по ведению бухгалтерского учета и составлению на его основе отчетности, ведению бюджетного учета и формированию бюджетной отчетности» от 31.12.2019 № 1 следующих персональных данных:

фамилия, имя, отчество, дата и место рождения, гражданство;

прежние фамилия, имя, отчество, дата, место и причина изменения (в случае изменения);

выполняемая работа с начала трудовой деятельности (включая военную службу, работу по совместительству, предпринимательскую деятельность);

классный чин федеральной государственной гражданской службы и (или) гражданской службы субъекта Российской Федерации и (или) муниципальной службы, дипломатический ранг, воинское и (или) специальное звание, классный чин правоохранительной службы (кем и когда присвоены);

адрес регистрации по месту жительства и адрес фактического проживания; дата регистрации по месту жительства;

паспорт (серия, номер, кем и когда выдан);

номер телефона;

отношение к воинской обязанности, сведения по воинскому учёту (для граждан, пребывающих в запасе, и лиц, подлежащих призыву на военную службу);

идентификационный номер налогоплательщика;

реквизиты документа, подтверждающего регистрацию в системе индивидуального (персонифицированного) учета;

допуск к государственной тайне, оформленный за период работы, службы, учёбы (форма, номер и дата); наличие (отсутствие) заболевания, препятствующего поступлению на федеральную государственную гражданскую службу Российской Федерации или её прохождению, подтверждённого заключением медицинского учреждения;

сведения о последнем месте государственной или муниципальной службы.

Вышеуказанные персональные данные предоставляю для обработки в целях обеспечения соблюдения в отношении меня законодательства Российской Федерации в сфере отношений, связанных с поступлением на муниципальную службу, её прохождением и прекращением (трудовых и непосредственно связанных с ними отношений) для реализации полномочий, возложенных на Муниципальное казенное учреждение «Централизованная бухгалтерия» в соответствии с «Соглашением о передаче полномочий по ведению бухгалтерского учета и составлению на его основе отчетности, ведению бюджетного учета и формированию бюджетной отчетности» от 31.12.2019 № 1.

Я ознакомлен(а) и согласен, что:

1) согласие на обработку персональных данных действует с даты подписания настоящего согласия в течение всего срока муниципальной службы в Администрации ЗАТО г. Железногорск;

2) согласие на обработку персональных данных может быть отозвано на основании письменного заявления в произвольной форме;

3) в случае отзыва согласия на обработку персональных данных Администрация ЗАТО г. Железногорск вправе продолжить обработку персональных данных без согласия при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

4) после увольнения с муниципальной службы (прекращения трудовых отношений) персональные данные хранятся в Администрации ЗАТО г. Железногорск в течение срока хранения документов, предусмотренных законодательством Российской Федерации;

5) персональные данные, предоставляемые в отношении третьих лиц, будут обрабатываться только в целях осуществления и выполнения возложенных законодательством Российской Федерации на Администрацию ЗАТО г. Железногорск функций, полномочий и обязанностей.

Дата начала обработки персональных данных: 01 января 2020 года
(число, месяц, год)

Фамилия, И.О., подпись: _____

СОГЛАСИЕ
на поручение обработки персональных данных
Муниципальным казенным учреждением «Централизованная бухгалтерия»

г. Железногорск Красноярского края

« ____ » _____ 20__ года

Я, _____, зарегистрированный (ая) по адресу:

(Фамилия, Имя, Отчество)

(край, город, улица, дом, кв.)

имеющий паспорт:

(паспорт (другой документ, удостоверяющий личность) №, когда и кем выдан)

свободно, своей волей и в своем интересе даю согласие на поручение обработки персональных данных (любое действие (операцию) или совокупность действий (операций), совершаемых с использованием средств автоматизации и/или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение) Администрацией ЗАТО г. Железногорск (ИНН 2452012069, адрес: 662971, Россия, Красноярский край, ЗАТО Железногорск, г. Железногорск, ул. 22 Партсъезда, зд. 21) Муниципальному казенному учреждению «Централизованная бухгалтерия» (ИНН 2452036006, адрес: 662972, Россия, Красноярский край, ЗАТО Железногорск, г. Железногорск, ул. Свердлова, зд. 47, помещение 4) в соответствии с «Соглашением о передаче полномочий по ведению бухгалтерского учета и составлению на его основе отчетности, ведению бюджетного учета и формированию бюджетной отчетности» от 31.12.2019 № 1.

Согласие на поручение обработки персональных данных дается в отношении следующих персональных данных:

- фамилия, имя, отчество, дата и место рождения, гражданство;
- прежние фамилия, имя, отчество, дата, место и причина изменения (в случае изменения);
- выполняемая работа с начала трудовой деятельности (включая военную службу, работу по совместительству, предпринимательскую деятельность);
- классный чин федеральной государственной гражданской службы и (или) гражданской службы субъекта Российской Федерации и (или) муниципальной службы, дипломатический ранг, воинское и (или) специальное звание, классный чин правоохранительной службы (кем и когда присвоены);
- адрес регистрации по месту жительства и адрес фактического проживания; дата регистрации по месту жительства;
- паспорт (серия, номер, кем и когда выдан);
- номер телефона;
- отношение к воинской обязанности, сведения по воинскому учёту (для граждан, пребывающих в запасе, и лиц, подлежащих призыву на военную службу);
- идентификационный номер налогоплательщика;
- реквизиты документа, подтверждающего регистрацию в системе индивидуального (персонифицированного) учета;
- допуск к государственной тайне, оформленный за период работы, службы, учёбы (форма, номер и дата);
- наличие (отсутствие) заболевания, препятствующего поступлению на федеральную государственную гражданскую службу Российской Федерации или её прохождению, подтверждённого заключением медицинского учреждения;
- сведения о последнем месте государственной или муниципальной службы.

Вышеуказанные персональные данные предоставляю для обработки в целях обеспечения соблюдения в отношении меня законодательства Российской Федерации в сфере отношений, связанных с поступлением на муниципальную службу, её прохождением и прекращением (трудовых и непосредственно связанных с ними отношений) для реализации полномочий, возложенных на Муниципальное казенное учреждение «Централизованная бухгалтерия» в соответствии с «Соглашением о передаче полномочий по ведению бухгалтерского учета и составлению на его основе отчетности, ведению бюджетного учета и формированию бюджетной отчетности» от 31.12.2019 № 1.

Я ознакомлен(а), что:

- 1) согласие на обработку персональных данных действует с даты подписания настоящего согласия в течение всего срока муниципальной службы в Администрации ЗАТО г. Железногорск;
- 2) согласие на обработку персональных данных может быть отозвано на основании письменного заявления в произвольной форме;
- 3) в случае отзыва согласия на обработку персональных данных Администрация ЗАТО г. Железногорск вправе продолжить обработку персональных данных без согласия при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

4) после увольнения с муниципальной службы (прекращения трудовых отношений) персональные данные хранятся в Администрации ЗАТО г. Железногорск в течение срока хранения документов, предусмотренных законодательством Российской Федерации;

5) персональные данные, предоставляемые в отношении третьих лиц, будут обрабатываться только в целях осуществления и выполнения возложенных законодательством Российской Федерации на Администрацию ЗАТО г. Железногорск функций, полномочий и обязанностей.

Дата начала обработки персональных данных: 01 января 2020 года
(число, месяц, год)

Фамилия, И.О., подпись: _____

СОГЛАСИЕ
на поручение обработки персональных данных
Муниципальным казенным учреждением «Централизованная бухгалтерия»

г. Железногорск Красноярского края

« ____ » _____ 20__ года

Я, _____, зарегистрированный (ая) по адресу:
(Фамилия, Имя, Отчество)

(край, город, улица, дом, кв.)

имеющий паспорт:

(паспорт (другой документ, удостоверяющий личность) №, когда и кем выдан)

свободно, своей волей и в своем интересе даю согласие на поручение обработки персональных данных (любое действие (операцию) или совокупность действий (операций), совершаемых с использованием средств автоматизации и/или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение) Администрацией ЗАТО г. Железногорск (ИНН 2452012069, адрес: 662971, Россия, Красноярский край, ЗАТО Железногорск, г. Железногорск, ул. 22 Партсъезда, зд. 21) Муниципальному казенному учреждению «Централизованная бухгалтерия» (ИНН 2452036006, адрес: 662972, Россия, Красноярский край, ЗАТО Железногорск, г. Железногорск, ул. Свердлова, зд. 47, помещение 4) в соответствии с «Соглашением о передаче полномочий по ведению бухгалтерского учета и составлению на его основе отчетности, ведению бюджетного учета и формированию бюджетной отчетности» от 31.12.2019 № 1.

Согласие на поручение обработки персональных данных дается в отношении следующих персональных данных:

- фамилия, имя, отчество, дата и место рождения, гражданство;
- прежние фамилия, имя, отчество, дата, место и причина изменения (в случае изменения);
- выполняемая работа с начала трудовой деятельности (включая военную службу, работу по совместительству, предпринимательскую деятельность);
- адрес регистрации по месту жительства и адрес фактического проживания; дата регистрации по месту жительства;
- паспорт (серия, номер, кем и когда выдан);
- номер телефона;
- отношение к воинской обязанности, сведения по воинскому учёту (для граждан, пребывающих в запасе, и лиц, подлежащих призыву на военную службу);
- идентификационный номер налогоплательщика;
- реквизиты документа, подтверждающего регистрацию в системе индивидуального (персонифицированного) учета.

Вышеуказанные персональные данные предоставляю для обработки в целях обеспечения соблюдения в отношении меня законодательства Российской Федерации в сфере трудовых и непосредственно связанных с ними отношений для реализации полномочий, возложенных на Муниципальное казенное учреждение «Централизованная бухгалтерия» в соответствии с «Соглашением о передаче полномочий по ведению бухгалтерского учета и составлению на его основе отчетности, ведению бюджетного учета и формированию бюджетной отчетности» от 31.12.2019 № 1.

Я ознакомлен(а), что:

- 1) согласие на обработку персональных данных действует с даты подписания настоящего согласия в течение всего срока муниципальной службы в Администрации ЗАТО г. Железногорск;
- 2) согласие на обработку персональных данных может быть отозвано на основании письменного заявления в произвольной форме;
- 3) в случае отзыва согласия на обработку персональных данных Администрация ЗАТО г. Железногорск вправе продолжить обработку персональных данных без согласия при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;
- 4) после увольнения с муниципальной службы (прекращения трудовых отношений) персональные данные хранятся в Администрации ЗАТО г. Железногорск в течение срока хранения документов, предусмотренных законодательством Российской Федерации;
- 5) персональные данные, предоставляемые в отношении третьих лиц, будут обрабатываться только в целях осуществления и выполнения возложенных законодательством Российской Федерации на Администрацию ЗАТО г. Железногорск функций, полномочий и обязанностей.

Дата начала обработки персональных данных: 01 января 2020 года

(число, месяц, год)

Фамилия, И.О., подпись: _____

СОГЛАСИЕ
на обработку персональных данных **Муниципальным казенным учреждением**
«Централизованная бухгалтерия»

г. Железнодорожск Красноярского края

« ____ » _____ 20__ года

Я, _____, зарегистрированный (ая) по адресу:

(Фамилия, Имя, Отчество)

(край, город, улица, дом, кв.)

имеющий паспорт:

(паспорт (другой документ, удостоверяющий личность) №, когда и кем выдан)

свободно, своей волей и в своем интересе даю согласие на обработку (любое действие (операцию) или совокупность действий (операций), совершаемых с использованием средств автоматизации и/или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение) Муниципальным казенным учреждением «Централизованная бухгалтерия» (ИНН 2452036006, адрес: 662972, Россия, Красноярский край, ЗАТО Железнодорожск, г. Железнодорожск, ул. Свердлова, зд. 47, помещение 4) в соответствии с «Соглашением о передаче полномочий по ведению бухгалтерского учета и составлению на его основе отчетности, ведению бюджетного учета и формированию бюджетной отчетности» от 31.12.2019 № 1 следующих персональных данных:

фамилия, имя, отчество, дата и место рождения, гражданство;

прежние фамилия, имя, отчество, дата, место и причина изменения (в случае изменения);

выполняемая работа с начала трудовой деятельности (включая военную службу, работу по совместительству, предпринимательскую деятельность);

адрес регистрации по месту жительства и адрес фактического проживания; дата регистрации по месту жительства;

паспорт (серия, номер, кем и когда выдан);

номер телефона;

отношение к воинской обязанности, сведения по воинскому учёту (для граждан, пребывающих в запасе, и лиц, подлежащих призыву на военную службу);

идентификационный номер налогоплательщика;

реквизиты документа, подтверждающего регистрацию в системе индивидуального (персонифицированного) учета.

Вышеуказанные персональные данные предоставляю для обработки в целях обеспечения соблюдения в отношении меня законодательства Российской Федерации в сфере трудовых и непосредственно связанных с ними отношений для реализации полномочий, возложенных на Муниципальное казенное учреждение «Централизованная бухгалтерия» в соответствии с «Соглашением о передаче полномочий по ведению бухгалтерского учета и составлению на его основе отчетности, ведению бюджетного учета и формированию бюджетной отчетности» от 31.12.2019 № 1.

Я ознакомлен(а), что:

1) согласие на обработку персональных данных действует с даты подписания настоящего согласия в течение всего срока работы в Администрации ЗАТО г. Железнодорожск;

2) согласие на обработку персональных данных может быть отозвано на основании письменного заявления в произвольной форме;

3) в случае отзыва согласия на обработку персональных данных Администрация ЗАТО г. Железнодорожск вправе продолжить обработку персональных данных без согласия при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

4) после увольнения (прекращения трудовых отношений) персональные данные хранятся в Администрации ЗАТО г. Железнодорожск в течение срока хранения документов, предусмотренных законодательством Российской Федерации;

5) персональные данные, предоставляемые в отношении третьих лиц, будут обрабатываться только в целях осуществления и выполнения возложенных законодательством Российской Федерации на Администрацию ЗАТО г. Железнодорожск функций, полномочий и обязанностей.

Дата начала обработки персональных данных: 01 января 2020 года

(число, месяц, год)

Подпись: _____

Фамилия, Имя, Отчество: _____

Приложение № 6
к распоряжению Администрации
ЗАТО г. Железногорск
от 23.12. 2022 № 497пр

Приложение № 9
к распоряжению Администрации
ЗАТО г. Железногорск
от 30.06.2014 № 132пр

ИНСТРУКЦИЯ

администратора безопасности информационных систем персональных данных
Администрации ЗАТО г. Железногорск

1 ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая инструкция является руководящим документом администратора безопасности, обеспечивающего безопасность персональных данных (далее – ПДн), обрабатываемых, передаваемых и хранимых в информационных системах персональных данных (далее – ИСПДн) «Гаражи и усадьбы», «Кадры», «АРМ «Административная комиссия», «АРМ «Договора», «АРМ «ЖФСИ», «АРМ «Общественная приемная», «Муниципальный регистр», «АИСТ», «Личный кабинет сайта Администрации» Администрации ЗАТО г. Железногорск, настройку и функционирование средств защиты информации в соответствии приказом ФСТЭК России 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», организационно-распорядительной документацией.

Требования администратора безопасности к пользователям ИСПДн, связанные с выполнением им своих функций, обязательны для исполнения всеми пользователями ИСПДн.

Администратор безопасности должен быть ознакомлен под подпись с настоящей инструкцией (лист ознакомления) и предупрежден о возможной ответственности за ее нарушение.

2 ФУНКЦИИ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

В ходе исполнения своих обязанностей администратор руководствуется данной инструкцией и другими документами, регламентирующими защиту ПДн при их обработке в ИСПДн от несанкционированного доступа (далее – НСД) к ним, а также эксплуатационной документацией на установленные средства защиты информации (далее – СЗИ).

Администратор безопасности обеспечивает поддержку в работоспособном состоянии подсистем управления доступом пользователей к ресурсам ИСПДн, регистрации и учета информационных ресурсов ИСПДн, а именно:

- реализует полномочия доступа к ресурсам ИСПДн для каждого пользователя, допущенного к работе в ней и ознакомившегося с «Инструкцией пользователя ИСПДн», на основании «Положения о разрешительной системе доступа»;
- по согласованию с Заместителем Главы ЗАТО г. Железногорск по общественно-политической работе реализует полномочия доступа для сотрудников организации, оказывающих услуги аутсорсинга для Администрации ЗАТО г. Железногорск, а также контролирует их действия при их непосредственной работе в ИСПДн;
- своевременно проводит периодическую проверку работоспособности системы защиты от НСД к ней, а также принимает необходимые меры для восстановления системы защиты от НСД при сбоях;
- проводит генерацию и смену паролей пользователей для доступа в систему, в соответствии с действующей инструкцией по парольной защите. Периодически, по указанию ответственного за обработку ПДн в Администрации ЗАТО г. Железногорск, уточняет список сотрудников

(пользователей), допущенных к работе в ИСПДн, их права доступа и полномочия, с использованием которых осуществляется обработка персональных данных;

- по согласованию с ответственным за обработку ПДн регистрирует в ИСПДн (удаляет из ИСПДн) нового пользователя в соответствии с «Положением о разрешительной системе доступа».

Администратор безопасности контролирует целостность программно-аппаратной среды и хранимой и обрабатываемой информации в ИСПДн, а именно:

- следит за неизменностью программной и технической составляющей ИСПДн;
- своевременно принимает необходимые меры для восстановления ПДн, используя штатные средства операционных систем или специализированное программное обеспечение, позволяющее создавать резервные копии или архивирование необходимой информации, а также выясняет причины, приведшие к потере ПДн;
- проводит своевременное обновление антивирусных средств, а в случае обнаружения вирусов в ИСПДн, принимает необходимые меры в соответствии с «Инструкцией по организации антивирусного контроля».

Администратор безопасности осуществляет настройку и сопровождение подсистемы регистрации и учета действий пользователей при работе в ИСПДн, а именно:

- производит настройку операционной системы для обеспечения регистрации и учета входа (выхода) пользователей в систему (из системы) с регистрацией даты и временем входа и результатом попытки (успешной или неуспешной);
- проводит регулярный анализ соответствующих журналов СЗИ от НСД и операционной системы для выявления факта попыток несанкционированного доступа пользователей к защищаемым ресурсам ИСПДн или выявления фактов нарушения установленного порядка работы с персональными данными, представленного в «Описании технологического процесса обработки ПДн в ИСПДн».

Администратор безопасности контролирует размещение и состав технических средств ИСПДн, определенных в Техническом паспорте ИСПДн.

Внесение изменений в системное программное обеспечение осуществляется администратором безопасности ИСПДн, с обязательным документированием изменений в соответствующем журнале и уведомлением каждого пользователя ИСПДн, которого касается изменение.

Администратор безопасности проводит проверки соответствия текущего состояния ИСПДн уровню безопасности, удовлетворяющему требованиям организационной и распорядительной документации Администрации ЗАТО г. Железногорск (далее – проверка соответствия требованиям). Проверки соответствия требованиям производятся ежеквартально и в случаях нарушения информационной безопасности ИСПДн. Они включают в себя проведение

обзоров безопасности, активное и пассивное тестирование системы защиты ИСПДн, контроль внесения изменений в системное программное обеспечение.

Обзоры безопасности имеют целью выявление всех несоответствий между текущим состоянием системы и состоянием, соответствующем специально составленному списку для проверки.

Обзоры безопасности должны включать:

- отчеты о безопасности пользовательских ресурсов, включающие наличие повторяющихся пользовательских имен и идентификаторов, неправильных форматов регистрационных записей, пользователей без пароля, неправильной установки домашних каталогов пользователей и уязвимостей пользовательских окружений;
- проверку содержимого файлов конфигурации на соответствие списку для проверки;
- обнаружение изменений системных файлов со времени проведения последней проверки (контроль целостности системных файлов);
- проверку прав доступа и других атрибутов системных файлов (команд, утилит и таблиц);
- проверку правильности настройки механизмов аутентификации и авторизации сетевых сервисов;
- проверку корректности конфигурации системных и активных сетевых устройств (мостов, маршрутизаторов, концентраторов и сетевых экранов).

Активное тестирование надежности механизмов контроля доступа производится путем осуществления попыток проникновения в информационную систему в обход системы защиты информации (с помощью систем анализа защищенности или вручную).

Пассивное тестирование механизмов контроля доступа осуществляется путем анализа конфигурационных файлов системы. Информация об известных уязвимостях извлекается из документации и внешних источников. Затем осуществляется проверка конфигурации системы с целью выявления опасных состояний системы, т. е. таких состояний, в которых могут проявлять себя известные уязвимости. Если система находится в опасном состоянии, то, с целью нейтрализации уязвимостей, необходимо либо изменить конфигурацию системы (для ликвидации условий проявления уязвимости), либо установить программные коррекции, либо установить другие версии программ, в которых данная уязвимость отсутствует, либо отказаться от использования системного сервиса, содержащего данную уязвимость.

3 ПРАВА И ОБЯЗАННОСТИ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ ИСПДн

На администратора безопасности возлагаются следующие обязанности:

- следить за сохранностью наклеек с защитной и идентификационной информацией на корпусах технических средств ИСПДн, состав которых определен в Техническом паспорте ИСПДн, а в случае их нарушения

информировать ответственного за обработку ПДн в Администрации ЗАТО г. Железнодорожск;

- своевременно информировать ответственного за обработку ПДн обо всех выявленных фактах попыток несанкционированного доступа пользователей к защищаемым ресурсам ИСПДн или фактов нарушения установленного порядка работы с ПДн, представленного в «Описании технологического процесса обработки ПДн в ИСПДн»;
- поддерживать и контролировать функционирование СЗИ, применяемых в ИСПДн, в соответствии с настройками, обеспечивающими необходимый уровень защищенности ПДн;
- поддерживать применяемые СЗИ в работоспособном состоянии и информировать ответственного за обработку ПДн в случае выхода их из строя (отклонения от нормального режима работы);
- не допускать к работе на рабочих станциях и серверах ИСПДн посторонних лиц;
- своевременно информировать ответственного за обработку ПДн обо всех компрометирующих действиях пользователей ИСПДн при работе в ИСПДн;
- совместно с ответственным за обработку ПДн принимать решение о прекращении обработки ПДн в ИСПДн при несанкционированном доступе (попытках) к ним или возникновении ситуаций, послуживших причиной возможной утраты ПДн;
- совместно с ответственным за обработку ПДн вести разбирательства по фактам нарушения порядка обработки ПДн, хранения носителей ПДн или нарушения порядка эксплуатации СЗИ;
- совместно с ответственным за обработку ПДн осуществлять работы по выбору, закупке и приемке нового программного обеспечения, средств защиты информации, технического оснащения, а также вести работы при подборе кадрового обеспечения организации в области защиты информации;
- обобщать результаты своей деятельности и готовить предложения по ее совершенствованию ответственному за обработку ПДн;
- следить за неизменностью условий функционирования и эксплуатации ИСПДн с последующим информированием ответственного за обработку ПДн в случае каких-либо изменений, руководствуясь настоящей инструкцией и другими нормативными документами по защите персональных данных в организации;
- подчиняться непосредственно ответственному за обработку ПДн или в случае его отсутствия Заместителю Главы ЗАТО г. Железнодорожск по общественно-политической работе Администрации ЗАТО г. Железнодорожск;
- проводить инструктаж пользователей ИСПДн по правилам работы с используемыми средствами защиты информации;
- вести журнал учета своей работы по обеспечению безопасности персональных данных при их обработке в ИСПДн (форма «Журнала работ администратора безопасности» приведена в приложении № 1);

4 ПОРЯДОК ДЕЙСТВИЙ ПРИ НАРУШЕНИЯХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В случае выявления фактов нарушений информационной безопасности администратор безопасности принимает меры, необходимые для предотвращения негативных последствий и информирует ответственного за обработку ПДн в ИСПДн и непосредственное руководство о факте нарушения и принятых мерах.

Администратор безопасности анализирует и устанавливает причины возникшего нарушения и принимает меры по предотвращению подобных нарушений в дальнейшем.

По факту нарушения администратор безопасности составляет служебную записку на имя Заместителя Главы ЗАТО г. Железногорск по общественно-политической работе с указанием причин нарушения и принятых мер.

В случае создания комиссии по расследованиям причин нарушения администратор безопасности принимает участие в ее работе.

В случае, если администратор безопасности ИСПДн подозревает или получил сообщение о том, что ИСПДн подвергается атаке или уже была скомпрометирована, он должен установить:

- факт попытки несанкционированного доступа (НСД);
- продолжается ли НСД в настоящий момент;
- источник НСД;
- объект НСД;
- время осуществления попытки НСД;
- обстоятельства, при которых была предпринята попытка НСД;
- точку входа нарушителя в систему;
- успешность попытки НСД;
- определить системные ресурсы, безопасность которых была нарушена;

Для выявления попытки НСД необходимо установить, какие пользователи в настоящее время работают в системе, на каких рабочих станциях. Выявить подозрительную активность пользователей, проверить, что все пользователи вошли в систему со своих рабочих мест, и никто из них не работает в системе необычно долго. Кроме того, необходимо проверить, что никто из пользователей не выполняет подозрительных программ и программ, не относящихся к его области деятельности.

Для обнаружения в системе следов, оставленных злоумышленником, в виде файлов, вирусов, троянских программ, изменения системной конфигурации необходимо:

- составить базовую схему системы;
- провести поиск подозрительных файлов, скрытые файлы, имена файлов и каталогов, которые обычно используются злоумышленниками;
- проверить содержимое системных файлов, которые обычно изменяются злоумышленниками;
- проверить целостность системных программ;
- проверить систему аутентификации и авторизации.

В случае заражения значительного количества рабочих станций после устранения его последствий проводится проверка соответствия требованиям.

5 ОТВЕТСТВЕННОСТЬ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ

Администратор безопасности несет всю полноту ответственности за качество и своевременность выполнения задач и функций, возложенных на него в соответствии с настоящей инструкцией и другими нормативными документами по защите ПДн в организации.

Персональные данные не подлежат разглашению (распространению). Прекращение доступа к такой информации не освобождает администратора от взятых им обязательств по неразглашению сведений ограниченного распространения. За разглашение информации ограниченного распространения, нарушение порядка работы с документами или машинными носителями, содержащими такую информацию, сотрудник может быть привлечен к дисциплинарной или иной, предусмотренной законодательством ответственности.

Администратор безопасности, получивший доступ к ПДн, обязан хранить в тайне сведения ограниченного распространения, ставшие ему известными во время работы или иным путем и пресекать действия других лиц, которые могут привести к разглашению такой информации.

В случае оставления занимаемой должности администратор безопасности обязан вернуть все документы и материалы, относящиеся к деятельности подразделения, организации, ответственному за обработку ПДн.

Приложение № 7
к распоряжению Администрации
ЗАТО г. Железногорск
от 23.12 2022 № 497пр

Приложение № 10
к распоряжению Администрации
ЗАТО г. Железногорск
от 30.06.2014 № 132пр

ИНСТРУКЦИЯ

пользователя информационных систем персональных данных
Администрации ЗАТО г. Железногорск

1 ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая инструкция определяет порядок работы пользователей при обработке персональных данных (ПДн) в информационных системах персональных данных (ИСПДн) «Гаражи и усадьбы», «Кадры», «АРМ «Административная комиссия», «АРМ «Договора», «АРМ «ЖФСИ», «АРМ «Общественная приемная», «Муниципальный регистр», «АИСТ», «Личный кабинет сайта Администрации» Администрации ЗАТО г. Железногорск. Пользователем является каждый сотрудник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки персональных данных и имеющий доступ к аппаратным средствам, программному обеспечению и средствам защиты.

Доступ пользователей к ресурсам ИСПДн осуществляется в соответствии с «Положением о разрешительной системе доступа».

Каждый пользователь должен осознавать, что контроль, осуществляемый администратором безопасности за его действиями, является постоянным, и в случае совершения им не регламентированных данной инструкцией операций, к нему могут быть применены дисциплинарные и административные взыскания.

Все пользователи ИСПДн Администрации ЗАТО г. Железногорск должны быть ознакомлены под подпись с настоящей инструкцией (лист ознакомления) и предупреждены о возможной ответственности за ее нарушение.

2 ПРАВА И ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ

Пользователь должен обладать определенными навыками работы на ПЭВМ, достаточными для выполнения требований настоящей Инструкции.

В процессе обработки ПДн пользователь обязан:

- осуществлять доступ к ресурсам ИСПДн при выполнении своих функциональных обязанностей строго в соответствии с «Положением о разрешительной системе доступа»;
- выполнять требования, предъявляемые к парольной защите согласно «Инструкции по организации парольной защиты»;
- выполнять требования «Инструкции по организации антивирусного контроля»;
- соблюдать требования администратора безопасности, а, в случае возникновения конфликтных ситуаций, привлекать для их разрешения ответственного за обработку ПДн;
- использовать для работы, только учтенные съемные носители информации;
- соблюдать меры по предотвращению просмотра ПДн посторонними лицами и сотрудниками организации, не имеющими доступа к ним;
- следить за изменениями программной среды компьютера, попытками несанкционированного доступа к информации, правильным функционированием средств вычислительной техники и средств защиты информации, а в случае обнаружения нарушений в их

- функционировании незамедлительно сообщить об этом администратору безопасности и прекратить обработку ПДн до принятия решения ответственным за обработку ПДн;
- привлекать для производства ремонта или настройки персональной ЭВМ (ПЭВМ) только сотрудников, уполномоченных на то руководством организации;
 - на время отсутствия на рабочем месте блокировать доступ к ПЭВМ штатными средствами операционной системы или при помощи средств защиты информации (СЗИ);
 - соблюдать размещение и состав технических средств (ТС) ИСПДн, описанные в «Техническом паспорте» каждой информационной системы персональных данных Администрации ЗАТО г. Железногорск;
 - осуществлять визуальный контроль работоспособности СЗИ;
 - проводить регламентный антивирусный контроль жестких дисков, а также съемных носителей информации;
 - сообщать администратору безопасности об утере носителя с персональными данными, о подозрении компрометации личных ключей и паролей, а также целостности пломб (наклеек с защитной и идентификационной информацией, нарушении или несоответствии номеров печатей) на ТС ИСПДн;
 - следить за действиями сотрудников, проводящих регламентную уборку помещений, в которых расположены ТС ИСПДн и/или носители ПДн;
 - не оставлять на рабочих местах и в незакрытых сейфах документы ограниченного распространения, а также запирают и, в предусмотренных случаях, опечатывать после окончания работы сейфы, помещения и хранилища с носителями ПДн;
 - ставить в известность администратора безопасности при необходимости:
 - обновления антивирусных баз;
 - обновления программного обеспечения;
 - проведения регламентных работ (текущий ремонт, профилактические работы и т. д.);
 - вскрытия системных блоков персональных компьютеров, входящих в состав ИСПДн;
 - резервного копирования информации;
 - иных действий с ПЭВМ.

Пользователю запрещена установка на АРМ специальных программ-анализаторов пакетов (sniffer-ов).

3 ОТВЕТСТВЕННОСТЬ ПОЛЬЗОВАТЕЛЯ

Пользователь несет всю полноту ответственности за качество и своевременность выполнения задач и функций, возложенных на него в соответствии с настоящей инструкцией и другими нормативными документами по защите информации в организации.

За разглашение информации ограниченного распространения, нарушение порядка работы с документами или машинными носителями, содержащими такую информацию, пользователь может быть привлечен к дисциплинарной, административной или уголовной ответственности, предусмотренной законодательством.

Пользователи обязаны хранить в тайне сведения ограниченного распространения, ставшие им известными во время работы или иным путем и пресекать действия других лиц, которые могут привести к разглашению такой информации.

В случае оставления занимаемой должности сотрудник обязан вернуть все документы и материалы, относящиеся к деятельности подразделения и организации, ответственному за обработку персональных данных.

Приложение № 8
к распоряжению Администрации
ЗАТО г. Железнодорожск
от 23.12 2022 № 497 пр

Приложение № 11
к распоряжению Администрации
ЗАТО г. Железнодорожск
от 30.06.2014 № 132пр

ИНСТРУКЦИЯ

по организации парольной защиты в информационных системах персональных
данных
Администрации ЗАТО г. Железнодорожск

1. Общие положения

Настоящая инструкция предназначена для использования в работе пользователями информационных систем персональных данных (ИСПДн) «Гаражи и усадьбы», «Кадры», «АРМ «Административная комиссия», «АРМ «Договора», «АРМ «ЖФСИ», «АРМ «Общественная приемная», «Муниципальный регистр», «АИСТ», «Личный кабинет сайта Администрации Администрации ЗАТО г. Железногорск и определяет порядок обеспечения защиты от несанкционированного доступа к информации (НСД).

Парольная защита при работе в ИСПДн осуществляется с целью предотвращения НСД к конфиденциальной информации и персональным данным, обрабатываемым в ней.

Парольная защита является составной частью подсистемы управления доступом системы защиты информации от НСД.

Компрометация действующих паролей является служебным проступком, о чем администратор безопасности сообщает ответственному за защиту и обработку конфиденциальной информации и персональных данных.

Под компрометацией понимается хищение, утрата действующих паролей, передача или сообщение их лицам, не имеющим на то право, другие действия сотрудника, приведшие к получению его пароля лицами, не имеющими на то право. Скомпрометированные пароли выводятся из действия немедленно.

2. Требования к организации парольной защиты

Личные пароли доступа ОС выбираются пользователями самостоятельно, но при этом необходимо руководствоваться следующими требованиями:

- длина пароля должна быть не менее 6 символов;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имя, фамилия, день рождения и другие памятные даты, номер телефона, автомобиля, адрес местожительства, наименования АРМ, общепринятые сокращения (ЭВМ, ЛВС, USER, SYSOP, GUEST, ADMINISTRATOR и т.д.), и другие данные, которые могут быть подобраны злоумышленником путем анализа информации о пользователе;
- не использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;
- не использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 или 1йфячыц2 и т. п.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 5 позициях;
- не использовать ранее использованные пароли.

Лица, использующие пароли, обязаны:

- четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по использованию парольной защиты;
- своевременно сообщать администратору безопасности обо всех нештатных ситуациях и нарушениях работы подсистем защиты от НСД, возникающих при работе с паролями.

При организации парольной защиты запрещается:

- записывать свои пароли в очевидных местах (стикерах, мебели, на обратной стороне клавиатуры и т.п.);
- сообщать посторонним лицам свои пароли, а также сведения о применяемой системе защиты информации от НСД.
- самостоятельно производить смену пароля для входа в операционную систему.

3. Смена пароля пользователя

Плановая смена паролей в ИСПДн проводится регулярно, не реже одного раза в 6 месяцев.

Удаление (в том числе внеплановая смена) личного пароля любого пользователя ИСПДн должна производиться в следующих случаях:

- по окончании срока действия;
- в случае прекращения его полномочий (увольнение, переход на другую работу) после окончания последнего сеанса работы;
- при обнаружении факта успешной попытки несанкционированного доступа к элементам ИСПДн;
- по указанию администратора безопасности.

Пароли, используемые для доступа к ресурсам ИСПДн, вводятся пользователем с клавиатуры.

Приложение № 9
к распоряжению Администрации
ЗАТО г. Железногорск
от 23.12 2022 № 497пр

Приложение № 12
к распоряжению Администрации
ЗАТО г. Железногорск
от 30.06.2014 № 132пр

ИНСТРУКЦИЯ

по организации антивирусного контроля в информационных системах
персональных данных Администрации ЗАТО г. Железногорск

1 Общие положения

Настоящая инструкция предназначена для пользователей информационных систем персональных данных (ИСПДн) «Гаражи и усадьбы», «Кадры», «АРМ «Административная комиссия», «АРМ «Договора», «АРМ «ЖФСИ», «АРМ «Общественная приемная», «Муниципальный регистр», «АИСТ», «Личный кабинет сайта Администрации» Администрации ЗАТО г. Железногорск.

Инструкция устанавливает требования и ответственность пользователей ИСПДн при организации ими защиты информации от разрушающего воздействия компьютерных вирусов.

Инструкция регулирует как вопросы организации антивирусной защиты, так и требования к порядку проведения антивирусного контроля.

2 Требования к организации антивирусной защиты

2.1 Требования к порядку организации антивирусной защиты

Для организации антивирусной защиты в ИСПДн допускаются к использованию только сертифицированные антивирусные средства.

Не реже чем один раз в месяц должно быть произведено обновление антивирусных баз. Разработка и осуществление мероприятий по проведению антивирусного контроля осуществляется администратором безопасности.

Пользователи не должны допускать использования в персональных ЭВМ, входящих в состав ИСПДн программного обеспечения и данных, не связанных с выполнением своих функциональных обязанностей в технологическом процессе обработки информации.

2.2 Требования к порядку проведения антивирусного контроля

Установка (изменение) системного и прикладного программного обеспечения на ПЭВМ, входящих в состав каждой ИСПДн осуществляется администратором безопасности только по предварительному согласованию с организацией имеющей лицензию на деятельность по технической защите конфиденциальной информации. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера, должна быть выполнена антивирусная проверка.

При загрузке компьютера должен проводиться антивирусный контроль в автоматическом режиме. Полная антивирусная проверка должна осуществляться не реже одного раза в две недели.

Обязательному антивирусному контролю подлежит любая информация со съемных носителей (магнитные диски, CD-ROM и т. п.) перед ее обработкой в ИСПДн.

При возникновении подозрения на наличие компьютерного вируса пользователь должен провести антивирусный контроль.

2.3 Обязанности пользователя при обнаружении компьютерного вируса

При обнаружении компьютерного вируса пользователь обязан:

- приостановить использование ИСПДн (работу со съемными носителями информации);
- провести лечение или уничтожение зараженных файлов (при необходимости привлечь администратора безопасности);
- в случае обнаружения вируса, неподдающегося лечению, в возможно короткий срок направить зараженный вирусом файл (при необходимости, удалив конфиденциальную информацию) разработчику антивирусного ПО.

3 Ответственность при организации антивирусной защиты

Ответственность за организацию и поддержание установленного порядка, и соблюдение требований настоящей инструкции возлагается на пользователей ИСПДн и администратора безопасности.

Периодический контроль за выполнением всех требований настоящей инструкции и состоянием антивирусной защиты осуществляется администратором безопасности.

Приложение № 10
к распоряжению Администрации
ЗАТО г. Железногорск
от 23.12. 2022 № 497пр

Приложение № 15
к распоряжению Администрации
ЗАТО г. Железногорск
от 30.06.2014 № 132пр

Положение о разрешительной системе доступа в информационных
системах персональных данных Администрации ЗАТО г. Железногорск

1 Общие положения

Настоящее Положение разработано в соответствии с «Составом и содержанием организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденным приказом ФСТЭК России 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». Положение определяет порядок установления уровня полномочий пользователей, а также правила разграничения доступа к защищенным техническим, программным средствам и информационным ресурсам информационных систем персональных данных (ИСПДн) «АРМ «Общественная приемная», «Гаражи и усадьбы», «Кадры», «АРМ «ЖФСИ», «АРМ «Договора», «АРМ «Административная комиссия», «Муниципальный регистр», «АИСТ», «Личный кабинет сайта Администрации» Администрации ЗАТО г. Железногорск (далее Администрация).

Положение определяет порядок установления уровня полномочий пользователей информационных систем персональных данных (ИСПДн) Администрации, в которых производится обработка сведений, содержащих персональные данные, а также правила разграничения доступа к защищаемым техническим, программным средствам и информационным ресурсам ИСПДн.

Под разрешительной системой доступа (РСД) понимается процесс определения для всех категорий пользователей соответствующей программно-аппаратной среды или информационных и программных ресурсов (узлов сети, автоматизированных рабочих мест (АРМ), внешних устройств, файлов, программ, процессов и т.п.), которые будут им доступны для конкретных операций (Read, Write, и т. п.) с помощью заданных программно-аппаратных средств доступа.

Правила разграничения доступа, регламентирующие права доступа пользователей к защищаемым ресурсам ИСПДн, основываются на задании множества разрешительных отношений доступа в виде триады: <объект, субъект, тип доступа>. Правила доступа пользователя к ИСПДн определяются ответственным за обработку ПДн и администратором безопасности ИСПДн и задаются с помощью настроек системы защиты информации (СЗИ) от несанкционированного доступа (НСД), установленной на объекте.

Администрирование системы защиты информации от несанкционированного доступа, управление процессом установления прав и полномочий в ИСПДн, а также установку (изменение) имен пользователей, их паролей и прочих атрибутов идентификации в ИСПДн производит администратор безопасности ИСПДн по согласованию с ответственным за обработку ПДн.

При изменении (модернизации) действующих автоматизированных программных комплексов, появлении нового программного обеспечения, администратором безопасности разрабатываются предложения по изменению и (или) дополнению перечня прав и полномочий пользователей. Процедура

регистрации (создания учетной записи) пользователя для сотрудника и предоставления ему (или изменения его) прав доступа к ресурсам ИСПДн выполняется в соответствии с Регламентом предоставления прав доступа к персональным данным.

Уровень прав и полномочий пользователей ИСПДн, необходимый им для выполнения своих функций, уточняется и согласовывается с ответственным за обеспечение безопасности персональных данных.

Замена технических средств ИСПДн при проведении работ по устранению неисправностей, регламентных и других видов работ, осуществляется администратором безопасности ИСПДн только по согласованию с ответственным за обработку ПДн.

Техническое обслуживание и ремонт средств вычислительной техники, предназначенных для обработки персональных данных, рекомендуется проводить технически подготовленными сотрудниками предприятия, либо организациями, имеющими соответствующие лицензии.

При проведении технического обслуживания и ремонта запрещается передавать ремонтным организациям узлы и блоки с элементами накопления и хранения защищаемой информации. Они должны быть изъяты из системных блоков и оставлены для хранения в отделе системных администраторов или серверном помещении. При неисправности таких узлов и блоков - они уничтожаются установленным порядком.

Контроль за организацией и соблюдением пользователями систем установленного порядка разграничения доступа к разделяемым ресурсам ИСПДн осуществляется администратором безопасности.

Периодически проводится проверка разрешенных и запрещенных связей между субъектами и объектами доступа к защищаемым ресурсам с привязкой к конкретному АРМ ИСПДн и пользователю, а также их соответствие РСД.

2 Разрешительная система доступа пользователей к техническим и программным средствам и информационным ресурсам ИСПДн

Обработка ПДн осуществляется в ИСПДн, состав которой определен в Техническом паспорте ИСПДн. Пользователь, в соответствии со своими правами доступа к информации, осуществляет ее обработку с использованием программных средств, установленных в ИСПДн. Файлы с персональными данными, в процессе обработки и хранения, записываются на НЖМД. Подробное описание обработки информации в ИСПДн отражено в Описании технологического процесса обработки информации.

2.1 Доступ к информационным ресурсам работников Администрации

Доступ к персональным данным разрешает Глава ЗАТО г. Железногорск только специально уполномоченным лицам с соблюдением требований «Положения по обработке персональных данных».

Фактом ознакомления с разрешением на доступ является подпись работника в листе ознакомления Инструкции пользователя ИСПДн.

2.2 Доступ к информационным ресурсам сторонних организаций, деятельность которых регламентируется законодательством Российской Федерации

К организациям, деятельность которых регламентируется законодательством РФ, могут относиться:

- правоохранительные органы;
- судебные органы;
- органы статистики;
- органы исполнительной и законодательной власти субъектов Российской Федерации;
- средства массовой информации и пр.

Допуск к информационным ресурсам таких организаций регламентируется законодательством Российской Федерации, договорами и соглашениями об информационном обмене и другими нормативными актами.

2.3 Доступ к информационным ресурсам Администрации сторонних организаций, выполняющих работы в Администрации на договорной основе

К организациям, выполняющим работы на договорной основе, могут относиться:

- организации, выполняющие строительные работы и осуществляющие ремонт зданий, систем инженерно-технического обеспечения (отопления, освещения, водоснабжения, канализации, электропитания, кондиционирования и т.п.);
- организации, осуществляющие монтаж и настройку ПЭВМ, сопровождение программно-прикладного обеспечения и технических средств;
- организации, оказывающие услуги в области защиты информации (проведение объектовых исследований, монтаж и настройка средств защиты информации, контроль эффективности системы защиты информации, аттестация объектов информатизации и т.п.);
- организации, осуществляющие поставку товаров для обеспечения повседневной деятельности (канцтоваров, оргтехники, расходных материалов, мебели и т.п.);
- организации и частные лица, оказывающие юридические услуги, услуги по информационно-техническому обеспечению, осуществляющие преподавательскую деятельность и т.п.

Порядок доступа к информационным ресурсам Администрации определяется в договоре на выполнение работ (оказание услуг).

Решением о предоставлении/не предоставлении доступа является подписанный в установленном порядке «Договор на выполнение работ или оказание услуг».

2.4 Перечень субъектов доступа

Субъектами, права доступа которых рассматриваются при работе в ИСПДн являются:

- администратор безопасности с правами полного доступа к техническим и программным средствам ИСПДн;
- пользователь ИСПДн, обрабатывающий ПДн в ИСПДн;
- процессы, выполняемые на АРМ от имени администратора безопасности;
- процессы, выполняемые на АРМ от имени пользователя.

Для работы в ИСПДн предусмотрены учетные записи с правами администратора или пользователя:

- Учетная запись администратора.
- Учетная запись пользователя, обрабатывающего ПДн в ИСПДн.

Вход в систему осуществляется с помощью персонального имени (логин) и пароля условно-постоянного действия.

2.5 Перечень объектов доступа.

Объектами доступа являются:

- ПЭВМ в целом;
- принтер;
- многофункциональное устройство;
- USB-порты;
- USB-накопители с защищаемой информацией;
- устройства чтения/записи оптических дисков;
- оптические диски с защищаемой информацией;
- НЖМД рабочих станций с защищаемой информацией;
- монитор с отображаемой на нем защищаемой информацией;
- оперативная память ПЭВМ;
- операционные системы (ОС) ПЭВМ;
- программы, предназначенные для разработки и печати документов, содержащих персональные данные;
- программные средства, осуществляющие функции по защите информации на ПЭВМ, а также функции контроля безопасности;
- бумажный носитель информации, на который/с которого выводится защищаемая информация.

2.6 Разрешительная система доступа

Присвоение конкретным пользователям прав доступа, а также закрепление за ними конкретных рабочих папок, директорий и файлов с обрабатываемой информацией в ИСПДн осуществляется по согласованию с ответственным за обработку ПДн.

Права доступа различных пользователей к техническим и программным средствам и информационным ресурсам ИСПДн указаны в приложении 1.

2.7 Доступ к информационным ресурсам ИСПДн Администрации сторонних организаций, деятельность которых регламентируется законодательством Российской Федерации

Доступ (предоставление) сторонних организаций к информационным ресурсам организации регламентируется федеральными законами, приказами и распоряжениями министерств и служб, законодательно наделенных полномочиями на получение информации, а также настоящим Положением.

Доступ к информационным ресурсам организации сторонних организаций осуществляется на основании:

- письменных запросов;
- письменных соглашений (договоров) сторон об обмене информацией.

В письменном запросе (договоре) указывается:

- для каких целей необходима информация;
- ее конкретное наименование;
- способ доступа (предоставления).

Основанием для доступа (предоставления) к информации служит руководство на соответствующем документе.

При наличии официального соглашения со сторонней организацией о допуске (предоставлении) к информации доступ к ней осуществляется в порядке, указанном в подписанном соглашении (договоре).

Запрещается передача электронных копий баз данных любым сторонним организациям.

2.8 Доступ к информационным ресурсам ИСПДн Администрации сторонних организаций, выполняющих работы на договорной основе

Доступ к информационным ресурсам Администрации сторонних организаций, выполняющих работы на договорной основе, осуществляется на основании подписанного договора на оказание услуг, а также настоящего Положения.

Дополнительно к договору на оказание услуг между Администрацией и сторонней организацией заключается соглашение о конфиденциальности и неразглашении сведений, содержащих персональные данные (и/или

составляющих коммерческую тайну). В рамках данного соглашения, работники сторонней организации обязаны хранить в тайне сведения, содержащие персональные данные, а также служебную информацию, ставшие известными в ходе выполнения работ, если для их выполнения предусмотрено использование таких сведений.

3 Правила разграничения доступа

Каждому пользователю присваивается персональный идентификатор и пароль для входа в систему.

Разработка, редактирование защищаемых документов производится с применением установленного на рабочей станции программного обеспечения.

Правила работы пользователей ИСПДн регламентируются соответствующей «Инструкцией пользователя информационных систем персональных данных Администрации ЗАТО г. Железногорск», администратора безопасности «Инструкцией администратора безопасности информационных систем персональных данных Администрации ЗАТО г. Железногорск», ответственного за обработку ПДн - «Инструкцией ответственного за обработку персональных данных в информационных системах персональных данных Администрации ЗАТО г. Железногорск».

Контроль функционирования разрешительной системы допуска к информационным ресурсам организуется в соответствии с:

- планом основных мероприятий по защите информации на текущий год;
- функциональными обязанностями должностных лиц;
- распоряжениями руководства.

Контроль функционирования разрешительной системы допуска к информационным ресурсам осуществляется ответственными лицами. Организация контроля возлагается на администратора безопасности ИСПДн.

Права доступа различных пользователей к техническим и программным средствам и информационным ресурсам ИСПДн

Матрица доступа

Категория пользователя	Доступные ресурсы	Права доступа
Администратор безопасности	1. Средства ОС, необходимые для запуска и работы ПЭВМ	Полный доступ
	2. Основные конфигурационные файлы ОС	Полный доступ
	3. Средства настройки и управления СЗИ; Журналы работы пользователей	Полный доступ
	4. Разрабатываемые документы	Нет доступа (Доступ к рабочим папкам пользователей ограничен организационными мерами)
	5. Средства разработки документов	Полный доступ
	6. Внешние устройства: Принтер, МФУ	Полный доступ
Пользователь	1. Средства ОС, необходимые для запуска и работы ПЭВМ	Чтение, исполнение
	2. Основные конфигурационные файлы ОС	Нет доступа
	3. Средства настройки и управления СЗИ; Журналы работы пользователей	Нет доступа
	4. Разрабатываемые документы	Полный доступ
	5. Средства разработки документов	Полный доступ
	6. Внешние устройства: Принтер, МФУ	Печать, копирование, сканирование