Департамент промышленности
Ханты-Мансийского автономного округа – Югры
(Деппромышленности Югры)

ПРИКАЗ

О защите информации

г. Ханты-Мансийск
«25» августа 2017 года № 38-П-139

В соответствии с Федеральными законами Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27.07.2006 № 152-ФЗ «О персональных данных, постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных па обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, Департаментами, являющимися государственными или муниципальными органами», приказом ФСТЭК Российской Федерации от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», **п р и к а з ы в а ю:**

1. Назначить ответственными:

1.1. За руководство работами по защите информации и за организацию обработки персональных данных - заместителя директора Департамента промышленности Ханты-Мансийского автономного округа – Югры Киселева Александра Константиновича.

1.2. За обеспечение безопасности в информационных системах

начальника отдела автоматизации процесса Управления правового и экономического регулирования Департамента промышленности Ханты-Мансийского автономного округа – Югры Хаперского Олега Анатольевича.

2. Создать постоянно действующую техническую комиссию по защите информации в Департаменте промышленности Ханты-Мансийского автономного округа – Югры, утвердить её состав (приложение 1) и положение о ней (приложение 2).

3. Создать комиссию по определению класса защищённости информационных систем и определения уровня защищённости персональных данных в Департаменте промышленности Ханты-Мансийского автономного округа – Югры (приложение 3).

3.1.Комиссии в срок до «31» августа 2017г. определить перечень информационных систем, классы (уровни) защищённости информационных систем.

4.Утвердить:

4.1. Политику в отношении обработки персональных данных (приложение 4).

4.2. Положение об организации режима обеспечения безопасности помещений, в которых размещены информационные системы, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения (приложение 5).

4.3. Перечень должностей Департамента промышленности Ханты-Мансийского автономного округа – Югры, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, в случае обезличивания персональных данных (приложение 6).

4.4. Перечень должностей Департамента промышленности Ханты-Мансийского автономного округа – Югры, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным (приложение 7).

4.5. Перечень информационных систем персональных данных (приложение 8).

4.6. Перечень обрабатываемых персональных данных (приложение 9).

4.7. Инструкции и правила по защите информации (приложения 10-18).

4.8. Порядок уничтожения персональных данных при достижении целей обработки и (или) при наступлении иных законных оснований (приложение 19).

4.9. Правила:

4.9.1. работы лиц, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими служебных (трудовых) обязанностей (приложение 20).

4.9.2. рассмотрения запросов субъектов персональных данных или их представителей (приложение 21).

4.9.3. осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (приложение 22).

4.9.4. работы с обезличенными данными в случае обезличивания персональных данных (приложение 23).

4.10. План мероприятий по защите информации (приложение 24).

4.11. Регламент работников, эксплуатирующих информационную систему обработки информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в том числе персональные данные в Департаменте промышленности Ханты-Мансийского автономного округа – Югры (приложение 25).

4.12. Регламент администратора безопасности информации в Департаменте промышленности Ханты-Мансийского автономного округа – Югры (приложение 26).

4.13. Инструкцию должностного лица, ответственного за организацию

обработки персональных данных в Департаменте промышленности Ханты-Мансийского автономного округа – Югры (приложение 27).

4.14. Типовые формы документов по защите информации:

4.14.1. Список лиц, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими служебных (трудовых) обязанностей (приложение 28).

4.14.2. Обязательство о неразглашении информации, содержащей персональные данные (приложение 29).

4.14.3. Типовую форму согласия субъекта на обработку их персональных данных (приложение 30).

4.14.4. Типовую форму разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные (приложение 31).

4.14.5. Журналы по защите информации (приложение 32).

4.14.6. Акт определения уровня защищенности персональных данных и класса защищенности информационной системы (приложение 33).

4.14.7. Акт классификации информационной системы (приложение 34).

4.14.8. Акт об уничтожении персональных данных субъектов персональных данных (приложение 35).

5. Начальнику отдела автоматизации процесса Управления правового и экономического регулирования (Хаперский О.А.);

5.1. Ознакомить с настоящим приказом руководителей и работников всех структурных подразделений Департамента промышленности Ханты-Мансийского автономного округа – Югры.

5.2. Направить в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций уведомление об обработке персональных данных;

5.3. Разместить настоящий приказ на официальном сайте Департамента промышленности Ханты-Мансийского автономного округа – Югры в разделе

«Политика в отношении обработки персональных данных» не позднее 10дней после регистрации.

6. Контроль за исполнением настоящего приказа оставляю за собой.

И.о.директора Департамента — В.С.Дудниченко

Приложение 1
к приказу Департамента промышленности Ханты-Мансийского автономного округа – Югры от 25.08.2017 №38-П-139

Состав постоянно действующей технической комиссии по защите информации в Департаменте промышленности Ханты-Мансийского автономного округа – Югры

Роль	Должность	Ф.И.О.
Председатель комиссии	Заместитель директора Департамента	Киселев А.К.
Члены комиссии	Заместитель директора Департамента - начальник Управления правового и экономического регулирования	Шиповалов А.В.
	Помощник директора	Кугаевская А.Т.
	Начальник отдела автоматизации процесса Управления правового и экономического регулирования	Хаперский О.А.
	Начальник отдела промышленной политики и методологии	Торгашин Е.Ю.
	Главный специалист - эксперт отдела отраслевых секторов промышленности Управления промышленной политики	Усольцева А.В.

Приложение 2
к приказу Департамента промышленности Ханты-Мансийского автономного округа – Югры от 25.08.2017 №38-П-139

Положение о постоянно действующей технической комиссии по защите информации в Департаменте промышленности Ханты-Мансийского автономного округа – Югры

I. Общие положения

1. Настоящее Положение разработано в соответствии с Законом Российской Федерации от 21.07.1993 № 5485-I «О государственной тайне», Федеральным законом от 18.07.1999 № 183-ФЗ «Об экспортном контроле», Федеральным законом от 28.12.2010 № 390-ФЗ «О безопасности», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» Федеральным законом 27.07.2006 № 152-ФЗ «О персональных данных», а также Положением о государственной системе защиты информации в Российской Федерации, утвержденным Постановлением Совета Министров Правительства Российской Федерации от 15.09.1993 № 912-51, распоряжения Правительства Российской Федерации от 28.06.2001 № 852-р «Об образовании в органах исполнительной власти субъектов РФ постоянно действующих технических комиссий (советов) по защите государственной тайны», Рекомендациями по проведению экспертизы материалов, предназначенных к открытому опубликованию, одобренные решением межведомственной комиссии по защите государственной тайны от 24.01.2012 № 225 (далее – МВК), совместного приказа ФСТЭК России и ФСБ России от 28.07.2001 № 405/309 «Об утверждении Положения о постоянно действующих технических комиссиях по защите государственной тайны», решения Гостехкомиссии России от 14.03.1995 № 32 «О нормативно-правовом обеспечении защиты информации от иностранных технических разведок и от ее утечки по техническим каналам» и распоряжения Аппарата Губернатора автономного округа от 28.11.2011 № 174-р «О проведении в исполнительных органах государственной власти Ханты-Мансийского автономного округа – Югры экспертизы материалов, предназначенных для открытого опубликования».

2. Положение определяет функции, состав, полномочия и порядок функционирования постоянно действующей технической комиссии по защите информации в исполнительных органах государственной власти Ханты-Мансийского автономного округа – Югры (далее – ПДТК по ЗИ).

3. ПДТК по ЗИ является коллегиальным совещательным органом при руководителе Департамента промышленности Ханты-Мансийского автономного округа – Югры (далее – Департамент), созданная для координации деятельности в сфере защиты информации и информационных ресурсов, составляющих информацию ограниченного доступа (персональные данные, служебная тайна, коммерческая тайна, нотариальная тайна, врачебная тайна и иная охраняемая законом информация), а так же информации обрабатываемой в государственных информационных системах (далее – ГИС) Департамента.

4. ПДТК по ЗИ вносит руководству Департамента предложения по вопросам защиты, как общедоступной информации, так и информации ограниченного доступа обрабатываемой, циркулирующей, накапливаемой в Департаменте.

5. ПДТК по ЗИ в своей работе руководствуется Конституцией Российской Федерации, федеральными законами, указами и распоряжениями Президента Российской Федерации, постановлениями и распоряжениями Правительства Российской Федерации, законами Ханты-Мансийского автономного округа – Югры, постановлениями и распоряжениями Губернатора и Правительства Ханты-Мансийского автономного округа – Югры и настоящим Положением.

6. Методическое руководство деятельностью ПДТК по ЗИ в пределах своей компетенции осуществляют ПДТК по защите государственной тайны Ханты-Мансийского автономного округа – Югры и Совет по вопросам технической защите информации на территории Ханты-Мансийского автономного округа – Югры, являющихся координирующими органами защиты информации в Ханты-Мансийском автономном округе – Югре.

7. Ответственность за организацию деятельности ПДТК по ЗИ возлагается на руководителя Департамента.

II. Основные функции ПДТК по ЗИ

8. Изучает все стороны деятельности Департамента, подведомственных учреждений в области защиты информации.

9. ПДТК по ЗИ вырабатывает рекомендации руководству Департамента, направленные на обеспечение решения следующих вопросов:

надежное и эффективное управление системой защиты информации в Департаменте и подведомственных учреждениях и ее функционирование;

разработки организационных и распорядительных документов по вопросам выявления и закрытия возможных каналов неправомерного распространения информации ограниченного доступа, в том числе по защите информационных систем, а также по совершенствованию системы физической защиты объектов;

изучения и анализа возможностей иностранных технических разведок с учетом профиля работ Департамента и оперативной обстановки, определения видов и средств разведки, которым необходимо осуществлять противодействие;

разработки системы мер, организация и координация разработки, внедрения и эксплуатации систем защиты и безопасности информации, обрабатываемой техническими средствами;

организация и координация работ по технической защите информации;

совершенствование системы физической и технической защиты объектов информатизации Департамента, направленной на обеспечение их безопасности.

10. Проводит анализ обстоятельств и причин неправомерного распространения информации ограниченного доступа.

11. Осуществляет контроль и координацию работ по обеспечению безопасности общедоступной информации в соответствии с требованиями Указа Президента Российской Федерации от 17.03.2008 № 351, Приказа Министерства связи и массовых коммуникаций Российской Федерации от 25.08.2009 № 104 и Совместного приказа Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю от 31.08.2010 № 416/489.

12. Участвует в разработке проектов основных направлений работ по комплексной защите информации, целевых программ и соответствующих разделов планов работ в этой области.

13. Осуществляет экспертизу материалов, предназначенных для открытого опубликования, которая осуществляется в соответствии с требованиями распоряжения Аппарата Губернатора автономного округа от 28.11.2011 № 174-р «О проведении в исполнительных органах государственной власти Ханты-Мансийского автономного округа – Югры экспертизы материалов, предназначенных для открытого опубликования» разработанного в соответствии с требованиями Положением о государственной системе защиты информации в Российской Федерации, утвержденным Постановлением Совета Министров Правительства Российской Федерации от 15.09.1993 № 912-51, распоряжения Правительства Российской Федерации от 28.06.2001 № 852-р «Об образовании в органах исполнительной власти субъектов РФ постоянно действующих технических комиссий

(советов) по защите государственной тайны», Рекомендациями по проведению экспертизы материалов, предназначенных к открытому опубликованию, одобренные решением МВК по защите государственной тайны от 24.01.2012 № 225.

III. Состав и порядок работы ПДТК по ЗИ

14. В состав ПДТК по ЗИ **могут** включатся:

лица, имеющие допуск к государственной тайне;

руководители структурных подразделений Департамента, где непосредственно обрабатывается информация ограниченного доступа;

лицо, назначенное ответственным за организацию обработки информации ограниченного доступа в Департаменте (структурном подразделении Департамента);

мобилизационный работник;

руководитель структурного подразделения (штатный специалист) по защите информации в Департаменте.

Численность и персональный состав ПДТК по ЗИ определяются распорядительным документом по Департаменту.

15. Председателем ПДТК по ЗИ назначается лицо, из числа заместителей руководителя Департамента, ответственного за руководство работами по защите информации в Департаменте.

16. Председатель ПДТК по ЗИ несет ответственность за планирование и организацию работы комиссии.

17. Из членов ПДТК по ЗИ назначаются заместители председателя ПДТК по ЗИ и ее секретарь.

18. Секретарь ПДТК по ЗИ отвечает за подготовку заседаний ПДТК по ЗИ, оформляет протоколы ее заседаний, контролирует выполнение решений ПДТК по ЗИ и готовит отчеты о ее работе.

19. Деятельность ПДТК по ЗИ организуется и проводится в соответствии с перспективными и текущими планами работы ПДТК по ЗИ.

20. Планы работы ПДТК по ЗИ формируются под руководством председателя или одного из заместителей председателя ПДТК по ЗИ и утверждаются руководителем Департамента.

При необходимости вопросы, не нашедшие отражения в планах работы ПДТК по ЗИ, могут быть внесены на рассмотрение во внеплановом порядке.

21. Заседания ПДТК по ЗИ проводятся не реже одного раза в полгода. При необходимости на заседания ПДТК по ЗИ могут приглашаться компетентные в рассматриваемых на заседаниях вопросах специалисты и консультанты.

22. Рассмотрение вопросов, выносимых на заседания ПДТК по ЗИ, не должно приводить к необоснованному расширению круга лиц, допускаемых к сведениям по рассматриваемой тематике. Приглашенные присутствуют только при рассмотрении вопросов, для обсуждения которых они приглашены.

23. Материалы к обсуждению на заседаниях ПДТК по ЗИ готовятся секретарем или по его поручению иными соответствующими специалистами или консультантами.

24. По результатам заседаний ПДТК по ЗИ секретарем оформляются протоколы, которые подписываются председателем (заместителем председателя), присутствующими членами комиссии и секретарем ПДТК по ЗИ.

25. ПДТК по ЗИ правомочна принимать решения при наличии на заседании более половины членов ПДТК по ЗИ.

26. Решение считается принятым при голосовании за него большинства членов ПДТК по ЗИ, присутствующих на заседании.

IV. Полномочия ПДТК по ЗИ

ПДТК по ЗИ имеет право:

27. Знакомиться в установленном порядке с документами и материалами, необходимыми для выполнения возложенных на нее задач.

28. Привлекать в установленном порядке специалистов, имеющих непосредственное отношение к рассматриваемым проблемам, для более детального изучения отдельных вопросов, возникающих в процессе работы ПДТК по ЗИ, и выработки соответствующих рекомендаций и заключений.

29. Вносить руководству Департамента и подведомственных учреждений предложения о приостановлении действий организационных и распорядительных документов, противоречащих законодательству и иным нормативным актам, по вопросам, отнесенным к компетенции ПДТК по ЗИ.

30. Рассматривать проекты организационных и распорядительных документов Департамента по вопросам сохранения и защиты информации в Департаменте.

V. Контроль за работой ПДТК по ЗИ

31. ПДТК по ЗИ подотчетна руководителю Департамента.

32. Председатель ПДТК по ЗИ периодически, но не реже одного раза в год, заслушивается руководителем Департамента об итогах работы ПДТК по ЗИ и реализации ее предложений и рекомендаций.

33. Итоги работы ПДТК по ЗИ отражаются в годовых отчетах, направляемых в Управление защиты информации и специальной документальной связи Аппарата Губернатора Ханты-Мансийского автономного округа – Югры.

Приложение 3
к приказу Департамента промышленности Ханты-Мансийского автономного округа – Югры от 25.08.2017 №38-П-139

Состав комиссии по определению класса защищённости информационных систем и определения уровня защищённости персональных данных в Департаменте промышленности Ханты-Мансийского автономного округа – Югры

Роль	Должность	Ф.И.О.
Председатель комиссии	Заместитель директора Департамента	Киселев А.К.
Члены комиссии	Заместитель директора Департамента - начальник Управления правового и экономического регулирования	Шиповалов А.В.
	Начальник отдела автоматизации процесса Управления правового и экономического регулирования	Хаперский О.А.
	Начальник отдела промышленной политики и методологии	Торгашин Е.Ю.

Приложение 4
к приказу Департамента промышленности Ханты-Мансийского автономного округа – Югры от 25.08.2017 №38-П-139

ПРАВИЛА
обработки персональных данных

1. **Общие положения**

1.1. Правила обработки персональных данных в Департаменте промышленности Ханты-Мансийского автономного округа – Югры (далее – Правила) разработана в соответствии с Конституцией Российской Федерации, Федеральным законом Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», Трудовым кодексом Российской Федерации.

1.2. Правила определяют порядок и условия обработки персональных данных в Департаменте с использованием средств автоматизации и без использования таких средств.

1.3. Обработка персональных данных осуществляется в целях предоставления государственных и муниципальных услуг в соответствии с административными регламентами предоставления указанных услуг на основании соглашений, заключенных федеральными органами исполнительной власти и органами государственных внебюджетных фондов с Департаментом, обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, получении образования и продвижении по Департаменте, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

2. **Основные понятия, используемые в настоящих Правилах**

2.1. Информация - сведения (сообщения, данные) независимо от формы их представления.

2.2. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

2.3. Обработка персональных данных – 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.

2.4. Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

2.5. Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

2.6. Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

2.7. Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения

персональных данных).

2.8. Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

2.9. Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

2.10. Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

2.11. Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.12. Трансграничная передача персональных данных – передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

2.13. Автоматизированное рабочее место (АРМ) – совокупность информационно-программно-технических ресурсов, обеспечивающая конечному пользователю обработку данных и автоматизацию управленческих функций в конкретной предметной области.

3. **Принципы обработки персональных данных**

3.1. Обработка персональных данных осуществляется на законной основе.

3.2. Обработка персональных данных ограничивается достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

3.3. Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

3.4. Обработке подлежат только те персональные данные, которые отвечают целям их обработки.

3.5. Содержание и объем персональных данных соответствуют заявленным целям обработки. Обрабатываемые персональные данные не являются избыточным по отношению к заявленным целям обработки.

3.6. При обработке персональных данных обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Департаментом обеспечивается принятие необходимых мер по удалению или уточнению неполных или неточных данных.

3.7. Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

4. **Условия обработки персональных данных**

4.1. Обработка персональных данных осуществляется с соблюдением принципов и правил, предусмотренных Федеральным законом «О персональных данных». Обработка персональных данных допускается в следующих случаях:

4.1.1. Обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных;

4.1.2. Обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом для осуществления и выполнения возложенных законодательством Российской Федерации на Департамент функций, полномочий и обязанностей;

4.1.3. Обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных Федеральным законом от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», включая регистрацию субъекта персональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг;

4.1.4. Обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

4.1.5. Обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

4.1.6. Обработка персональных данных необходима для осуществления прав и законных интересов Департамента или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных;

4.1.7. Осуществляется обработка персональных данных, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных либо по его просьбе;

4.1.8. Осуществляется обработка персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

4.2. В случае если Департамент поручает обработку персональных данных другому лицу, ответственность перед субъектом персональных данных за действия указанного лица несет Департамент. Лицо, осуществляющее обработку персональных данных по поручению Департамента, несет ответственность перед Департаментом.

5. **Конфиденциальность персональных данных**

5.1. Департамент и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

6. **Право субъекта персональных данных на доступ к его персональным данным**

6.1. Субъект персональных данных имеет право на получение сведений, указанных в п. 6.7 настоящих Правил, за исключением случаев, при которых доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц. Субъект персональных данных вправе требовать от Департамента уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

6.2. Сведения, указанные в п. 6.7 настоящей Правил, должны быть предоставлены субъекту персональных данных Департаментом в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

6.3. Сведения, указанные в п. 6.7 настоящих Правил, предоставляются субъекту персональных данных или его представителю Департаментом при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с Департаментом (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Департаментом, подпись субъекта персональных данных или его представителя Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

6.4. В случае если сведения, указанные в п. 6.7 настоящих Правил, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к Департаменту или направить ему повторный запрос в целях получения сведений, указанных в п. 6.7 настоящего положения, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

6.5. Субъект персональных данных вправе обратиться повторно к Департаменту или направить ему запрос в целях получения сведений, указанных в п. 6.7 настоящих Правил, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в п. 6.4 настоящих Правил, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в п. 6.3 настоящих Правил, должен содержать основание направления повторного запроса.

6.6. Департамент вправе отказать субъекту персональных данных в выполнении повторного запроса, несоответствующего условиям, предусмотренным п. 6.3 и п. 6.4.

настоящих Правил. Такой отказ должен быть мотивированным. Обязанность предоставления доказательств обоснованности отказа в выполнении повторного запроса лежит на Департаменте.

6.7. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

6.7.1. Подтверждение факта обработки персональных данных Департаментом;

6.7.2. Правовые основания и цели обработки персональных данных;

6.7.3. Цели и применяемые Департаментом способы обработки персональных данных;

6.7.4. Наименование и местонахождение Департамента, сведения о лицах (за исключением работников Департамента), которые имеют доступ к персональным данным или которые могут быть раскрыты персональные данные на основании договора с Департаментом или на основании федерального закона;

6.7.5. Обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок предоставления таких данных не предусмотрен федеральным законом;

6.7.6. Сроки обработки персональных данных, в том числе сроки их хранения;

6.7.7. Порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных»;

6.7.8. Информацию об осуществленной или о предполагаемой трансграничной передаче данных;

6.7.9. Наименование или имя, фамилию, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Департамента, если обработка поручена или будет поручена такому лицу.

6.7.10. Иные сведения, предусмотренные Федеральным законом «О персональных данных» или другими федеральными законами.

7. **Право на обжалование действий или бездействий Департамента**

7.1. Если субъект персональных данных считает, что Департамент осуществляет обработку его персональных данных с нарушением требований Федерального закона «О персональных данных» или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействия Департамента в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

7.2. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

8. **Обязанности Департамента при сборе персональных данных**

8.1. При сборе персональных данных Департамент обязан предоставить субъекту персональных данных по его просьбе информацию, предусмотренную частью 6.7 настоящих Правил.

8.2. Если предоставление персональных данных является обязательным в соответствии с федеральным законом, Департамент обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

8.3. Если персональные данные получены не от субъекта персональных данных, Департамент, за исключением случаев, предусмотренных п. 8.4 настоящих Правил, до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию:

8.3.1. Наименование либо фамилия, имя, отчество и адрес Департамента или его представителя;

8.3.2. Цель обработки персональных данных и ее правовое основание;

8.3.3. Предполагаемые пользователи персональных данных;

8.3.4. Установленные настоящим Федеральным законом права субъекта персональных данных;

8.3.5. Источник получения персональных данных.

8.4. Департамент освобождается от обязанности предоставить субъекту персональных данных сведения, предусмотренные п. 8.3 настоящего Положения, в случаях, если:

8.4.1. Субъект персональных данных уведомлен об осуществлении обработки его персональных данных Департаментом;

8.4.2. Персональные данные получены Департаментом на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;

8.4.3. Персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника;

8.4.4. Предоставление субъекту персональных данных сведений, предусмотренных частью 8.3 настоящих Правил, нарушает права и законные интересы третьих лиц.

9. **Меры направленные на обеспечение выполнения Департаментом обязанностей, предусмотренных Федеральным законом «О персональных данных»**

9.1. Назначен ответственный за организацию обработки персональных данных.

9.2. Изданы документы, определяющие правила обработки персональных данных, локальные акты по вопросам обработки персональных данных, локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

9.3. Утверждены правила проведения внутреннего контроля соответствия обработки персональных данных требованиям Федерального закона «О персональных данных» и принятых в соответствии с ним нормативных правовых актов, настоящих Правил, локальным актам.

9.4. Проведена оценка вреда, который может быть причинен субъектам персональных данных, соотношение указанного вреда и применяемых Департаментом мер.

9.5. Проведено ознакомление работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе документами, определяющими политику Департамента в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных.

10. **Меры по обеспечению безопасности персональных данных при их обработке**

10.1. Определены угрозы безопасности персональных данных при их обработке в информационных системах персональных данных.

10.2. Применяются организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимые для выполнения требований к защите персональных данных.

10.3. Применяются прошедшие в установленном порядке процедуру оценки соответствия средства защиты информации.

10.4. Проведена оценка соответствия принимаемых мер по обеспечению безопасности персональных данных, получен аттестат соответствия требованиям по безопасности информации.

10.5. Ведется учет машинных носителей персональных данных.

10.6. Выполняются меры по обнаружению фактов несанкционированного доступа к персональным данным и принятию соответствующих мер.

10.7. Определен комплекс мер по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

10.8. Установлены правила доступа к персональным данным, обрабатываемым в информационных системах персональных данных, обеспечена регистрация и учет всех действий, совершаемых с персональными данными в информационных системах персональных данных.

10.9. Осуществляется контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровнем защищенности информационных систем персональных данных.

11. **Порядок управления учетными записями**

11.1. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику, допущенному к работе на компьютерах конкретной ИСПДн, должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать на данном компьютере.

11.2. Использование несколькими сотрудниками при работе в ИСПДн одного и того же имени пользователя («группового имени») запрещено.

11.3. Процедура регистрации (создания учетной записи) пользователя и предоставления ему (или изменения его) прав доступа к ресурсам ИСПДн инициируется заявкой ответственного за эксплуатацию данной ИСПДн.

В заявке указывается:

- содержание запрашиваемых изменений (регистрация нового пользователя ИСПДн, удаление учетной записи пользователя, расширение или сужение полномочий и прав доступа к ресурсам ИСПДн ранее зарегистрированного пользователя);
- должность (с полным наименованием отдела), фамилия, имя и отчество сотрудника;
- имя пользователя (учетной записи) данного сотрудника;
- полномочия, которых необходимо лишить пользователя или которые необходимо добавить пользователю (путем указания решаемых пользователем задач в ИСПДн).

11.4. Заявку рассматривает руководитель или ответственный за организацию обработки персональных данных в Департаменте, визируя ее, утверждая тем самым

производственную необходимость допуска (изменения прав доступа) данного сотрудника к необходимым для решения им указанных в заявке задач ресурсам ИСПДн, затем подписывает задание администратору защиты информации на внесение необходимых изменений в списки пользователей соответствующих подсистем ИСПДн.

11.5. На основании задания, в соответствии с документацией на средства защиты от несанкционированного доступа, администратор производит необходимые операции по созданию (удалению) учетной записи пользователя, присвоению ему начального значения пароля (возможно также регистрацию персонального идентификатора), заявленных прав доступа к ресурсам ИСПДн и другие необходимые действия, указанные в задании. Для всех пользователей должен быть установлен режим принудительного запроса смены пароля не реже одного раза в течение 90 дней.

11.6. После внесения изменений в списки пользователей администратор информационной безопасности должен обеспечить настройки средств защиты, соответствующие требованиям безопасности указанной ИСПДн. По окончании внесения изменений в списки пользователей в заявке делается отметка о выполнении задания за подписью исполнителя - администратора информационной безопасности.

11.7. Сотруднику, зарегистрированному в качестве нового пользователя ИСПДн, сообщается имя соответствующего ему пользователя и может выдаваться персональный идентификатор (для работы в режиме усиленной аутентификации) и начальное (-ые) значение (-ия) пароля (-ей), которое (-ые) он обязан сменить при первом же входе в систему.

11.8. Исполненные, подписанные заявка и задание находится на хранении у администратора информационной безопасности **в течении 6месяцев** после увольнения (блокировки) работника.

Они могут впоследствии использоваться:

- для восстановления полномочий пользователей после аварий ИСПДн;
- для контроля правомерности наличия у конкретного пользователя прав доступа к тем или иным ресурсам ИСПДн при разборе конфликтных ситуаций;
- для проверки сотрудниками контролирующих органов правильности настройки средств разграничения доступа к ресурсам ИСПДн.

11.9. При наступлении момента прекращения срока действия полномочий пользователя (окончание договорных отношений, увольнение сотрудника) учетная запись должна немедленно блокироваться.

11.10. Блокирование сеанса доступа в ИСПДн, **после 15 минут времени бездействия** (неактивности) пользователя или по его запросу. Блокирование сеанса доступа пользователя в ИСПДн обеспечивает временное приостановление работы пользователя с СВТ, с которого осуществляется доступ к ИСПДн. Для заблокированного сеанса осуществляется блокирование любых действий по доступу к информации и устройствам отображения, кроме необходимых для разблокирования сеанса. Блокирование сеанса доступа пользователя в ИСПДн сохраняется до прохождения им повторной идентификации и аутентификации.

11.11. Запрет всех действий пользователей до прохождения процедур идентификации и аутентификации в ИСПДн (кроме необходимых для прохождения процедур идентификации и аутентификации). Администратору ИБ разрешаются действия в обход установленных процедур идентификации и аутентификации, необходимые только для восстановления функционирования ИСПДн в случае сбоев в работе или выходе из строя отдельных ТС (устройств).

11.12. Ответственный за хранение, выдачу, инициализацию, блокирование средств аутентификации и принятия мер в случае утраты и (или) компрометации средств аутентификации является администратор ИБ.

Таблица 1

1.Перечень программного обеспечения, разрешенного к установке на рабочее место пользователя

№ п/п	Тип ПО	Наименование ПО
1.	Операционная система	Microsoft Windows 7 Professional Сертифицированная ФСТЭК России операционная система семейства Линукс (АСТРА Линукс, BaseAlt...)
2.	Пакет офисных приложений	Microsoft Office 2007 и выше Libreoffice 5.2 и выше
3.	Почтовая программа	Mozilla Thunderbird версии 51 и выше
4.	Браузер	Internet Explorer 9 и выше
		Mozilla Firefox 51 и выше
5.	Система электронного документооборота*	Клиентская часть «СЭД ДЕЛО»
5.	Архиватор	7-Zip
6.	Средство работы с PDF файлами	Acrobat Reader версии 9 и выше
		Foxit reader версии 4.0 и выше
7.	Антивирусное программное обеспечение	Dr.web версии 10.0 и выше
8.	Географическая информационная система (ГИС), предназначена для сбора, хранения, отображения, редактирования и анализа пространственных данных	Мапинфо (Mapinfo) версии 12 и выше
9.	Векторные программы	CorelDraw Graphics Suit версии 4 и выше
10.	Программы распознавания текста	ABBYY FineReader версии 8.0 и выше

Примечание *: использование ПО определяется необходимостью работы в информационной системе с использование толстого клиента.

Приложение 5
к приказу Департамента промышленности
Ханты-Мансийского автономного округа – Югры
от 25.08.2017 №38-П-139

Положение
об организации режима обеспечения безопасности помещений, в которых размещены информационные системы, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения

1. Общие положения

1.1. Положение об организации режима обеспечения безопасности помещений, в которых размещены ИС Департамента, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения (далее – Положение) разработано в соответствии с Постановлением правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

1.2. Защита от проникновения посторонних лиц в помещения Департамента обеспечивается организацией порядка доступа.

2. Границы контролируемой зоны

2.1. Контролируемая зона – границы пространства (территория, здание, часть здания, кабинет), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска.

2.2. План-схемы контролируемой зоны помещений приведены в приложении 1 к настоящему положению.

3. Порядок доступа в помещения

3.1. Список лиц, доступ которых в помещения, находящиеся в пределах границы контролируемой зоны, необходим для выполнения ими служебных (трудовых обязанностей), приведен в приложении 3 к настоящему приказу.

3.2. Неконтролируемое пребывание лиц в помещениях, находящихся в пределах границы контролируемой зоны, указанных в п. 3.1 настоящего Положения, разрешено в период рабочего времени в соответствии с утвержденным графиком работы Департамента, либо вне периода рабочего времени с письменного разрешения ответственного за организацию обработки персональных данных или ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных.

3.3. Лица, не указанные в п. 3.1 настоящего Положения допускаются в помещения в присутствии лиц, доступ которых в помещения, находящиеся в пределах границы контролируемой зоны, необходим для выполнения ими служебных (трудовых обязанностей).

Приложение 1

План-схема границ контролируемой зоны Департамента промышленности Ханты-Мансийского автономного округа – Югры

Адрес: ул. Студенческая, дом 2, г.Ханты-Мансийск,
Ханты-Мансийский автономный округ - Югра, Тюменская область, 628007

СХЕМА КОНТРОЛИРУЕМОЙ ЗОНЫ

- - - - - - - граница контролируемой зоны

Приложение 2

План-схема границ контролируемой зоны Департамента промышленности Ханты-Мансийского автономного округа – Югры

Адрес: ул. Рознина, дом 64, г.Ханты-Мансийск,
Ханты-Мансийский автономный округ - Югра, Тюменская область, 628011

СХЕМА КОНТРОЛИРУЕМОЙ ЗОНЫ

- - - - - - - - граница контролируемой зоны

Приложение 6
к приказу Департамента промышленности
Ханты-Мансийского автономного округа – Югры
от 25.08.2017 №38-П-139

Перечень
должностей Департамента промышленности Ханты-Мансийского автономного округа – Югры, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, в случае обезличивания персональных данных.

№ п/п	Должность
1	Заместитель директора Департамента-начальник Управления правового и экономического регулирования
2	Заместитель начальника управления правового и экономического регулирования
3	Начальник Управления промышленной политики
4	Начальник отдела отраслевых секторов промышленности
5	Начальник отдела промышленной политики и методологии
6	Начальник отдела автоматизации процесса
7	Начальник управления агропромышленного комплекса
8	Начальник отдела поддержки научно-технической деятельности и инноваций
9	Заместитель начальника управления - начальник отдела по обращению с отходами
10	Начальник отдела реализации программ
11	Начальник отдела развития пищевой промышленности
12	Начальник управления туризма
13	Начальник отдела развития туризма
14	Заместитель начальника управления - начальник отдела мониторинга туризма и межрегионального сотрудничества
15	Начальник отдела правового регулирования
16	Начальник отдела экономики

Приложение 7
к приказу Департамента промышленности
Ханты-Мансийского автономного округа – Югры
от 25.08.2017 №38-П-139

Перечень
должностей Департамента промышленности Ханты-Мансийского автономного округа – Югры, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным

№	Должность
1.	**Директор Департамента**
2.	**Первый заместитель директора Департамента**
3.	**Заместитель директора Департамента**
4.	**Заместитель директора Департамента-начальник Управления правового и экономического регулирования**
5.	Помощник директора Департамента
6.	Секретарь приемной руководителя
7.	**Начальник Управления промышленной политики**
8.	**Начальник отдела отраслевых секторов промышленности**
9.	**Заместитель начальника отдела отраслевых секторов промышленности**
10.	Консультант отдела отраслевых секторов промышленности
11.	Главный специалист — эксперт отдела отраслевых секторов промышленности
12.	**Начальник отдела промышленной политики и методологии**
13.	**Заместитель начальника отдела промышленной политики и методологии**
14.	Консультант отдела промышленной политики и методологии
15.	Главный специалист-эксперт отдела промышленной политики и методологии
16.	**Начальник отдела поддержки научно-технической деятельности и инноваций**
17.	Консультант отдела поддержки научно-технической деятельности и инноваций
18.	Главный специалист-эксперт отдела поддержки научно-технической деятельности и инноваций
19.	**Заместитель начальника управления - начальник отдела по обращению с отходами**
20.	Консультант отдела по обращению с отходами
21.	**Начальник управления агропромышленного комплекса**
22.	**Заместитель начальника управления - начальник отдела развития агропромышленного комплекса**
23.	Консультант отдела развития агропромышленного комплекса
24.	Главный специалист-эксперт отдела развития агропромышленного комплекса
25.	Эксперт отдела развития агропромышленного комплекса
26.	**Начальник отдела реализации программ**
27.	**Заместитель начальника отдела реализации программ**
28.	Консультант отдела реализации программ
29.	Главный специалист-эксперт отдела реализации программ

30.	Эксперт отдела реализации программ
31.	**Начальник отдела развития пищевой промышленности**
32.	**Заместитель начальника отдела развития пищевой промышленности**
33.	Консультант отдела развития пищевой промышленности
34.	Главный специалист-эксперт отдела развития пищевой промышленности
35.	**Начальник управления туризма**
36.	**Начальник отдела развития туризма**
37.	Консультант отдела развития туризма
38.	Главный специалист-эксперт отдела развития туризма
39.	**Заместитель начальника управления - начальник отдела мониторинга туризма и межрегионального сотрудничества**
40.	Консультант отдела мониторинга туризма и межрегионального сотрудничества
41.	Главный специалист-эксперт отдела мониторинга туризма и межрегионального сотрудничества
42.	**Заместитель начальника управления правового и экономического регулирования**
43.	**Начальник отдела правового регулирования**
44.	**Заместитель начальника отдела правового регулирования**
45.	Консультант отдела правового регулирования
46.	Юрист отдела правового регулирования
47.	**Начальник отдела экономики**
48.	Консультант отдела экономики
49.	**Начальник отдела автоматизации процесса**
50.	Консультант отдела автоматизации процесса

Приложение 8
к приказу Департамента промышленности
Ханты-Мансийского автономного округа – Югры
от 25.08.2017 №38-П-139

Перечень информационных систем персональных данных

№ п/п	Наименование	Адрес расположения
1	Сегмент информационной системы «Территориальная информационная система и Система автоматизации делопроизводства и электронного документооборота "Дело" Департамента промышленности Ханты-Мансийского автономного округа – Югры	ул. Студенческая, дом 2, г.Ханты-Мансийск, Ханты-Мансийский автономный округ - Югра, Тюменская область, 628007
		ул. Рознина, дом 64, г.Ханты-Мансийск, Ханты-Мансийский автономный округ - Югра, Тюменская область, 628011

Приложение 9
к приказу Департамента промышленности
Ханты-Мансийского автономного округа – Югры
от 25.08.2017 №38-П-139

ПЕРЕЧЕНЬ

обрабатываемых персональных данных

Таблица 1. Перечень обрабатываемых персональных данных

Группа персональных данных	Состав персональных данных	Цели обработки персональных данных
Сведения о гражданах	1) фамилия, имя и отчество; 2) число, месяц, год и место рождения; 3) адрес и дата регистрации по месту жительства (месту пребывания); 4) вид, серия, номер документа, удостоверяющего личность; 5) номер контактного телефона или сведения о других способах связи.	Обеспечение соблюдения законов и иных нормативно-правовых актов, заключения и исполнения обязательств по гражданско-правовым договорам, пользования различного вида льготами, заполнения первичной статистической документации. Для предоставления государственной или муниципальной услуги в соответствии с Федеральным законом от 27 июля 2010 года № 210-ФЗ. Осуществление контроля за сроками исполнения поручений в системе автоматизации делопроизводства и электронного документооборота «Дело».

Таблица 2. Правовое основание обработки персональных данных и сроки их хранения

Категория персональных данных	Основание для обработки персональных данных
Специальные категории ПДн	Конституция Российской Федерации, Трудовой кодекс Российской Федерации, Федеральный закон от 27.07.2006 года № 152-ФЗ «О персональных данных»

Приложение 10
к приказу Департамента промышленности
Ханты-Мансийского автономного округа – Югры
от 25.08.2017 №38-П-139

ИНСТРУКЦИЯ
ответственного за организацию обработки персональных данных

1. Общие положения

Настоящая инструкция определяет права, обязанности и ответственность лица, ответственного за организацию обработки персональных данных.

Ответственный за организацию обработки персональных данных в своей деятельности руководствуется:

- Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 01.11.2012 № 1119;
- Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным постановлением Правительства Российской Федерации от 15.09.2008 № 687;
- Приказом Федеральной Департамента по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

2. Обязанности

Ответственный за организацию обработки персональных данных обязан:

- Доводить до сведения работников положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к обеспечению безопасности персональных данных;
- Осуществлять внутренний контроль за соблюдением Департаментом и его работниками законодательства Российской Федерации о персональных данных, а именно организовывать проведение периодических (не менее одного раза в год) проверок соответствия обработки персональных данных. О результатах проведенной проверки и мерах, необходимых для устранения выявленных нарушений, докладывать непосредственному руководителю в письменном виде;
- Организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и/или осуществлять контроль за приемом и обработкой таких обращений и запросов.

3. Ответственность

За неисполнение (ненадлежащее исполнение) своих должностных обязанностей, предусмотренных настоящей инструкцией, ответственный за организацию обработки персональных данных несет персональную ответственность в соответствии с законодательством Российской Федерации.

4. Права

Ответственный за организацию обработки персональных данных имеет право:

- Требовать от работников письменных объяснений по фактам нарушения ими требований законодательства Российской Федерации, локальных актов о персональных данных и защите персональных данных;
- Вносить предложения непосредственному руководителю об отстранении работников от обработки персональных данных, применению к ним дисциплинарных взысканий, при обнаружении нарушения ими требований законодательства Российской Федерации, локальных актов по вопросам обработки персональных данных или требований к защите персональных данных.

Приложение 11
к приказу Департамента промышленности
Ханты-Мансийского автономного округа – Югры
от 25.08.2017 №38-П-139

ИНСТРУКЦИЯ
ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных

1. Общие положения

Настоящая инструкция определяет права и обязанности лица, ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных (далее – ИСПДн).

Лицо ответственное за обеспечение безопасности персональных данных в ИСПДн (далее – администратор информационной безопасности) это лицо, отвечающее за обеспечение заданных характеристик информации, содержащей персональные данные (конфиденциальности, целостности и доступности) в процессе их обработки в ИСПДн.

Администратор информационной безопасности в ИСПДн осуществляет контроль за выполнением требований нормативно-правовых и организационно-распорядительных документов по организации обработки и обеспечению безопасности персональных данных при их обработке в ИСПДн с использованием автоматизированных рабочих мест.

Администратор информационной безопасности является ответственным пользователем СКЗИ.

2. Обязанности администратора информационной безопасности

Администратор информационной безопасности обязан:

- Знать требования нормативно-правовых и организационно-распорядительных документов по обеспечению безопасности персональных данных при их обработке в ИСПДн;
- Знать перечень обрабатываемых персональных данных, состав, структуру, назначение и выполняемые задачи ИСПДн, а также состав информационных технологий и технических средств, позволяющих осуществлять обработку персональных данных;
- Уметь пользоваться средствами защиты информации и осуществлять их непосредственное администрирование;
- Осуществлять резервное копирование информации, содержащей персональные данные (при необходимости);
- Обязан осуществлять периодический контроль за выполнением работниками, эксплуатирующими ИСПДн (пользователями ИСПДн), мероприятий по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн;
- Участвовать в работе по проведению внутреннего контроля соответствия обработки персональных данных требованиям по защите информации;
- Обязан обеспечивать строгое выполнение требований по обеспечению защиты информации при организации технического обслуживания АРМ;
- Обязан вести журнал учета средств защиты информации, используемых в ИСПДн;

- Обязан присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию АРМ;
- Обязан проводить инструктаж пользователей ИСПДн по правилам работы с используемыми техническими средствами и средствами защиты информации в соответствии с технической документацией на используемые средства защиты;
- Обязан проводить мероприятия по организации антивирусной защиты;
- Организовать защиту информации при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны;
- Осуществлять организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль за действиями пользователей при работе с паролями, согласно инструкции по организации парольной защиты в информационных системах персональных данных;
- Выполнять своевременное обновление программного обеспечения элементов ИСПДн и средств защиты персональных данных в ручном режиме по мере появления таких обновлений;
- Обязан организовать ведение журнала учета машинных носителей информации, использующихся в ИСПДн для обработки, хранения и транспортировки информации;
- Осуществлять хранение, выдачу, инициализацию, блокирование средств аутентификации и принятие мер в случае утраты или компрометации средств аутентификации;
- Выполнять проверку электронных журналов средств защиты информации и штатных журналов операционной системы на наличие ошибок, состава и времени изменений, которые привели к изменению состояния защищенности или к несанкционированному доступу;
- Реагировать на сбои при регистрации событий безопасности согласно инструкции по работе с инцидентами информационной безопасности.
- Обязан немедленно сообщать ответственному за организацию обработки персональных данных информацию об имевших место попытках несанкционированного доступа к информации и техническим средствам АРМ, а также принимать необходимые меры по устранению нарушений:
- Установить причины, по которым стал возможным НСД;
- Установить последствия, к которым привел НСД;
- Зафиксировать случай НСД в виде документа (акта, служебной записки и т.д.) с описанием причин НСД, предполагаемых или установленных нарушителей и последствий;
- Провести проверку настроек средств защиты информации и операционных систем на соответствие требованиям руководящих документов и разрешительной системы доступа пользователей к защищаемым информационным ресурсам и объектам доступа ИСПДн, при необходимости провести настройку;
- Осуществлять контроль состава технических средств, программного обеспечения и средств защиты информации;
- Провести инструктаж пользователей ИСПДн по выполнению требований по обеспечению защиты персональных данных.

3. Права администратора информационной безопасности.

Администратор информационной безопасности имеет право:

- Требовать от пользователей ИСПДн соблюдения установленной технологии обработки информации и выполнения инструкции о порядке работы пользователей в ИСПДн в части обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных;
- Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИСПДн;
- Обращаться за необходимыми разъяснениями по вопросам обработки и обеспечения безопасности персональных данных к ответственному за организацию обработки персональных данных в ИСПДн и/или ответственному за эксплуатацию ИСПДн;

4. Ответственность администратора информационной безопасности

На администратора информационной безопасности возлагается персональная ответственность за качество проводимых им работ по обеспечению безопасности ПДн в ИСПДн;

Администратор информационной безопасности в ИСПДн несет ответственность в соответствии с действующим законодательством Российской Федерации.

Приложение 12
к приказу Департамента промышленности
Ханты-Мансийского автономного округа – Югры
от 25.08.2017 №38-П-139

ИНСТРУКЦИЯ
по организации резервирования

1. Общие положения

Настоящая инструкция разработана с целью обеспечения возможности оперативного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

Инструкция определяет правила и объемы резервирования, а также порядок восстановления работоспособности информационной системы персональных данных (далее – ИСПДн).

2. Резервируемое программное обеспечение и базы персональных данных

В ИСПДн резервированию подлежит:

- Общее программное обеспечение (операционная система и программные драйверы устройств (принтера, монитора, видеокарты и т.п.), поставляемые с компонентами автоматизированных рабочих мест (далее – АРМ), входящими в состав ИСПДн);
- Прикладное программное обеспечение, используемое для обработки персональных данных (средства обработки текстов и таблиц, специализированные программы и т.п.);
- Базы персональных данных (тестовые и табличные файлы, а также файлы баз данных специализированных программ);
- Программное обеспечение средств защиты информации, в том числе средств антивирусной защиты.

3. Порядок резервирования и хранения резервных копий

Резервирование общего и прикладного программного обеспечения, а также программного обеспечения средств защиты информации обеспечивается путем хранения у администратора информационной безопасности в ИСПДн машинных носителей информации, содержащих дистрибутивы данного программного обеспечения.

Машинные носители информации обновлений общего и прикладного программного обеспечения, а также программного обеспечения средств защиты информации должны также храниться у администратора информационной безопасности в ИСПДн.

Допускается хранение машинных носителей прикладного программного обеспечения и машинных носителей с обновлениями к нему в структурных подразделениях, эксплуатирующих ИСПДн.

Резервирование баз персональных данных, а также текстовых и табличных файлов, содержащих персональные данные, допускается только на учтенные установленным порядком машинные носители информации.

Резервирование осуществляется ежемесячно.

Резервные носители персональных данных хранятся в структурных подразделениях, эксплуатирующих ИСПДн, в порядке, предусмотренном для носителей информации персональных данных.

К резервному носителю персональных данных должна быть приложена учетная карточка, в которой делаются отметки о дате резервирования.

Резервные носители персональных данных не могут быть переданы за пределы структурных подразделений, эксплуатирующих ИСПДн.

Копирование информации с резервных носителей персональных данных, за исключением случая восстановления работоспособности ИСПДн, запрещается.

4. Порядок восстановления работоспособности ИСПДн

Восстановление работоспособности ИСПДн осуществляется в случаях сбоев, отказов и аварий технических средств и систем ИСПДн, а также ее программного обеспечения.

При восстановлении работоспособности средств защиты информации следует выполнить их настройку в соответствии с требованиями безопасности информации, предъявляемым к определенному уровню защищенности персональных данных и классу защищенности информационной системы.

Восстановление средств защиты информации производится с использованием эталонных сертифицированных дистрибутивов, которые хранятся в хранилище. После успешной настройки средств защиты информации необходимо выполнить резервное копирование настроек данных средств с помощью встроенных в них функций.

В случае необходимости привлечения для восстановления работоспособности ИСПДн представителей сторонних организаций, должна быть обеспечена невозможность их ознакомления с персональными данными. Ответственность за выполнение данного требования возлагается на администратора информационной безопасности в ИСПДн и руководителя структурного подразделения, обеспечивающего ее эксплуатацию.

Учетная карточка резервного носителя персональных данных

№ _____

Дата резервного копирования	**Объект копирования**	**Кто производил копирование**	**Подпись**

Приложение 13
к приказу Департамента промышленности
Ханты-Мансийского автономного округа – Югры
от 25.08.2017 №38-П-139

ИНСТРУКЦИЯ
по организации парольной защиты

Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей в информационных системах персональных данных (далее – ИСПДн), а также контроль за действиями пользователей при работе с паролями.

Личные пароли генерируются и распределяются централизованно Администратором информационной безопасности:

- Длина пароля должна быть не менее 8 символов;
- В числе символов пароля обязательно должны присутствовать буквы, цифры и/или специальные символы (@, #, $, &, *, % и т.п.);
- Символы паролей должны вводиться в режиме латинской раскладки клавиатуры;
- Пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);
- При смене пароля новое значение должно отличаться от предыдущих;
- При смене пароля должны быть изменены не менее 3 символов;
- Пользователь не имеет права сообщать личный пароль другим лицам;

Полная плановая смена паролей пользователей ИСПДн должна проводиться регулярно, не реже одного раза в 3 месяца.

Внеплановая смена личного пароля или удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий (увольнение и т.п.) должна производиться администратором информационной безопасности в ИСПДн немедленно после окончания последнего сеанса работы данного пользователя ИСПДн с системой на основании письменного указания непосредственного руководителя структурного подразделения.

Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение и другие обстоятельства) администратора информационной безопасности в ИСПДн.

В случае компрометации (утеря, передача другому лицу) личного пароля, Пользователь ИСПДн обязан незамедлительно сообщить об этом администратору информационной безопасности для принятия соответствующих мер.

В случае 3-х кратного ввода не верного пароля пользователя ИСПДн должна осуществляться перезагрузка АРМ.

В случае 15-ти кратного ввода не верного ПИН аппаратного идентификатора пользователя, идентификатор должен быть заблокирован.

Приложение 14
к приказу Департамента промышленности
Ханты-Мансийского автономного округа – Югры
от 25.08.2017 №38-П-139

ИНСТРУКЦИЯ
по организации антивирусной защиты

1. Общие требования

Настоящая инструкция определяет требования к организации антивирусной защиты информационных систем персональных данных (далее – ИСПДн) от разрушающего воздействия вирусов и вредоносных программ и устанавливает ответственность руководителя и работников структурных подразделений, эксплуатирующих и сопровождающих ИСПДн, за их выполнение. Инструкция распространяется на все существующие и вновь разрабатываемые ИСПДн. Для отдельных ИСПДн могут быть разработаны свои инструкции, учитывающие особенности работы.

К использованию в ИСПДн допускаются только лицензионные антивирусные средства, закупленные у разработчиков (поставщиков) указанных средств.

Установка и настройка средств антивирусного контроля осуществляется специалистами БУ Ханты-Мансийского автономного округа - Югры "Окружной центр информационно-коммуникационных технологий" под контролем администратором информационной безопасности в ИСПДн или специально назначенным лицом в соответствии с эксплуатационной документацией на антивирусные средства.

2. Применение средств антивирусного контроля

При загрузке АРМ в автоматическом режиме должен проводиться антивирусный контроль служб операционной системы, исполняемых приложений, находящихся в автозагрузке, реестра операционной системы.

Полному антивирусному контролю автоматизированные рабочие места (АРМ) должны подвергаться не реже одного раза в неделю.

Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, оптических и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень эффективности контроля. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

Файлы, помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц.

Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов и других вредоносных программ. Непосредственно после установки (изменения) программного обеспечения, администратором информационной безопасности в ИСПДн должна быть выполнена антивирусная проверка на защищаемых серверах и пользовательских АРМ.

При возникновении подозрения на наличие вируса либо вредоносной программы (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) работник структурного подразделения самостоятельно или вместе с администратором информационной безопасности в ИСПДн должен провести внеочередной антивирусный контроль своего АРМ.

В случае обнаружения при проведении антивирусной проверки зараженных вирусами либо вредоносными программами файлов, необходимо:

- Приостановить работу в ИСПДн;
- Немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя структурного подразделения и администратора информационной безопасности в ИСПДн, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;
- Совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- Провести лечение или уничтожение зараженных файлов.

3. Обновление баз САВЗ

Обновление баз средств антивирусной защиты (далее САВЗ) на АРМ ИСПДн, не имеющих подключения к локальной вычислительной сети (ЛВС) Департамента и сетям связи общего пользования, осуществляется администратором сегмента ИСПДн вручную с использованием учтенных носителях информации, в обязательном порядке проверяемых САВЗ перед их использованием или подключением к АРМ ИСПДн, еженедельно.

Обновление баз САВЗ на АРМ ИСПДн, не имеющих подключения к ЛВС Департамента, но подключенных к сетям связи общего пользования, осуществляется ежедневно в установленное время с официального сервера обновлений производителя САВЗ.

При централизованном управлении антивирусной защитой консоль (сервер) администрирования ежедневно в установленное время обновляет базы САВЗ с официального сервера обновлений производителя САВЗ и размещает их в общедоступное для АРМ ИСПДн хранилище.

Обновление баз САВЗ на АРМ ИСПДн, подключенных к ЛВС Департамента, осуществляется ежедневно в установленное время из общедоступного хранилища консоли (сервера) администрирования.

При локальном управлении антивирусной защитой роль консоли (сервера) администрирования по обновлению баз САВЗ и их размещению в общедоступное хранилище выполняет САВЗ, установленное на одном из АРМ ИСПДн.

4. Ответственность

Ответственность за проведение мероприятий антивирусного контроля в подразделениях и соблюдение требований настоящей Инструкции возлагается на администратора информационной безопасности в ИСПДн и всех работников, являющихся пользователями ИСПДн.

Приложение 15
к приказу Департамента промышленности
Ханты-Мансийского автономного округа – Югры
от 25.08.2017 №38-П-139

ИНСТРУКЦИЯ
о пропускном и внутриобъектовом режимах

1. Общие положения

Данная Инструкция регламентирует условия и порядок осуществления доступа лиц в помещения со средствами ИС в Департаменте промышленности Ханты-Мансийского автономного округа – Югры в целях обеспечения предотвращения несанкционированного доступа к персональным данным (далее – ПДн). При обеспечении доступа лиц соблюдаются требования по защите ПДн.

Обеспечение доступа лиц в помещения предусматривает комплекс специальных мер, направленных на поддержание и обеспечение установленного порядка деятельности подразделений и определяет порядок пропуска сотрудников Департамента промышленности Ханты-Мансийского автономного округа – Югры, сотрудников иных организаций и учреждений, граждан в помещения.

Контроль за порядком обеспечения доступа лиц в помещения отделов возлагается на руководителей подразделений.

Помещения и оборудование размещены таким образом, чтобы исключить возможность бесконтрольного проникновения в данные помещения и к данному оборудованию посторонних лиц.

2. Организация пропускного и внутриобъектового режима

Пропускной режим в Департаменте промышленности Ханты-Мансийского автономного округа – Югры устанавливается в целях:

- исключения фактов хищений собственности;
- исключения фактов вандализма со стороны недобросовестных посетителей;
- исключения возможности несанкционированного доступа персонала и посетителей в помещения.

Внутриобъектовый режим устанавливается в целях:

- соблюдения персоналом и посетителями правил внутреннего распорядка и пожарной безопасности;
- установления порядка допуска персонала в помещения ограниченного доступа предприятия;
- исключения возможности бесконтрольного передвижения посетителей по территории предприятия.

Надёжность пропускного и внутриобъектового режимов достигается:

- осуществлением контроля за перемещением персонала;
- осуществлением охраны помещений предприятия силами сторожей-вахтеров, ЧОП;
- контролем за состоянием технических средств охраны.

Ответственным за организацию пропускного и внутриобъектового режимов является Руководитель.

Организация пропускного и внутриобъектового режимов предприятия осуществляется руководителями соответствующих подразделений.

3. Порядок доступа в помещения сотрудников и граждан

3.1 Перечень лиц, доступ которых в помещения, находящиеся в пределах границы контролируемой зоны, необходим для выполнения ими служебных (трудовых) обязанностей приведен в приложении 1 к настоящему приказу.

3.2 Неконтролируемое пребывание лиц в помещениях, находящихся в пределах границы контролируемой зоны, указанных в п. 3.1 настоящей Инструкции, разрешено в период рабочего времени в соответствии с утвержденным графиком работы, либо вне периода рабочего времени с письменного разрешения ответственного за организацию обработки персональных данных или ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных.

3.3 Лица, не указанные в п. 3.1 настоящей Инструкции, допускаются в помещения в присутствии лиц, доступ которых в помещения, находящиеся в пределах границы контролируемой зоны, необходим для выполнения ими служебных (трудовых) обязанностей.

4. Внутриобъектовый режим на территории Департамента промышленности Ханты-Мансийского автономного округа – Югры.

Ответственным за соблюдение правил внутреннего трудового распорядка, установленного режима функционирования, порядка содержания служебных помещений и мер противопожарной безопасности на объектах является Руководитель.

Сотрудники по окончании рабочего дня должны закрывать кабинеты на ключ, ключи от помещений, в которых размещена информационная система персональных данных, хранятся у сотрудников.

В случае отсутствия сотрудников в кабинетах в рабочее время помещения должны быть закрыты на ключ.

На территории помещений, в которых расположена информационная система персональных данных, запрещается:

- проводить без разрешения руководства фото-, кино-, видеосъемки, в том числе с использованием мобильных телефонов;
- курить;
- пользоваться неисправными или самодельными электронагревательными и другими электробытовыми приборами;
- загромождать территорию, основные и запасные входы (выходы), лестничные площадки материалами и предметами, которые создают помехи для системы видеонаблюдения, затрудняют эвакуацию людей, материальных ценностей, препятствуют ликвидации очагов возгорания;
- совершать действия, нарушающие установленные режимы функционирования пожарной сигнализации.

5. Организация и порядок производства ремонтно-строительных работ в здании

Рабочие и специалисты ремонтно-строительных организаций пропускаются в помещение для проведения ремонтно-строительных работ на основании заявок, подписанных руководством. Работы проводятся только в присутствии контролирующего

лица из числа сотрудников.

Для предотвращения несанкционированного доступа к информации, содержащей ПДн, осуществляется контроль деятельности рабочих.

6. Организация охраны

Должна быть организована охрана помещений Департамента промышленности Ханты-Мансийского автономного округа – Югры. Режим работы охраны устанавливается штатным расписанием и должностными инструкциями.

Для исключения несанкционированного доступа к информации, содержащей ПДн, при покидании помещения необходимо запирать его на ключ.

7. Уборка помещений

Уборка помещений должна производиться под контролем сотрудника, имеющего доступ в помещение и постоянно в нем работающего.

Во время уборки в помещении должна быть приостановлена работа с ПДн, должны быть заблокированы все АРМ, на которых хранятся ПДн, носители, содержащие ПДн, должны быть убраны в сейф.

8. Требования по техническому укреплению

Ответственный за обеспечение безопасности ПДн обеспечивает обязательное выполнение мероприятий по техническому укреплению помещений, в которых обрабатываются ПДн, и должен руководствоваться следующими основными требованиями:

- двери и окна должны иметь прочные и надежные петли, шпингалеты, крючки или задвижки и быть плотно подогнаны к рамам и дверным коробам. Допускается применение электромеханических, электромагнитных замков и задвижек;
- конструкция оконных рам должна исключать возможность демонтажа с наружной стороны оконного проема стекол. Стекла в рамах должны быть надежно закреплены в пазах. Рамы указанных оконных проемов оборудуются запорными устройствами. На окнах первого этажа, а также верхних этажей – при возможности прямого просмотра помещения с улицы, должны быть установлены жалюзи.

Приложение 16
к приказу Департамента промышленности
Ханты-Мансийского автономного округа – Югры
от 25.08.2017 №38-П-139

ИНСТРУКЦИЯ
по работе с инцидентами информационной безопасности

Ответственность за выявление инцидентов ИБ и реагирование на них в Департаменте промышленности Ханты-Мансийского автономного округа – Югры возлагается на администратора информационной безопасности.

Администратор информационной безопасности имеет полномочия инициировать проведение служебных проверок (ходатайствовать о наложении дисциплинарного взыскания перед Руководителем) по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации.

Предположение о том, что произошел инцидент безопасности в ИС, базируется на трех основных факторах:

- события информационной безопасности поступают одновременно из нескольких источников (пользователи, средства защиты, журнальные файлы);
- средства защиты сигнализируют о множественном повторяющемся событии или попытках нарушения установленных правил;
- анализ электронных журналов средств защиты информации и штатных журналов операционной системы на наличие ошибок дает основание для вывода системным администраторам о возможности наступления события инцидента.

В информационной системе подлежат регистрации следующие события:

- вход (выход), а также попытки входа субъектов доступа в информационную систему и загрузки (останова) операционной системы;
- подключение машинных носителей информации и вывод информации на носители информации;
- запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации;
- попытки доступа программных средств к определяемым Департаментом защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей) и иным объектам доступа;
- попытки удаленного доступа.

Состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности, должны обеспечить возможность идентификации типа события безопасности, даты и времени события безопасности, идентификационной информации источника события безопасности, результат события безопасности (успешно или неуспешно), субъект доступа (пользователь и (или) процесс), связанный с данным событием безопасности.

При регистрации входа (выхода) субъектов доступа в информационную систему и загрузки (останова) операционной системы состав и содержание информации должны, как

минимум, включать дату и время входа (выхода) в систему (из системы) или загрузки (останова) операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки (останова) операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа.

При регистрации подключения машинных носителей информации и вывода информации на носители информации состав и содержание регистрационных записей должны, как минимум, включать дату и время подключения машинных носителей информации и вывода информации на носители информации, логическое имя (номер) подключаемого машинного носителя информации, идентификатор субъекта доступа, осуществляющего вывод информации на носитель информации.

При регистрации запуска (завершения) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации состав и содержание регистрационных записей должны, как минимум, включать дату и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный).

При регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам состав и содержание регистрационных записей должны, как минимум, включать дату и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого файла (логическое имя, тип).

При регистрации попыток доступа программных средств к защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, записям, полям записей) состав и содержание информации должны, как минимум, включать дату и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификацию защищаемого объекта доступа (логическое имя (номер).

При регистрации попыток удаленного доступа к информационной системе состав и содержание информации должны, как минимум, включать дату и время попытки удаленного доступа с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), используемый протокол доступа, используемый интерфейс доступа и (или) иную информацию о попытках удаленного доступа к информационной системе.

Сроки хранения соответствующих записей регистрационных журналов должны обеспечивать возможность обнаружения, идентификации и анализа инцидентов, возникших в ИСПДн, в течение 3-х месяцев.

Процедуры сбора, записи и хранения информации о событиях безопасности в течение установленного времени хранения предусматривают:

1) возможность выбора администратором информационной безопасности событий безопасности, подлежащих регистрации в текущий момент времени из перечня событий безопасности, определенных выше;

2) генерацию (сбор, запись) записей регистрации (аудита) для событий безопасности, подлежащих регистрации (аудиту) в соответствии с составом и содержанием информации, установленными для соответствующего типа события;

3) хранение информации о событиях безопасности в течение времени, установленного в соответствии с настоящей Инструкцией.

Объем памяти для хранения информации о событиях безопасности рассчитывается и выделяется администратором информационной безопасности ИСПДн Фонда с учетом типов событий безопасности, подлежащих регистрации в соответствии с в пункте 2 настоящих Правил, составом и содержанием информации о событиях безопасности, подлежащих регистрации, прогнозируемой частоты возникновения подлежащих регистрации событий безопасности, срока хранения информации о зарегистрированных событиях безопасности.

Состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности, а также сроки хранения определяются администратором информационной безопасности согласно требованиям предъявляемым к информационным системам определенного класса защищенности.

Реагирование на сбои при регистрации событий безопасности должно предусматривать:

- предупреждение (сигнализация, индикация) администраторов о сбоях (аппаратных и программных ошибках, сбоях в механизмах сбора информации или переполнения объема (емкости) памяти) при регистрации событий безопасности;
- реагирование на сбои при регистрации событий безопасности путем изменения администраторами параметров сбора, записи и хранения информации о событиях безопасности, в том числе отключение записи информации о событиях безопасности от части компонентов информационной системы, запись поверх устаревших хранимых записей событий безопасности.

События безопасности подлежат защите согласно организационным мерам, а также матрице доступа и соответствующим настройкам системы защиты информации на ограничение доступа пользователей к настройкам и изменениям параметров средств защиты информации.

Любой сотрудник должен согласовывать следующие действия с администратором информационной безопасности:

- замена прикладного оборудования (мышь, клавиатура, принтер, монитор);
- установка дополнительного ПО;
- изменение сетевых настроек рабочего места;
- замена, изменение любой аппаратной части рабочего места.

Ответственный за организацию обработки персональных данных не может требовать от администратора информационной безопасности действий, направленных на нарушение настоящего руководства и других организационно-распорядительных документов Департамента промышленности Ханты-Мансийского автономного округа – Югры, требовать сокрытия инцидентов ИБ, вызванных любыми должностными лицами, требовать сообщения ему паролей на средства защиты информации и нарушения установленного разграничения прав по допуску к информационным ресурсам, установленным матрицей доступа к информационными ресурсам ИС.

Выявление (поиск), анализ и устранение уязвимостей в информационной системе включает в себя:

- выявление (поиск) уязвимостей, связанных с ошибками кода в программном (микропрограммном) обеспечении (общесистемном, прикладном, специальном), а также программном обеспечении средств защиты информации, правильностью установки и настройки средств защиты информации, технических средств и программного

обеспечения, а также корректностью работы средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением;

- разработку по результатам выявления (поиска) уязвимостей отчетов с описанием выявленных уязвимостей и планом мероприятий по их устранению;

- анализ отчетов с результатами поиска уязвимостей и оценки достаточности реализованных мер защиты информации;

- устранение выявленных уязвимостей, в том числе путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств;

- информирование должностных лиц Департамента (пользователей, администраторов, подразделения по защите информации) о результатах поиска уязвимостей и оценки достаточности реализованных мер защиты информации.

В случае невозможности устранения выявленных уязвимостей путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного программного обеспечения или микропрограммного обеспечения технических средств необходимо предпринять действия (настройки средств защиты информации, изменение режима и порядка использования информационной системы), направленные на устранение возможности использования выявленных уязвимостей.

Необходимо использовать для выявления (поиска) уязвимостей средств анализа (контроля) защищенности (сканеров безопасности), имеющих стандартизованные (унифицированные) в соответствии с национальными стандартами описание и перечни программно-аппаратных платформ, уязвимостей программного обеспечения, ошибочных конфигураций, правил описания уязвимостей, проверочных списков, процедур тестирования и языка тестирования информационной системы на наличие уязвимостей, оценки последствий уязвимостей, имеющих возможность оперативного обновления базы данных выявляемых уязвимостей.

Необходимо уточнять перечень сканируемых в информационной системе уязвимостей с установленной им периодичностью, а также после появления информации о новых уязвимостях.

Доступ к функциям выявления (поиска) уязвимостей предоставляется только администраторам (предоставление такой возможности только администраторам безопасности).

Настоящие правила регламентируют обеспечение безопасности информации при проведении обновлении, модификации общесистемного и прикладного программного обеспечения, технического обслуживания и при возникновении нештатных ситуаций в работе ИСПДн.

Все изменения конфигураций технических и программных средств ИСПДн должны производиться только на основании заявок ответственного за эксплуатацию конкретной ИСПДн.

Право внесения изменений в конфигурацию аппаратно-программных средств защищенных ИСПДн предоставляется:

- в отношении системных и прикладных программных средств - администратору защиты по согласованию (в случае, если проводилась аттестация) с органом по

аттестации, проводившим аттестацию данной ИСПДн;

- в отношении аппаратных средств, а также в отношении программно-аппаратных средств защиты - администратору защиты по согласованию (в случае, если проводилась аттестация) с органом по аттестации, проводившим аттестацию данной ИСПДн.

Изменение конфигурации аппаратно-программных средств ИСПДн кем-либо, кроме вышеперечисленных уполномоченных работников и подразделений, запрещено.

Процедура внесения изменений в конфигурацию системных и прикладных программных средств ИСПДн, а также средств защиты информации инициируется заявкой ответственного за эксплуатацию ИСПДн.

В заявке могут указываться следующие виды необходимых изменений в составе аппаратных и программных средств ИСПДн:

- установка (развертывание) на компьютер(ы) программных средств, необходимых для решения определенной задачи (добавление возможности решения данной задачи в данной ИСПДн;
- обновление (замена) на компьютере(ах) программных средств, необходимых для решения определенной задачи (обновление версий используемых для решения определенной задачи программ);
- изменение настроек средств защиты информации;
- удаление с компьютера программных средств, использовавшихся для решения определенной задачи (исключение возможности решения данной задачи на данном компьютере).

Также в заявке указывается условное наименование ИСПДн. Наименования задач указываются в соответствии с перечнем задач архива дистрибутивов установленного программного обеспечения, которые можно решать с использованием указанного компьютера.

Заявку ответственного за эксплуатацию ИСПДн, в которой требуется произвести изменения конфигурации, рассматривает руководитель, визирует ее, утверждая тем самым производственную необходимость проведения указанных в заявке изменений.

После чего заявка передается администратору защиты для непосредственного исполнения работ по внесению изменений в конфигурацию компьютера указанного в заявке ИСПДн.

Подготовка обновления, модификации общесистемного и прикладного программного обеспечения ИСПДн тестирование, стендовые испытания (при необходимости) и передача исходных текстов, документации и дистрибутивных носителей программ в архив дистрибутивов установленного программного обеспечения, внесение необходимых изменений в настройки средств защиты от НСД и средств контроля целостности файлов на компьютерах, (обновление) и удаление системных и прикладных программных средств производится администратором безопасности по согласованию с органом по аттестации (в случае, если проводилась аттестация), проводившим аттестацию данной ИСПДн. Работы производятся в присутствии ответственного за эксплуатацию данной ИСПДн.

Установка или обновление подсистем ИСПДн должны проводиться в строгом соответствии с технологией проведения модификаций программных комплексов данных подсистем.

Установка и обновление ПО (системного, тестового и т.д.) на компьютерах

производится только с оригинальных лицензионных дистрибутивных носителей (дискет, компакт дисков и т.п.), полученных установленным порядком, прикладного ПО - с эталонных копий программных средств, полученных из архива дистрибутивов установленного программного обеспечения.

Все добавляемые программные и аппаратные компоненты должны быть предварительно установленными порядком проверены на работоспособность, а также отсутствие опасных функций.

После установки (обновления) ПО, администратор защиты должен произвести требуемые настройки средств управления доступом к компонентам компьютера и проверить работоспособность ПО и правильность их настройки и произвести соответствующую запись в «Журнале учета нештатных ситуаций в ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн», делает отметку о выполнении (на обратной стороне заявки) и в «Техническом паспорте».

Формат записей «Журнала учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн» устанавливается приказом руководителя Департамента.

При возникновении ситуаций, требующих передачи технических средств в сервисный центр с целью ремонта, ответственный за ее эксплуатацию докладывает об этом ответственному за защиту информации, который в свою очередь связывается с работниками органа по аттестации (в случае, если проводилась аттестация) и в дальнейшем действует согласно их инструкций. В данном случае администратор защиты обязан предпринять необходимые меры для затирания защищаемой информации, которая хранилась на дисках компьютера. Оригиналы заявок (документов), на основании которых производились изменения в составе программных средств компьютеров с отметками о внесении изменений в состав программных средств, должны храниться вместе с техническим паспортом на ИСПДн и «Журналом учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн» у ответственного за защиту информации.

Копии заявок могут храниться у администратора защиты:

- для восстановления конфигурации ИСПДн после аварий;
- для контроля правомерности установки на ИСПДн средств для решения соответствующих задач при разборе конфликтных ситуаций;
- для проверки правильности установки и настройки средств защиты ИСПДн факт уничтожения данных, находившихся на диске компьютера, оформляется актом за подписью администратора защиты и работника ответственного за эксплуатацию данной ИСПДн.

Данный раздел определяет порядок контроля соблюдения условий использования средств защиты информации (далее — СЗИ).

Порядок работы с техническими СЗИ определен в соответствующих руководствах по настройке и использованию СЗИ обязательных для исполнения, как работниками обрабатывающими конфиденциальную информацию, так и администратором безопасности ИСПДн.

Право проверки соблюдения условий использования средств защиты информации имеют:

- руководитель;
- ответственный за защиту информации;
- администратор безопасности.

Пользователю ИСПДн категорически запрещается:

- обрабатывать конфиденциальную информацию с отключенными СЗИ;
- менять настройки СЗИ.

Администратору безопасности запрещается менять настройки программно-аппаратных СЗИ предустановленные специалистом организации, имеющей лицензию на деятельность по технической защите информации, без согласования с этой организацией.

В информационной системе должны обеспечиваться регистрация событий и оповещение (сигнализация, индикация) администратора безопасности о событиях, связанных с нарушением работоспособности (правильности функционирования) и параметров настройки программного обеспечения и средств защиты информации.

При контроле состава технических средств, программного обеспечения и средств защиты информации осуществляется:

- контроль соответствия состава технических средств, программного обеспечения и средств защиты информации приведенному в эксплуатационной документации с целью поддержания актуальной (установленной в соответствии с эксплуатационной документацией) конфигурации информационной системы и принятие мер, направленных на устранение выявленных недостатков;
- контроль состава технических средств, программного обеспечения и средств защиты информации на соответствие сведениям действующей (актуализированной) эксплуатационной документации и принятие мер, направленных на устранение выявленных недостатков;
- контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принятие мер, направленных на устранение выявленных недостатков;
- исключение (восстановление) из состава информационной системы несанкционированно установленных (удаленных) технических средств, программного обеспечения и средств защиты информации.

В информационной системе должна обеспечиваться регистрация событий безопасности, связанных с изменением состава технических средств, программного обеспечения и средств защиты информации.

При контроле правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе осуществляется:

- контроль правил генерации и смены паролей пользователей в соответствии с ИАФ.1 и ИАФ.4;
- контроль заведения и удаления учетных записей пользователей в соответствии с УПД.1;
- контроль реализации правил разграничения доступом в соответствии с УПД.2;
- контроль реализации полномочий пользователей в соответствии с УПД.4 и ПД.5;
- контроль наличия документов, подтверждающих разрешение изменений учетных записей пользователей, их параметров, правил разграничения доступом и полномочий пользователей, предусмотренных организационно-распорядительными документами по

защите информации Департамента;

- устранение нарушений, связанных с генерацией и сменой паролей пользователей, заведением и удалением учетных записей пользователей, реализацией правил разграничения доступом, установлением полномочий пользователей.

В информационной системе должна обеспечиваться регистрация событий, связанных со сменой паролей пользователей, заведением и удалением учетных записей пользователей, изменением правил разграничения доступом и полномочий пользователей.

Приложение 17
к приказу Департамента промышленности
Ханты-Мансийского автономного округа – Югры
от 25.08.2017 №38-П-139

ИНСТРУКЦИЯ
по обеспечению безопасности эксплуатации средств криптографической защиты информации

1. Общие положения

1.1. Настоящая Инструкция определяет порядок учета, хранения и использования средств криптографической защиты информации (СКЗИ) и криптографических ключей, а также порядок изготовления, смены, уничтожения и компрометации криптографических ключей в целях обеспечения безопасности эксплуатации в Департамента промышленности Ханты-Мансийского автономного округа – Югры.

1.2. Пользователь должен выполнять все требования настоящей Инструкции, правила, изложенные в эксплуатационной документации на СКЗИ, а также другие документы, регламентирующие порядок работы с СКЗИ. Перечень пользователей СКЗИ представлен в Приложении 1 настоящего Приказа.

2. Обязанности Пользователя

2.1. Пользователь обязан соблюдать требования по обеспечению безопасности функционирования СКЗИ.

2.2. Пользователь обязан обеспечить конфиденциальность всей информации ограниченного распространения, доступной по роду выполняемых функциональных обязанностей.

2.3. Пользователь обязан сдать носители ключевой информации (далее – НКИ) при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ, ответственному за обработку персональных данных.

2.4. Пользователь обязан сдать носители ключевой информации (далее – НКИ) по окончании срока действия сертификата ключа, а также в случае компрометации ключа.

2.5. Пользователь обязан немедленно уведомлять Ответственного за обработку персональных данных о компрометации криптографических ключей.

2.6. Пользователь обязан немедленно уведомлять Ответственного за обработку персональных данных о фактах утраты или недостачи СКЗИ, НКИ.

3. Порядок обращения со средствами криптографической защиты информации

3.1. Монтаж и установка СКЗИ осуществляются только уполномоченным лицом, либо организацией, имеющей необходимые лицензии.

3.2. Все СКЗИ и НКИ должны учитываться в журнале.

3.3. Служебные помещения, в которых размещаются СКЗИ, должны оборудоваться охранной сигнализацией, по убытии сотрудников закрываться и сдаваться под охрану.

3.4. Для хранения носителей ключевой информации помещения обеспечиваются сейфами (металлическими шкафами).

3.5. Несанкционированное изготовление дубликатов ключей ЗАПРЕЩЕНО. В случае утери ключа механизм (секрет) замка (либо сам сейф) должен быть заменён.

3.6. К эксплуатации СКЗИ допускаются лица, изучившие правила пользования

данным СКЗИ.

3.7. Все программное обеспечение ПЭВМ, предназначенной для установки СКЗИ, должно иметь соответствующие лицензии. Установка средств разработки и отладки программ на рабочую станцию, использующую СКЗИ, не допускается.

4. Порядок обращения с ключами ЭЦП

4.1. Криптографический ключ применяется для подписания (проверки электронной цифровой подписи) электронных документов до окончания срока его действия или наступления события, трактуемого как компрометация криптографических ключей.

4.2. Изготовление и выдача ключей ЭЦП осуществляется только Удостоверяющим центром.

4.3. Выработанные закрытые (конфиденциальные) криптографические ключи хранятся исключительно в электронном виде на цифровых носителях информации, которые получают статус НКИ.

4.4. НКИ являются объектами особой важности, т.к. они содержат информацию, предназначенную для гарантированной идентификации владельца ключа, защиты электронного документа от подделки и обеспечения конфиденциальности документа.

4.5. Владельцы ключей несут персональную ответственность за обеспечение конфиденциальности ключевой информации и защиту НКИ от несанкционированного использования.

4.6. Для хранения носителей ключевой информации Пользователь должен быть обеспечен личным сейфом.

5. Запрещается

5.1. Осуществлять несанкционированное и без учётное копирование ключевых данных.

5.2. Хранить НКИ вне сейфов и помещений, гарантирующих их сохранность и конфиденциальность.

5.3. Передавать НКИ третьим лицам.

5.4. Во время работы оставлять НКИ без присмотра (например, на рабочем столе или в разъеме системного блока ПЭВМ).

5.5. Хранить на НКИ какую-либо информацию, кроме ключевой.

5.6. Использование выведенных из действия криптографических ключей.

6. Действия при компрометации действующих ключей и восстановлении конфиденциальной связи

6.1. Под компрометацией криптографического ключа понимается утрата доверия к тому, что данный ключ обеспечивает однозначную идентификацию Владельца и конфиденциальность информации, обрабатываемой с его помощью. К событиям, связанным с компрометацией действующих криптографических ключей, относятся:

- Утрата (хищение) НКИ, в том числе – с последующим их обнаружением;
- Увольнение (переназначение) сотрудников, имевших доступ к ключевой информации;
- Передача закрытых (конфиденциальных) ключей по линии связи в открытом виде;
- Нарушение правил хранения криптографических ключей;
- Вскрытие фактов утечки передаваемой информации или её искажения (подмены, подделки);

- Отрицательный результат при проверке наложенной ЭЦП;
- Несанкционированное или без учётное копирование ключевой информации;
- Все случаи, когда нельзя достоверно установить, что произошло с НКИ (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута вероятность того, что данный факт произошел в результате злоумышленных действий).

6.2. При наступлении любого из перечисленных выше событий Владелец ключа должен немедленно прекратить связь с другими абонентами и сообщить о факте компрометации (или предполагаемом факте компрометации) в Удостоверяющий центр, производивший генерацию ключей ЭЦП.

6.3. При подтверждении факта компрометации действующих ключей Пользователь обязан обеспечить немедленное изъятие из обращения скомпрометированных криптографических ключей.

6.4. Для восстановления конфиденциальной связи после компрометации действующих ключей Пользователь получает в Удостоверяющем центре новые ключи ЭЦП.

7. Ответственность Пользователя

7.1. Владелец ключа несет персональную ответственность за конфиденциальность личных ключевых носителей.

В случае неисполнения или ненадлежащего выполнения требований настоящей Инструкции Пользователь несёт ответственность в соответствии с действующим Законодательством Российской Федерации.

Приложение 18
к приказу Департамента промышленности
Ханты-Мансийского автономного округа – Югры
от 25.08.2017 №38-П-139

ИНСТРУКЦИЯ
ответственного за эксплуатацию информационных систем персональных данных

1. Общие положения

Настоящая инструкция определяет права и обязанности лица, ответственного за эксплуатацию информационной системы персональных данных.

Методическое руководство работой ответственного за эксплуатацию ИСПДн осуществляется ответственным за организацию обработки персональных данных.

Ответственный за эксплуатацию в своей работе руководствуется положениями, руководящими и нормативными документами ФСТЭК и ФСБ России по защите информации и организационно-распорядительными документами для данной ИСПДн, а также иными нормативными документами в части защиты информации.

Ответственный за эксплуатацию ИСПДн несет ответственность за свои действия и действия сотрудников вверенного структурного подразделения в соответствии с действующим законодательством РФ.

2. Функции ответственного за эксплуатацию ИСПДн

Осуществление контроля за целевым использованием ИСПДн, всех периферийных устройств и технических средств, входящих в состав ИСПДн.

Контроль за отсутствием в период обработки защищаемой информации в помещении, где осуществляется обработка, посторонних лиц, не допущенных к обрабатываемой информации.

Контроль использования сотрудниками структурных подразделений, эксплуатирующими ИСПДн, средств защиты информации, установленных на АРМ, входящих в состав ИСПДн.

Контроль за правильностью использования и хранения сотрудниками структурных подразделений, эксплуатирующими ИСПДн, машинных носителей информации и документов, содержащих персональные данные.

Представление заявок на пользователей, допускаемых к защищаемым ресурсам ИСПДн, с целью закрепления за ними носителей информации устройств блокировки, паролей и других средств разграничения доступа к информации, а также прав пользования средствами вычислительной техники.

Организация повышения уровня осведомленности подчиненных должностных лиц по вопросам информационной безопасности.

3. Обязанности ответственного за эксплуатацию ИСПДн

Четко знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководств по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

Обеспечивать функционирование ИСПДн в пределах возложенных на него функций.

Обеспечивать контроль выполнения установленного комплекса мероприятий по обеспечению безопасности ПДн.

Контролировать целостность печатей (пломб) на устройствах ИСПДн.

Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств ИСПДн и отправке их в ремонт.

Присутствовать при выполнении технического обслуживания ИСПДн при установке (модификации) программного обеспечения.

Информировать администратора информационной безопасности о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн.

Контролировать соответствие состава ИСПДн техническому паспорту на ИСПДн.

Приложение 19
к приказу Департамента промышленности
Ханты-Мансийского автономного округа – Югры
от 25.08.2017 №38-П-139

ПОРЯДОК
уничтожения персональных данных при достижении целей обработки и (или) при наступлении иных законных оснований

Настоящий документ устанавливает порядок уничтожения информации, содержащей персональные данные, при достижении целей обработки или при наступлении иных законных оснований в соответствии с Федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

Документы, дела, книги и журналы учета, содержащие персональные данные, при достижении целей обработки, или при наступлении иных законных оснований, (например, утратившие практическое значение, а также с истекшим сроком хранения), подлежат уничтожению.

Уничтожение документов производится в присутствии ответственного за организацию обработки персональных данных, который несет персональную ответственность за правильность и полноту уничтожения перечисленных в акте документов (Акт составляется в свободной форме).

Отобранные к уничтожению материалы измельчаются механическим способом до степени, исключающей возможность прочтения текста или сжигаются.

После уничтожения материальных носителей ответственный за организацию подписывает акт в двух экземплярах, также в номенклатурах и описях дел проставляется отметка «Уничтожено. Акт №__(дата)».

Уничтожение информации на носителях необходимо осуществлять путем стирания информации с использованием сертифицированного программного обеспечения, установленного на АРМ с гарантированным уничтожением (в соответствии с заданными характеристиками для установленного программного обеспечения с гарантированным уничтожением).

Информация, содержащая персональные данные при достижении целей обработки или при наступлении иных законных оснований (например, утратившие практическое значение, с истекшим сроком хранения) в электронном виде, подлежит уничтожению.

Приложение 20
к приказу Департамента промышленности
Ханты-Мансийского автономного округа – Югры
от 25.08.2017 №38-П-139

ПРАВИЛА
работы лиц, доступ которых к персональным данным,
в том числе обрабатываемым в информационных системах персональных данных,
необходим для выполнения ими служебных (трудовых) обязанностей

Допуск для работы на автоматизированных рабочих местах (далее – АРМ) состоящих в составе сегмента информационной системы персональных данных (далее – ИСПДн) осуществляется на основании утвержденного списка лиц, доступ которых к персональным данным, в том числе обрабатываемым в ИСПДн, необходим для выполнения ими служебных (трудовых) обязанностей (далее – Пользователи ИСПДн).

Пользователь ИСПДн имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн. При этом для хранения и записи информации, содержащей персональные данные (далее – ПДн), разрешается использовать только машинные носители информации, учтенные в журнале учета машинных носителей информации, использующихся в ИСПДн для обработки, хранения и транспортировки информации.

Пользователь несет ответственность за правильность включения и выключения АРМ, входа и выхода в систему и за все свои действия при работе в ИСПДн.

Вход пользователя в систему осуществляется по выдаваемому ему электронному идентификатору и по персональному паролю.

При работе со съемными машинными носителями информации пользователь каждый раз перед началом работы обязан проверить их на отсутствие вирусов и иных вредоносных программ с использованием штатных антивирусных средств, установленных на АРМ. В случае обнаружения вирусов либо вредоносных программ пользователь ИСПДн обязан немедленно прекратить их использование и действовать в соответствии с требованиями инструкции по организации антивирусной защиты.

Каждый работник, участвующий в рамках своих служебных обязанностей в процессах обработки персональных данных в ИСПДн и имеющий доступ к АРМ, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и обязан:

- Строго соблюдать установленные соответствующими инструкциями правила обеспечения безопасности информации в ИСПДн;
- Знать и строго выполнять правила работы со средствами защиты информации, установленными на АРМ;
- Хранить в тайне свой пароль (пароли). Выполнять требования инструкции по организации парольной защиты в полном объеме;
- Выполнять требования инструкции по организации антивирусной защиты в полном объеме;
- Немедленно известить ответственного за обеспечение безопасности персональных данных в случае утери электронного идентификатора или при подозрении

компрометации личных ключей и паролей, а также при обнаружении:

- Несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации АРМ;
- Отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования компонентов АРМ, а также перебоев в системе электроснабжения;
- Некорректного функционирования установленных на АРМ технических средств защиты;
- Непредусмотренных отводов кабелей и подключенных устройств.

Пользователю АРМ категорически запрещается:

- Использовать компоненты программного и аппаратного обеспечения АРМ в личных целях;
- Самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения АРМ;
- Записывать и хранить конфиденциальную информацию (содержащую персональные данные) на неучтенных машинных носителях информации (гибких магнитных дисках, флэш-накопителях и т.п.);
- Оставлять включенным без присмотра АРМ, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);
- Оставлять без личного присмотра на рабочем месте или в ином месте машинные носители и распечатки, содержащие персональные данные;
- Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты;
- Размещать средства ИСПДн так, чтобы с них существовала возможность визуального считывания информации, содержащей персональные данные.

Приложение 21
к приказу Департамента промышленности
Ханты-Мансийского автономного округа – Югры
от 25.08.2017 №38-П-139

ПРАВИЛА
рассмотрения запросов субъектов персональных данных или их представителей

1. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- Подтверждение факта обработки персональных данных;
- Правовые основания и цели обработки персональных данных;
- Цели и применяемые Департаментом способы обработки персональных данных;
- Наименование и место нахождения Департамента, сведения о лицах (за исключением работников Департамента), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Департаментом или на основании Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» (далее – Федеральный закон);
- Обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен Федеральным законом;
- Сроки обработки персональных данных, в том числе сроки их хранения;
- Наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Департамента, если обработка поручена или будет поручена такому лицу.

2. Субъект персональных данных вправе требовать от Департамента уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

3. Сведения должны быть предоставлены субъекту персональных данных Департаментом в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

4. Сведения предоставляются субъекту персональных данных или его представителю Департаментом при обращении либо при получении запроса субъекта персональных данных или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с Департаментом (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных Департаментом, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской

Федерации.

5. В случае если обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно к Департаменту или направить ему повторный запрос в целях ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной по которому является субъект персональных данных.

6. Субъект персональных данных вправе обратиться повторно к Департаменту или направить ему повторный запрос в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в пункте 5 настоящих правил, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в пункте 4 настоящих правил, должен содержать обоснование направления повторного запроса.

7. Департамент вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 5 и 6 настоящих правил. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Департаменте.

8. Обязанности Департамента при обращении к нему субъекта персональных данных либо при получении запроса субъекта персональных данных или его представителя, а также уполномоченного органа по защите прав субъектов персональных данных:

- Департамент обязан сообщить в порядке, предусмотренном статьей 14 Федерального закона, субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя либо в течение 30 (тридцати) дней с даты получения запроса субъекта персональных данных или его представителя.

- В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя Департамент обязан дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона или иного федерального закона, являющееся основанием для такого отказа, в срок, не превышающий 30 (тридцати) дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя.

- Департамент обязан предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий 7 (семи)

рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, Департамент обязан внести в них необходимые изменения. В срок, не превышающий 7 (семи) рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Департамент обязан уничтожить такие персональные данные. Департамент обязан уведомить субъекта персональных данных или его представителя о внесенных изменениях, предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы.

- Департамент обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение 30 (тридцати) дней с даты получения такого запроса.

Нарушение установленного порядка рассмотрения запросов влечет в отношении виновных должностных лиц ответственность в соответствии с законодательством Российской Федерации.

Приложение 22
к приказу Департамента промышленности
Ханты-Мансийского автономного округа – Югры
от 25.08.2017 №38-П-139

ПРАВИЛА
осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных

1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных в Департаменте промышленности Ханты-Мансийского автономного округа – Югры требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных» (далее – Правила), устанавливают процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяют порядок проведения процедур внутреннего контроля исполнения требований законодательства.

2. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям к защите персональных данных организовывается проведение периодических проверок.

3. Проверки осуществляются ответственным за организацию обработки персональных данных совместно с ответственным за обеспечение безопасности персональных данных в информационных системах персональных данных.

4. Плановые проверки проводятся не чаще чем один раз в три месяца.

5. Внеплановые проверки проводятся по инициативе ответственного за организацию обработки персональных данных либо ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных.

6. Основанием для проведения проверки служит приказ руководителя Департамента промышленности Ханты-Мансийского автономного округа – Югры «О проведении внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных»

7. При проведении проверки должны быть полностью, объективно и всесторонне установлены:

- соответствие целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям Департамента персональных данных;

- соответствие объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;

- достаточность (избыточность) персональных данных для целей обработки персональных данных, заявленных при сборе персональных данных;

- отсутствие (наличие) объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных;

- порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

- порядок и условия применения средств защиты информации;
- соблюдение правил доступа к персональным данным;
- наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер.

8. Ответственный за организацию обработки персональных данных и ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных в ходе проверки имеют право:

- запрашивать у работников информацию, необходимую для реализации своих полномочий;
- требовать от уполномоченных на обработку персональных данных должностных лиц уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;
- принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;
- вносить предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;
- вносить предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

9. Ответственный за организацию обработки персональных данных в течение 3 (трех) рабочих дней направляет в адрес Руководителя результаты проведения проверки в форме служебной записки.

Приложение 23
к приказу Департамента промышленности
Ханты-Мансийского автономного округа – Югры
от 25.08.2017 №38-П-139

ПРАВИЛА
работы с обезличенными данными в случае обезличивания персональных данных

1. Общие положения

Настоящие Правила работы с обезличенными персональными данными разработаны с учетом Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и определяют порядок работы с обезличенными данными в Департаменте промышленности Ханты-Мансийского автономного округа – Югры.

2. Термины и определения

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» в настоящих Правилах используются следующие понятия:

- персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных);
- обработка персональных данных - 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;
- обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

3. Условия обезличивания

Обезличивание персональных данных может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса информационных систем персональных данных и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

Способы обезличивания при условии дальнейшей обработки персональных данных:

- уменьшение перечня обрабатываемых сведений;
- замена части сведений идентификаторами;
- обобщение – понижение точности некоторых сведений;
- понижение точности некоторых сведений (например, «Место жительства» может состоять из страны, индекса, города, улицы, дома и квартиры, а может быть указан только населенный пункт)
- деление сведений на части и обработка в разных информационных системах;
- другие способы.

Способом обезличивания в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня персональных данных.

4. Порядок работы с обезличенными персональными данными

Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

Обезличенные персональные данные могут обрабатываться с использованием и без использования средств автоматизации.

При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение:

- парольной политики;
- антивирусной политики;
- правил работы со съемными носителями (если они используется);
- правил резервного копирования;
- правил доступа в помещения, где расположены элементы информационных систем.

При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:

- правил хранения бумажных носителей;
- правил доступа к ним и в помещения, где они хранятся.

В Департаменте промышленности Ханты-Мансийского автономного округа – Югры с целью обезличивания обрабатываемых персональных данных применяется метод изменения состава или семантики в целях представления в установленном порядке статистической информации (отчетности) для заинтересованных федеральных органов власти и исполнительных органов государственной власти Ханты-Мансийского автономного округа – Югры в соответствии с требованиями законодательства Российской Федерации.

Приложение 24
к приказу Департамента промышленности
Ханты-Мансийского автономного округа – Югры
от 25.08.2017 №38-П-139

ПЛАН

мероприятий по защите информации в
Департаменте промышленности Ханты-Мансийского автономного округа – Югры

1. Общие положения

План мероприятий по обеспечению защиты персональных данных (далее – План мероприятий) содержит необходимый перечень мероприятий для обеспечения защиты персональных данных в информационных системах Департамента.

Выбор конкретных мероприятий осуществляется на основании перечня актуальных угроз безопасности, указанных в Модели угроз безопасности для соответствующей ИС.

В План мероприятий включены следующие категории мероприятий:

- организационные (административные);
- физические;
- технические (аппаратные и программные);
- контролирующие.

В План мероприятий включена следующая информация:

- название мероприятия;
- периодичность мероприятия (разовое/периодическое);
- исполнитель мероприятия/ответственный за исполнение.

Исполнителем в части работ по:

- установке и настройке антивирусного програмного обеспечения, регистрации пользователя в домене (admugra/admugra.local) обеспечивающем доступ к сетевым ресурсам;

- регистрации пользователя на почтовом сервере @admhmao.ru;

- техническому обслуживанию, включающему: ремонт АРМ, настройку операционной системы требованиям безопасности (использование групповой/доменной политики), учетной записи пользователя, периферийного оборудования, программного обеспечения указанного в таблице 1 приложения 13 - является Бюджетное учреждение Ханты-Мансийского автономного округа - Югры "Окружной центр информационно-коммуникационных технологий" (далее - ИКТ-ХМАО).

Исполнителем в части работ по:

- установке и настройке средств криптографической защиты информации (СКЗИ) - является Автономное учреждение Ханты-Мансийского автономного округа - Югры "Югорский научно-исследовательский институт информационных технологий" (далее - ЮНИИ ИТ)

План внутренних проверок составляется на все информационные системы Департамента промышленности Ханты-Мансийского автономного округа – Югры.

1. План мероприятий по защите информации

Мероприятие	Периодичность	Исполнитель/ Ответственный
Организационные мероприятия		
Обследование информационных систем	Разовое срок до 31.12.2017	Хаперский О.А
Определение перечня ИСПДн	Разовое срок до 01.08.2017	Хаперский О.А
Определение обрабатываемых ПДн и объектов защиты	Разовое срок до 01.08.2017	Хаперский О.А
Определение круга лиц, участвующих в обработке ПДн	Разовое срок до 01.08.2017	Хаперский О.А
Определение прав разграничения доступа пользователей ИСПДн, необходимых для выполнения должностных обязанностей	Разовое срок до 01.08.2017	Хаперский О.А
Назначение ответственного за обеспечение безопасности ПДн	Разовое срок до 18.08.2017	Хаперский О.А
Классификация всех выявленных ИСПДн	Разовое срок до 18.08.2017	Хаперский О.А
Организация режима и контроля доступа (охраны) в помещения, в которых установлены аппаратные средства ИСПДн.	Разовое срок до 01.08.2017	Хаперский О.А
Организация порядка резервного копирования защищаемой информации на твердые носители	Разовое срок до 01.08.2017	Хаперский О.А
Организация информирования сотрудников о порядке обработки ПДн и их обучения	Разовое срок до 01.08.2017	Хаперский О.А
Организация информирования сотрудников о введенном режиме защиты ПДн	Разовое срок до 01.08.2017	Хаперский О.А
Подготовка и утверждение комплекта нормативной документации, регламентирующей обработку ПДн в ИСПДн	Разовое срок до 18.08.2017	Хаперский О.А
Физические мероприятия		
Установление границ контролируемой зоны ИСПДн	Разовое срок до 18.08.2017	Хаперский О.А
Организация постов охраны для пропуска в контролируемую зону	Разовое срок до 18.08.2017	Хаперский О.А
Установка жалюзи, штор на окнах или другие меры, исключающие несанкционированный доступ к ПДн снаружи здания	Разовое срок до 31.12.2017	Хаперский О.А
Технические мероприятия		
Внедрение специальной подсистемы управления доступом, регистрации и учета	Разовое срок до 01.08.2017	ИКТ-ХМАО/ Хаперский О.А.
Внедрение межсетевого экранирования	Разовое срок до 01.08.2017	ЮНИИ ИТ/ Хаперский О.А.
Внедрение криптографической защиты	Разовое срок до 01.08.2017	ЮНИИ ИТ/ Хаперский О.А.
Контролирующие мероприятия		
Контроль над соблюдением режима обработки ПДн	Ежемесячно	Хаперский О.А.

Мероприятие	Периодичность	Исполнитель/ Ответственный
Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации	Ежемесячно	Хаперский О.А
Контроль состава технических средств, программного обеспечения и средств защиты информации	Ежемесячно	Хаперский О.А
Проведение внутренних проверок на предмет выявления изменений в режиме обработки и защиты ПДн	Ежегодно	Хаперский О.А
Проведение анализа электронных журналов средств защиты информации и штатных журналов операционной системы на наличие ошибок	Ежемесячно	Хаперский О.А
Контроль за обновлениями программного обеспечения и единообразия применяемого ПО на всех элементах ИСПДн	Еженедельно	Хаперский О.А
Периодический контроль за выполнением работниками эксплуатирующими ИСПДн (пользователями ИСПДн), мероприятий по обеспечению безопасности персональных данных, обрабатываемых в ИСПДн	Еженедельно	Хаперский О.А
Контроль за обеспечением резервного копирования	Ежемесячно	Хаперский О.А
Организация анализа и пересмотра имеющихся угроз безопасности ПДн, а так же предсказание появления новых, еще неизвестных, угроз	Ежегодно	Хаперский О.А
Поддержание в актуальном состоянии нормативно-организационных документов	Ежемесячно	Хаперский О.А

Приложение 25
к приказу Департамента промышленности
Ханты-Мансийского автономного округа – Югры
от 25.08.2017 №38-П-139

РЕГЛАМЕНТ

работников, эксплуатирующих информационную систему обработки информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в том числе персональные данные в Департаменте промышленности Ханты-Мансийского автономного округа – Югры

1.Общие положения

1. Настоящий документ определяет основные обязанности, права и ответственность работников, эксплуатирующих информационную систему Департамента промышленности Ханты-Мансийского автономного округа – Югры (далее – Пользователь) информационных систем обработки информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в том числе персональные данные (далее – ИС) Департамента.

2. Пользователем ИС является работник Департамента, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИС, в соответствии со Списком лиц, допущенных к самостоятельной работе в ИС.

3. Пользователь должен принимать все необходимые меры по защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в том числе персональных данных (далее – конфиденциальная информация (КИ)) и контролю за соблюдением прав доступа к ней.

4. Положения настоящего документа обязательны для исполнения всеми пользователями.

Все пользователи должны быть ознакомлены под роспись с настоящим документом и предупреждены об индивидуальной ответственности за его нарушения.

5. Основными задачами при обработке информации в ИС являются:

обеспечение исполнения требований нормативных правовых актов, руководящих документов, регламентирующих защиту информации в Российской Федерации в процессе создания, хранения и передачи документов, содержащих конфиденциальную информацию в ИС Департамента;

обеспечение в ИС необходимого уровня безопасности обработки, хранения и передачи КИ;

обеспечение необходимого уровня безопасности носителей КИ;

обеспечение безопасности конфиденциальной информации при ее копировании, размножении;

резервное копирование, восстановление информации.

2. Основные положения

6. При первичном допуске к работе в ИС пользователь изучает требования настоящего документа, разрешительную систему доступа к ИС, технологический процесс обработки информации в ИС, руководящие, нормативно-методические и организационно-распорядительные документы по вопросам обеспечения безопасности обрабатываемой информации.

7. Каждый пользователь ИС, имеющий в рамках своих обязанностей доступ к аппаратным средствам, программному обеспечению и данным ИС, несет персональную ответственность за свои действия и **обязан**:

строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИС, в том числе положения настоящего документа;

знать и строго выполнять правила работы со средствами защиты информации, установленными на его рабочей станции;

располагать основные технические средства и системы (далее – ОТСС) в соответствии с техническим паспортом;

хранить в тайне свой пароль (пароли), парольную защиту организовывать в соответствии с инструкцией по организации парольной защиты;

выполнять требования «Инструкции по организации антивирусной защиты»;

немедленно вызывать администратора безопасности и ставить в известность руководителя подразделения при подозрении компрометации личных ключей и паролей или при обнаружении фактов совершения в его отсутствие попыток несанкционированного доступа (далее – НСД) к основным техническим средствам и системам (далее – ОТСС) ИС;

в случае появления у пользователя сведений или подозрений о фактах нарушения настоящих правил, а в особенности о фактах или попытках НСД к информации, обрабатываемой в ИС, пользователь должен немедленно сообщить об этом администратору безопасности;

немедленно сообщать администратору информационной безопасности об обнаруженных фактах нарушения информационной безопасности кем-либо;

сообщать администратору информационной безопасности об отклонениях в нормальной работе установленных на рабочей станции средств защиты информации;

при работе в ИС выполнять только служебные задания;

при отсутствии необходимости работы выключить (блокировать) компьютер;

при работе в ИС использовать только учтенные съемные носители, при обоснованной необходимости использования неучтённых носителей согласовывать использование с администратором информационной безопасности. После того как цель переноса информации на носители достигнута (переданы третьим лицам и т.п.) информация незамедлительно удаляется с носителей;

осуществлять установленным порядком уничтожение информации (сочетанием клавиш Shift+Del), содержащей сведения конфиденциального характера, с машинных (съемных) носителей информации;

немедленно выполнять предписания администратора безопасности в части обеспечения безопасности информации;

экран видеомонитора в помещении располагать во время работы так, чтобы исключалась возможность ознакомления с отображаемой на нем информацией посторонними лицами;

соблюдать установленный режим разграничения доступа к информационным ресурсам;

не разглашать известную им информацию, составляющую конфиденциальную информацию лицам, не имеющим допуска к этой информации;

все изменения конфигурации технических и программных средств ИС, ремонт, модификация и техническое обслуживание технических средств и систем, входящих в состав ИС производить только на основании «Инструкции пользователю по установке, модификации, ремонту, техническому обслуживанию и восстановлению работоспособности программного обеспечения и аппаратных средств».

8. Пользователю запрещается:

самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение, изменять установленный алгоритм функционирования технических и программных средств, устанавливать или удалять установленные техническим специалистом (администратором информационной безопасности) сетевые программы на компьютерах, вскрывать компьютеры, сетевое и периферийное оборудование, подключать к компьютеру дополнительное оборудование, вносить какие-либо изменения в конфигурацию аппаратно-программных средств рабочих станций или устанавливать дополнительно любые программные и аппаратные средства без согласования с администратором безопасности;

привлекать посторонних лиц для производства ремонта ОТСС без письменной заявки и согласования с администратором информационной безопасности;

запускать любые системные или прикладные программы, не входящие в состав программного обеспечения;

работать с неучтенными машинными (съемными) носителями информации;

отключать (блокировать) средства защиты информации;

производить какие-либо изменения в размещении технических средств;

обрабатывать на средствах вычислительной техники (далее – СВТ) входящих в состав ИСПДн информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к информационным ресурсам;

сообщать (или передавать) посторонним лицам личные атрибуты доступа к ресурсам ИС;

хранить на учтенных носителях программы и данные, не относящиеся к рабочей информации;

выполнять работы с документами ограниченного распространения на дому, выносить их за пределы контролируемой зоны;

передавать свои учтённые носители кому-либо;

вводить в ОТСС персональные данные под диктовку или с микрофона;

осуществлять попытки несанкционированного доступа к ресурсам ИСПДн, проводить или участвовать в сетевых атаках и сетевом взломе;

производить действия, направленные на взлом (несанкционированное получение привилегированного доступа) рабочих станций и серверов;

закрывать доступ к информации паролями без согласования с администратором информационной безопасности;

оставлять без личного присмотра на рабочем месте или где бы то ни было персональное устройство идентификации, машинные (съемные) носители и распечатки, содержащие защищаемую информацию;

9. Пользователь обязан обеспечить:

сохранность оборудования и физической целостности системных блоков компьютеров;

блокирование своей учетной записи в случае кратковременного оставления АРМ (нажатием клавиш Windows+L);

обязательное выключение компьютера после завершения работы;

10. Права пользователя:

участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения информационной безопасности, НСД, утраты, порчи защищаемой информации и технических компонентов ИС, если данное нарушение произошло под его идентификационными данными;

своевременно получать доступ к информационным ресурсам ИС, необходимым ему для выполнения своих должностных обязанностей;

требовать от администратора информационной безопасности смены идентификационных данных в случае появления сведений или подозрений на то, что эти данные стали известны третьим лицам.

11. Ответственность:

Пользователь несет персональную ответственность за соблюдение установленных требований во время работы. Пользователи, виновные в нарушении законодательства Российской Федерации о защите прав собственности и охраняемых по Закону сведений, несут уголовную, административную, гражданско-правовую или дисциплинарную ответственность в соответствии с действующим законодательством и организационно распорядительными документами;

пользователь отвечает за информацию, хранящуюся на его компьютере, технически исправное состояние компьютера и вверенной техники;

нарушение данной инструкции, повлекшее уничтожение, блокирование, модификацию либо копирование охраняемой законом компьютерной информации, нарушение работы компьютеров пользователей или ИСПДн в целом, может повлечь ответственность в соответствии с действующим законодательством.

3. Работа с файлами документов, внесение корректировок, уничтожение, хранение документов

№ п.п.	Этап	Описание этапа
12. Подготовка к обработке информации		
1	Получение допуска к работе	Допуск работников Департамента к ИС осуществляется в соответствии с Списком лиц, допущенных к самостоятельной работе на ИС и разрешительной системе допуска к информационным ресурсам и техническим средствам. Для работы в ИС каждый пользователь должен получить соответствующий допуск. Права по доступу к информационным ресурсам должны быть определенны утверждённой Разрешительной системой допуска к данной ИС
2	Получение исходной информации для обработки в системе	Исходная информация, обработка которой осуществляется в системе, может находиться на учтённых сменных носителях информации (съемных жестких дисках, дискетах, компакт-дисках, бумажных носителях)
3	Вход пользователя в систему	Авторизация пользователя осуществляется средствами защиты информации по имени и с использованием его персонального пароля длиной не менее 8 символов
13. Обработка информации		
1	Регистрация времени начала работы	Осуществляется средствами защиты информации
2	Ввод обрабатываемых исходных данных в систему	Ввод в систему обрабатываемой информации производится вручную с клавиатуры или путем считывания в электронном виде с дискет или компакт-дисков.

№ п.п.	Этап	Описание этапа
3	Обработка текстовой информации	Пользователь обязан принять меры по исключению возможности просмотра обрабатываемой информации с экрана монитора и с бумажных носителей (в том числе распечатываемых материалов) лицами, не допущенными к обрабатываемой информации.
4	Временное хранение обрабатываемой информации между сеансами работы пользователя в системе	Хранение обрабатываемой информации, между сеансами работы в системе, пользователь осуществляет в каталогах на жестком диске ПЭВМ, выделенных в системе для соответствующих видов обрабатываемой информации. Контроль доступа к ним осуществляется соответствующими средствами защиты информации
14. Сохранение результатов обработки информации		
1	Распечатка документов	Распечатка документов (данных) производится на принтере, входящем в состав ОТСС объекта, средствами защиты информации может осуществляться учет распечатанных документов.
2	Сохранение окончательных результатов работы	Готовые данные в электронном виде содержатся на жёстком диске ОТСС ИС, регистрация и контроль доступа к ним осуществляется средствами защиты информации.
3	Передача носителей информации и распечатанных документов	В соответствии с требованиями организационно-распорядительных документов Аппарата Губернатора и Правительства автономного округа
4	Очистка остаточной (удаленной) информации	Гарантированная очистка удаляемой с накопителей информации (без возможности ее восстановления) осуществляется средствами защиты информации
5	Регистрация времени работы и действий пользователя в системе	Осуществляется средствами защиты информации
6	Завершение работы	После окончания работы с ИС, сотрудник обязан на своем рабочем месте завершить работу всех программ, входящих в состав специализированного программного обеспечения и выключить компьютер (перегрузить). В случаи необходимости оставить свое рабочее место на непродолжительное время пользователь обязан его заблокировать (дальнейшая работа может быть продолжена

№ п.п.	Этап	Описание этапа
		пользователем только после ввода его логина и пароля). После окончания рабочего дня необходимо закрыть окна и форточки, выключать электроприборы, запереть дверь и включить охранную сигнализацию, при наличии таковой

15. Подготовка, отправка, размножение, копирование, учет, распечатка необходимого числа экземпляров подготовленных документов, содержащих информацию ограниченного доступа.

Печать производится на принтере, входящем в состав ИС.

Размножение (копирование) документов, содержащих информацию ограниченного доступа, осуществляется только на МФУ, входящих в состав аттестованного СВТ или на аттестованном средстве изготовления и размножения документов (копир) Департамента.

Подготовка, учет, отправка, документов содержащих информацию ограниченного доступа осуществляется в соответствии с требованиями раздела XI «Порядок обращения с конфиденциальной информацией» постановления Губернатора Ханты-Мансийского автономного округа – Югры от 30 декабря 2012 года № 176 «Об Инструкции по делопроизводству в государственных органах Ханты-Мансийского автономного округа – Югры и исполнительных органах государственной власти Ханты-Мансийского автономного округа – Югры» (с изменениями, внесенными постановлением Губернатора автономного округа от 16.05.2014 № 57).

Приложение 26
к приказу Департамента промышленности
Ханты-Мансийского автономного округа – Югры
от 25.08.2017 №38-П-139

РЕГЛАМЕНТ
администратора безопасности информации в
Департаменте промышленности Ханты-Мансийского автономного округа – Югры

1. Общие положения

1. Настоящий документ определяет основные обязанности, права и ответственность администратора информационной безопасности (далее – администратор ИБ) информационных систем обработки информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в том числе персональные данные (далее – ИС) Департамента.

2. Администратор ИБ осуществляет контроль выполнения требований организационных и технических мероприятий по обеспечению безопасности информации в ИС.

3. Методическое руководство и контроль работы администратора информационной безопасности Департамента осуществляется отделом технической защиты информации и противодействия иностранным техническим разведкам (далее - Отдел ТЗИ и ПД ИТР) Управления защиты информации и специальной документальной связи (далее – Управление ЗИ и СДС) Аппарата Губернатора Ханты-Мансийского автономного округа – Югры (далее – Аппарат Губернатора Югры).

4. Администратор безопасности назначается приказом по Департаменту из числа штатных работников Департамента**.**

5. Администратор ИБ должен принимать все необходимые меры по защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в том числе персональных данных (далее – конфиденциальная информация (КИ)) и контролю за соблюдением прав доступа к ней.

6. Основными задачами при обработке информации в ИС являются:

обеспечение исполнения требований нормативных правовых актов, руководящих документов, регламентирующих защиту информации в Российской Федерации в процессе создания, хранения и передачи документов, содержащих конфиденциальную информацию в ИС Департамента;

обеспечение в ИС необходимого уровня безопасности обработки, хранения и передачи КИ;

обеспечение необходимого уровня безопасности носителей КИ;

обеспечение безопасности конфиденциальной информации при ее копировании, размножении;

резервное копирование, восстановление информации.

2. Обязанности администратора информационной безопасности

7. Администратор информационной безопасности должен:

знать нормативно-методические документы в области безопасности информации и организационно-распорядительные документы в части его касающейся;

- знать состав ОТСС ИС и контролировать их соответствие техническому паспорту на ИС. Вести учет изменений аппаратно-программной конфигурации (архив заявок, на основании которых были произведены данные изменения);

- контролировать процесс управления (заведения, активации, блокирования, уничтожения) учетными записями пользователей ИС;

проверять соответствие прав доступа пользователей к объектам доступа ИС в соответствии с задачами, решаемыми пользователями в ИС и взаимодействующими с ней ИС и Разрешительной системой доступа к ИС:

контролировать назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование ИС;

проверять отсутствие в ИС учетных записей уволенных (отстраненных) сотрудников;

оповещать администратора, осуществляющего управление учетными записями пользователей, об изменении сведений о пользователях, их ролях, обязанностях, полномочиях, ограничениях;

проверять своевременность удаления временных учетных записей, предоставленных для однократного (ограниченного по времени) выполнения задач в ИС;

- контролировать неизменность настроек средств защиты информации, настройки средств защиты информации должны неизменно выполнять:

препятствие передаче защищаемой информации через сеть Интернет (или) другие информационно-телекоммуникационные сети международного информационного обмена по незащищенным линиям связи;

ограничение доступа к ИС на 10 минут при 3 неудачных попытках входа в ИС;

запрет доступа к ИС до прохождения процедур аутентификации и идентификации;

обеспечение запрета удаленного доступа к ИС;

- контролировать запрет использования в ИС технологий беспроводного доступа и мобильных технических средств;

- контролировать отсутствие доступа к ИС со стороны пользователей информационных систем сторонних организаций;

- контролировать установку на АРМ ИС ПО не связанного с задачами, решаемыми пользователями в ИС;

- вести учет съемных машинных носителей конфиденциальной информации (далее – СМНКИ);

- обеспечивать уничтожение (стирание) защищаемой информации с машинных носителей АРМ ИС, при их передаче в сторонние организации для ремонта или утилизации, либо контролировать процесс уничтожения (стирания), уничтожение защищаемой информации должно исключать возможность восстановления защищаемой информации.

- контролировать регистрацию в ИС следующих событий безопасности:

входа (выхода), а также попытки входа субъектов доступа в информационную систему и загрузки (останова) операционной системы (дата (время) входа/выхода в систему (из системы) или загрузки/останова операционной системы, результат попытки входа (успешная или неуспешная), результат попытки загрузки (останова) операционной системы (успешная или неуспешная), идентификатор, предъявленный при попытке доступа);

подключения машинных носителей информации и вывода информации на носители информации (дата и время подключения машинных носителей информации и вывода информации на носители информации, логическое имя (номер) подключаемого машинного носителя информации, идентификатор субъекта доступа, осуществляющего вывод информации на носитель информации);

запуска (завершения) программ и процессов (заданий, задач), связанных с обработкой защищаемой информации (дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа (устройства), запросившего программу (процесс, задание), результат запуска (успешный, неуспешный));

попыток доступа программных средств к защищаемым объектам доступа (дата и

время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), спецификация защищаемого файла (логическое имя, тип));

попыток удаленного доступа (дату и время попытки удаленного доступа с указанием ее результата (успешная, неуспешная), идентификатор субъекта доступа (устройства), используемый протокол доступа, используемый интерфейс доступа и (или) иную информацию о попытках удаленного доступа к информационной системе).

- контролировать права на доступ к информации о событиях безопасности: доступ должен предоставляться исключительно администратору информационной безопасности, а также системному администратору ИС, обеспечивающим функционирование ИС.

- обеспечивать постоянный контроль за выполнением пользователями ИС установленного комплекса мероприятий по обеспечению безопасности информации и соблюдения действующего законодательства в области информационной безопасности, а также инструкции пользователя и других организационно-распорядительных документов в части обеспечения безопасности информации;

- требовать от пользователей ИС и выполнять самому требования «Инструкции по установке, модификации, ремонту, техническому обслуживанию и восстановлению работоспособности программного обеспечения и аппаратных средств ИС»;

- контролировать порядок учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов;

- контролировать использование пользователями только учтенных съемных носителей. После того как цель переноса информации достигнута (переданы третьим лицам и т.п.), информация незамедлительно удаляется с носителей;

- контролировать настройки ОС и СЗИ АРМ пользователей

- проводить инструктаж пользователей по правилам работы с используемыми средствами и системами зашиты информации;

- устанавливать права доступа пользователей к информационным и техническим ресурсам ИС в соответствии с принятой и утвержденной разрешительной системой доступа;

- следить за изменением программной среды ИС и полномочиями пользователей;

- хранить дистрибутивы СЗИ, производить при необходимости восстановление программной среды СЗИ или настройки защитных механизмов операционной системы и привилегий пользователей по доступу к ресурсам ИС. При необходимости для данных мероприятий привлекать других технических специалистов отдела ЗИ;

- фиксировать и пресекать невыполнение пользователями ИС требований или норм нормативно-методических документов в области безопасности информации и организационно-распорядительных документов в информационной сфере, а также создания пользователями возможностей утечки информации;

- при получении информации о фактах нарушения политики и правил безопасности, а также попыток использования внешними нарушителями атак, в том числе с использованием методов социальной инженерии – немедленно докладывать ответственному за организацию обработки персональных данных, инициировать проведение служебной проверки (при нарушениях со стороны ответственного за организацию обработки персональных данных докладывать необходимо непосредственно вышестоящему руководству), регистрировать в журнале учёта инцидентов ИБ.

- не реже 1 раза в квартал просматривать журналы учёта и регистрации событий СЗИ (в соответствии с инструкцией по использованию программных и аппаратных средств защиты информации, операционной системы на предмет выявления подключения неучтённых носителей, попыток НСД и т.п.

- требовать от пользователей ИС и выполнять самому требования инструкции о пропускном и внутриобъектовом режимах в здании Департамента.

- контролировать отсутствие в составе ПО АРМ, входящих в ИС, средств разработки и отладки программ.

- реагировать на поступление в ИС спама (в случае присутствия данной информации в журналах событий межсетевого экрана) путем блокирования атакующего хоста.

- выполнять мероприятия по периодическому резервному копированию защищаемой информации в соответствии с «Инструкцией по резервному копированию и восстановлению данных».

- знать эксплуатационную документацию на применяемые СЗИ. Устанавливать и эксплуатировать СЗИ в соответствии с документацией.

- хранить документацию и дистрибутивы СЗИ в соответствии с техническими условиями. Компакт-диск с программным обеспечением системы должен упаковываться согласно требованиям, предусмотренным для оптических носителей;

- поддерживать настройки СЗИ, соответствующие требованиям нормативных документов по безопасности информации и протоколу аттестационных испытаний, при этом система должна реализовывать в совокупности на каждой АРМ ИС функции необходимые для выполнения требований по защите от НСД для ИС;

- контролировать срок действия сертификатов соответствия на СЗИ и обеспечить их продление в соответствии с порядком продления, приведённым ниже.

8. Администратор ИБ оказывает методическую помощь и контролирует выполнение руководителем структурного подразделения, эксплуатирующего ИС следующих действий:

при смене пользователя руководитель структурного подразделения, эксплуатирующего ИС, инициирует внесение изменений в список работников, допущенных к работе в данной ИС и в разрешительную систему доступа;

при исключении пользователя ИС из «Перечня лиц, имеющих доступ к самостоятельной работе в ИС» руководителем подразделения, эксплуатирующего ИС, принимаются меры по исключению возможности нарушения данным пользователем характеристик безопасности информации ИС.

Администратору информационной безопасности необходимо до момента доведения до сотрудника информации о прекращении его работы в ИС, лишить сотрудника возможности доступа к защищаемой информации.

9. Администратору ИБ **запрещается**:

фиксировать учетные данные пользователя (пароли, идентификаторы, ключи и др.) на твердых носителях, а также сообщать их кому бы то ни было, кроме самого пользователя;

раскрывать информацию об организации СЗ КИ в Департаменте и любую информацию, которая может создать предпосылки для возникновения канала утечки информации или создания угрозы безопасности информации.

3. Права администратора информационной безопасности

10. Требовать от пользователей ИС соблюдения установленных технологий обработки информации, выполнения нормативно-методических документов в области безопасности информации и организационно-распорядительных документов на ИС;

11. Давать своему непосредственному начальнику предложения по совершенствованию мер защиты в ИС;

12. Инициировать проведение служебных проверок по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации;

4. Ответственность

13. Администратор ИБ несет ответственность по действующему законодательству за разглашение сведений ограниченного распространения, ставших известными ему по роду деятельности.

14. Ответственность за защиту ИС от несанкционированного доступа к информации и за неукоснительное соблюдение положений настоящего руководства возлагается на администратора информационной безопасности.

5. Инструкция администратора информационной безопасности по работе с инцидентами информационной безопасности

15. Для регистрации и учета событий, которые могут привести к снижению уровня защищенности информации (далее – инцидент), в Департаменте используются встроенные механизмы регистрации и учета событий безопасности операционных систем, систем управления базами данных, прикладного программного обеспечения и средств защиты информации, а также применяться средства (системы) анализа защищенности.

16. В Департаменте обеспечен контроль заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в ИС.

Средства (системы) анализа защищенности должны обеспечивать, в том числе:

выявление и анализ уязвимостей, связанных с ошибками в конфигурации операционных систем и программного обеспечения рабочих станций и серверов ИС Департамента;

контроль установки обновлений программного обеспечения рабочих станций и серверов ИС Департамента.

17. Анализ инцидентов осуществляется:

администратором безопасности при просмотре журналов событий, формируемых средствами защиты информации, журналов событий, формируемых программным обеспечением ИС и системами управления базами данных;

системными администраторами при просмотре журналов событий сетевого и серверного оборудования, операционных систем и системного программного обеспечения.

18. Журналы аудита СЗИ от НСД и СКЗИ просматриваться администратором безопасности не реже одного раза в две недели.

19. О фактах обнаружения инцидентов администратор безопасности Департамента докладывает непосредственному руководителю, начальнику Отдела ТЗИ и ПД ИТР.

20. Управление инцидентами информационной безопасности и реагирование на них в Департаменте осуществляется в соответствии с Положением о порядке выявления и реагирования на инциденты информационной безопасности в Департаменте.

Приложение 27
к приказу Департамента промышленности
Ханты-Мансийского автономного округа – Югры
от 25.08.2017 №38-П-139

ИНСТРУКЦИЯ

должностного лица, ответственного за организацию обработки персональных данных в Департаменте промышленности Ханты-Мансийского автономного округа – Югры

1. Инструкция лица, ответственного за организацию обработки персональных данных в Департаменте промышленности Ханты-Мансийского автономного округа – Югры (далее – Инструкция), разработана в соответствии с требованиями постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных па обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, Департаментами, являющимися государственными или муниципальными органами».

2. Инструкция закрепляет обязанности, права и ответственность лица, ответственного за организацию обработки персональных данных в Департаменте.

3. Лицо, ответственного за организацию обработки персональных данных в органе назначается распорядительным документом Департамента.

4. Лицо, ответственное за организацию обработки персональных данных, в своей работе руководствуется Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», иными нормативными правовыми актами, настоящей Инструкцией, а также иными локальными нормативными актами организации, регламентирующими вопросы обработки персональных данных Департамента.

5. Лицо, ответственное за организацию обработки персональных данных в Аппарате Губернатора Югры определяет лиц, ответственных за контроль выполнения требований по обработке персональных данных, предусмотренных федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами в структурных подразделениях Департамента.

6. Перечень лиц, ответственных за контроль выполнения требований по обработке персональных данных в структурных подразделениях Департамента (по должностям) утверждает руководитель Департамента.

2. Должностные обязанности лица, ответственного за организацию обработки персональных данных в Департаменте

7. Лицо, ответственное за организацию обработки персональных данных в Департаменте обязан знать:

перечень персональных данных (далее – ПДн) обрабатываемых в Департаменте;

перечень информационных систем персональных данных Департамента (далее – ИСПДн);

перечень должностей работников Департаменте, замещение которых предусматривает осуществление обработки персональных данных, либо осуществление доступа к персональным данным;

условия и технологический процесс обработки персональных данных в Департаменте;

законодательство Российской Федерации о персональных данных, следить за его изменениями, своевременно и точно отражать изменения в локальных организационных актах по управлению средствами защиты информации в ИСПДн и правилам обработки ПДн.

8. Лицо, ответственное за организацию обработки персональных данных в

Департаменте обязано:

предоставлять на утверждение Руководителю Департамента перечень должностей работников Департамента, замещение которых предусматривает осуществление обработки персональных данных, либо осуществление доступа к персональным данным и изменения;

участвовать в определении полномочий пользователей ИСПДн (оформлении разрешительной системы доступа), минимально необходимых им для выполнения служебных (трудовых) обязанностей;

контролировать выполнение мероприятий защите информации в ИСПДн;

вносить свои предложения по совершенствованию мер защиты персональных данных в ИСПДн, разработке и принятии мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению уровня защищённости персональных данных в следствии неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных;

проводить занятия и инструктажи с работниками Департамента о порядке работы с персональными данными и изучение руководящих документов в области обеспечения безопасности ПДн;

контролировать соблюдение работниками Департаменте локальных документов, регламентирующих порядок работы с программными, техническими средствами ИСПДн и персональными данными, машинными носителями информации;

осуществлять внутренний контроль за соблюдением работниками Департамента требований законодательства Российской Федерации в области персональных данных, в том числе требований к защите персональных данных;

проводить разбирательства и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с документами, содержащими персональные данные, или по другим нарушениям, которые могут привести к снижению уровня защищённости персональных данных;

представлять интересы Департамента при проверках надзорных органов в сфере обработки персональных данных;

выполнять иные мероприятия, требуемые нормативными документами по защите персональных данных.

3. Должностные обязанности лиц, ответственных за контроль выполнения требований по обработке персональных данных в структурных подразделениях Департамента

9. Лицо, ответственное за контроль выполнения требований по обработке Пдн в структурных подразделениях Департамента организует в структурных подразделениях Департамента обработку ПДн в соответствии с требованиями предусмотренными федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

10. Лицо, ответственное за контроль выполнение требований по обработке Пдн в структурных подразделениях Департамента выполняет указания и распоряжения лица, ответственного за организацию обработки ПДн в Департаменте.

11. Лицо, ответственное за контроль выполнения требований по обработке персональных предусмотренных в структурных подразделениях Департамента обязан знать:

перечень ПДн обрабатываемых в структурном подразделении Департамента;

перечень и состав ИСПДн структурного подразделения Департамента;

перечень должностей работников структурного подразделения Департамента, замещение которых предусматривает осуществление обработки персональных данных, либо осуществление доступа к персональным данным;

перечень лиц, допущенных к самостоятельной обработки ПДн в ИСПДн;

условия и технологический процесс обработки ПДн в структурном подразделении Департамента;

законодательство Российской Федерации о персональных данных, следить за его изменениями, своевременно и точно отражать изменения в локальных организационных актах по управлению средствами защиты информации в ИСПДн и правилам обработки ПДн.

12. Лицо, ответственное за контроль выполнения требований по обработке Пдн в структурных подразделениях Департамента обязано:

своевременно представляет перечень должностей работников Департамента, замещение которых предусматривает осуществление обработки персональных данных, либо осуществление доступа к персональным данным и изменения к нему лицу, ответственному за организацию обработки ПДн в Департаменте;

осуществлять учет лиц, допущенных к работе с персональными данными в журнале учета лиц, допущенных к работе с персональными данными в ИСПДн структурного подразделения Департамента»;

доводить до сведения работников структурного подразделения Департамента положения законодательства Российской Федерации в области ПДн, локальных актов по вопросам обработки персональных данных, требований к защите Пдн;

организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей, а также осуществлять контроль за приемом и обработкой таких обращений и запросов;

осуществлять фиксацию фактов обращений и запросов субъектов персональных данных или их представителей в журнале учета обращений граждан (субъектов ПДн) о выполнении их законных прав при обработке персональных данных в Департаменте;

принимать необходимые меры по восстановлению нарушенных прав субъектов персональных данных;

осуществлять взаимодействие по обеспечению безопасности персональных данных с администратором информационной безопасности;

участвовать в определении полномочий пользователей ИСПДн (оформлении разрешительной системы доступа), минимально необходимых им для выполнения служебных (трудовых) обязанностей;

осуществлять учёт документов, содержащих персональные данные, их уничтожение, либо контроль процедуры их уничтожения;

блокировать доступ к персональным данным при обнаружении нарушений порядка их обработки;

своевременно реагировать на попытки несанкционированного доступа к информации.

контролировать осуществление мероприятий по установке и настройке средств защиты информации;

вносить свои предложения по совершенствованию мер защиты Пдн в ИСПДн, разработке и принятии мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению уровня защищённости ПДн в следствии неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн;

проводить занятия и инструктажи с работниками Департамента о порядке работы с персональными данными и изучение руководящих документов в области обеспечения безопасности ПДн;

контролировать соблюдение работниками структурного подразделения Департамента локальных документов, регламентирующих порядок работы с программными, техническими средствами ИСПДн и персональными данными, машинными носителями информации;

осуществлять внутренний контроль за соблюдением работниками структурного подразделения Департамента требований законодательства Российской Федерации в области персональных данных;

выполнять иные мероприятия, требуемые нормативными документами по защите персональных данных.

4. Действия при обнаружении попыток несанкционированного доступа

13. К попыткам несанкционированного доступа относятся:

сеансы работы с ПДн незарегистрированных пользователей, или пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истёк, или превышающих свои полномочия по доступу к данным;

действия третьего лица, пытающегося получить доступ (или уже получившего доступ) к ИСПДн, при использовании учётной записи администратора или другого пользователя ИСПДн, методом подбора пароля, использования пароля, разглашённого владельцем учётной записи или любым другим методом.

14. При выявлении факта несанкционированного доступа лицо, выявившее факт несанкционированного доступа (пользователи, ответственный за организацию обработки ПДн, лицо, ответственное за выполнение требований по обработке Пдн в структурных подразделениях Департамента, администратор информационной безопасности) обязаны:

законными способами прекратить несанкционированный доступ к ПДн;

известить администратора информационной безопасности ИСПДн о факте несанкционированного доступа;

известить руководителя структурного подразделения, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка несанкционированного доступа, о факте несанкционированного доступа;

известить руководство Департамента.

15. Лицо, ответственное за руководство работами по защите информации в Департаменте, организует разбирательство по факту несанкционированного доступа;

16. По результатам разбирательства лицо, ответственное за организацию обработки ПДн докладывает заместителю руководителя лицу, ответственному за руководство работами по защите информации в Департаменте служебной запиской о факте несанкционированного доступа, его результате (успешный, неуспешный) и предпринятых действиях.

5. Права

17. Ответственный за организацию обработки ПДн в Департаменте и лица, ответственные за контроль выполнения требований по обработке персональных данных в структурных подразделениях Департамента имеют право:

требовать от работников выполнения федерального закона «О персональных данных» и принятых в соответствии с ним нормативными правовыми актами, а также локальных нормативно-правовых актов в части работы с персональными данными;

блокировать доступ к ПДн любых пользователей, если это необходимо для предотвращения нарушения режима защиты ПДн;

проводить служебные расследования и опрашивать пользователей по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с техническими и программными средствами ИСПДн, в том числе со средствами защиты информации, или по другим нарушениям, которые могут привести к снижению уровня защищённости персональных данных;

привлекать к реализации мер, направленных на выполнение требований законодательства о персональных данных, иных работников Департамента с возложением на них соответствующих обязанностей и закреплением ответственности;

иметь доступ к информации, касающейся обработки персональных данных в

соответствующем структурном подразделении Департамента и включающей:

цели обработки персональных данных;

категории обрабатываемых персональных данных;

категории субъектов, персональные данные которых обрабатываются;

правовые основания обработки персональных данных;

перечень действий с персональными данными, общее описание используемых в центральном аппарате Роскомнадзора способов обработки персональных данных;

дату начала обработки персональных данных;

срок или условия прекращения обработки персональных данных;

сведения о наличии или об отсутствии трансграничной передачи персональных данных в процессе их обработки;

сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством Российской Федерации.

6. Ответственность

18. Ответственный за организацию обработки персональных данных в Департаменте и лица, ответственные за контроль выполнения требований по обработке персональных данных в структурных подразделениях Департамента несут персональную ответственность за соблюдение требований настоящей Инструкции, за качество проводимых ими работ по обработке и обеспечению безопасности персональных данных.

19. Ответственный за организацию обработки персональных данных в Департаменте и лица, ответственные за контроль выполнения требований по обработке персональных данных в структурных подразделениях Департамента при нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несёт дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

20. Пользователи несут персональную ответственность за все действия, совершенные от имени его учётной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учётной записи.

Приложение 28
к приказу Департамента промышленности
Ханты-Мансийского автономного округа – Югры
от 25.08.2017 №38-П-139

Список
лиц, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими служебных (трудовых) обязанностей

№	Должность	Ф.И.О.	Кабинет	Наименование ИСПДн
1.				
2.				
3.				

Доступ предоставил:_____
ФИО

Дата:_____ Подпись:_____

Приложение 29
к приказу Департамента промышленности
Ханты-Мансийского автономного округа – Югры
от 25.08.2017 №38-П-139

Обязательство
о неразглашении информации, содержащей персональные данные

Я, _____
(фамилия, имя, отчество полностью)

являясь работником Департамента промышленности Ханты-Мансийского автономного округа – Югры, в должности _____
_____
_____
_____
_____,
(указать должность и наименование структурного подразделения)

обязуюсь прекратить обработку персональных данных (т. е. 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), ставших известными мне в связи с исполнением должностных обязанностей, в случае расторжения со мной трудового договора.

В соответствии со статьей 7 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» я уведомлен(а) о том, что персональные данные являются конфиденциальной информацией, и я обязан(а) не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, ставшие известными мне в связи с исполнением должностных обязанностей.

Я предупрежден(а) о том, что в случае нарушения данного обязательства буду привлечен(а) к ответственности в соответствии с законодательством Российской Федерации.

дата	подпись	расшифровка

Приложение 30
к приказу Департамента промышленности
Ханты-Мансийского автономного округа – Югры
от 25.08.2017 №38-П-139

Типовая форма согласия субъекта
на обработку их персональных данных

Я, _____,
(Ф.И.О.)
_____ серия _____ № _____ выдан _____
(вид документа, удостоверяющего личность)
_____,
(когда и кем)
проживающий(ая) по адресу _____
_____,
настоящим даю свое согласие уполномоченным должностным лицам
_____
(наименование и адрес органа государственной власти)
на обработку моих персональных данных и подтверждаю, что, давая такое согласие, я действую своей волей и в своих интересах.

Согласие дается мною для целей _____
_____
(цель обработки персональных данных)
и распространяется на следующую информацию: _____
_____
_____
(перечень персональных данных)

Настоящее согласие предоставляется на осуществление любых действий в отношении моих персональных данных, которые необходимы для достижения указанных выше целей, включая без ограничения сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение, а также осуществление любых иных действий с моими персональными данными с учетом федерального законодательства.

В случае неправомерного использования предоставленных мною персональных данных согласие отзывается моим письменным заявлением.

Данное согласие действует с "__" _____ 20__ г. бессрочно и может быть отозвано в любое время по моему письменному заявлению.

"___" _____ 20__ г. _____
(подпись)

Приложение 31
к приказу Департамента промышленности
Ханты-Мансийского автономного округа – Югры
от 25.08.2017 №38-П-139

Типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные

Уважаемый(ая) _____

В соответствии с требованиями статей 26, 42 Федерального закона от 27.07.2004 №79-ФЗ «О государственной гражданской службе Российской Федерации», Положением о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела, утвержденным Указом Президента Российской Федерации от 30.05.2005 № 609, и Положением о конкурсе на замещение вакантной должности государственной гражданской службы Российской Федерации, утвержденным Указом Президента Российской Федерации от 01.02.2005 № 112, определены персональные данные, которые Вы, как субъект персональных данных, обязан предоставить в связи с оформлением трудовых отношений с Департаментом промышленности Ханты-Мансийского автономного округа-Югры (далее — Департамент) в случае отказа Вами предоставить свои персональные данные Департамент не сможет на законных основаниях реализовать с Вами трудовые или служебные отношения.

В соответствии с действующим законодательством РФ в области персональных данных Вы имеете право: на получение сведений о Департаменте (в объеме, необходимом для защиты своих прав и законных интересов по вопросам обработки своих персональных данных), о месте нахождения Департамента, о наличии своих персональных данных, а также на ознакомление с такими персональными данными; подавать запрос на доступ к своим персональным данным; требовать безвозмездного предоставления возможности ознакомления со своими персональными данными, а также внесения в них необходимых изменений, их уничтожения или блокирования при предоставлении сведений, подтверждающих, что такие персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки; получать уведомления по вопросам обработки персональных данных в установленных действующим законодательством Российской Федерации случаях и сроки; требовать от Департамента разъяснения порядка защиты субъектом персональных данных своих прав и законных интересов; обжаловать действия или бездействие Департамента в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке; на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

_____/ _____/ Работник отдела кадров /
(дата) (подпись) (расшифровка подписи)

Приложение 32
к приказу Департамента промышленности
Ханты-Мансийского автономного округа – Югры
от 25.08.2017 №38-П-139

ЖУРНАЛ
учета машинных носителей персональных данных (установленных в ПЭВМ)

№ п/п	Регистрационный номер	Тип и ёмкость	Дата и место установки (использования)	Ответственное должностное лицо (Ф.И.О)

ЖУРНАЛ
учета машинных носителей персональных данных (отчуждаемых)

№ п/п	Регистрационный номер	Тип и ёмкость	Получил (Ф.И.О, дата, подпись)	Сдал (Ф.И.О, дата, подпись)	Место хранения	Ответственное должностное лицо (Ф.И.О)

ЖУРНАЛ
учета лиц, допущенных к персональным данным

№ п/п	Сведения о допуске к персональным данным				Сведения о прекращении допуска к персональным данным	
	Наименование информационной системы персональных данных	ФИО, должность получившего допуск	Дата и номер приказа о допуске	Дата и подпись допускаемого лица	Дата и номер приказа о прекращении допуска	Номер приказа об увольнении или дата и подпись лица об ознакомлении с документом, прекращающим допуск к ПДн

ЖУРНАЛ
учета средств защиты информации

№ п/п	Индекс и наименование средства защиты информации	Серийный (заводской) номер	Номер специального защитного знака	Наименование организации, установившей СЗИ	Место установки	Примечание

ЖУРНАЛ
учета средств криптографической защиты информации

№ п/п	Наименование криптосредства, эксплуатационной и технической документации к ним, ключевых документов	Регистрационные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче		Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечания
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя криптосредств	Дата и расписка в получении	Ф.И.О. пользователя криптосредств, производившего подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены криптосредства	Дата изъятия (уничтожения)	Ф.И.О. пользователя СКЗИ, производившего изъятие (уничтожение)	Номер акта или расписка об уничтожении	
1														

ЖУРНАЛ
учета хранилищ

№ п/п	Регистрационный (учетный) номер хранилища	Вид хранилища	Дата постановки на учет	Фамилия и подпись принявшего (ответственного), дата	Место расположения (номер помещения)	Дата и номер акта о выводе из эксплуатации	Примечание

ЖУРНАЛ
учета выдачи паролей

№ п/п	Дата получения пароля	Ф.И.О. получателя	Подпись получателя

ЖУРНАЛ
учета обращений субъектов персональных данных по вопросам обработки персональных данных

№ п/п	Дата обращения	ФИО обратившегося	Цель обращения	Отметка о предоставлении информации или отказе в ее предоставлении / дата предоставления или отказа в предоставлении информации	Подпись ответственного	Примечание

ЖУРНАЛ
антивирусных проверок

№ п/п	Дата и время проверки	Наименование ИСПДн (составной части ИСПДн)	Какими средствами проводилась проверка	Результаты проверки		Наименование инфицированных файлов, источника поступления (носитель, организация)	Примечание (принятые меры)	Фамилия и подпись лица, проводившего проверку
				кол-во проверенных файлов	кол-во инфицированных файлов			
1								

ЖУРНАЛ
учета выявленных инцидентов информационной безопасности

№ п/п	Дата и время	Описание инцидента	Ответственный за реагирование на инцидент	Отметка об устранении инцидента	Дата устранения инцидента	Подпись ответственного лица	Примечание

ЖУРНАЛ
учета передачи персональных данных

№ п/п	Сведения о запрашивающем лице	Состав запрашиваемых персональных данных	Цель получения персональных данных	Отметка о передаче или отказе в передаче персональных данных	Дата передачи/отказа в передаче персональных данных	Подпись запрашивающего лица

ЖУРНАЛ
периодического тестирования средств защиты информации

№ п/п	Наименование средства защиты информации от НСД или криптосредства	Регистрационные номера СЗИ от НСД или криптосредства	Дата тестирования	Фамилия и подпись ответственного пользователя, проводившего тестирование	Наименование теста, используемые средства для проведения теста	Результат тестирования (успешный/неуспешный), комментарий	Дата очередного тестирования

ЖУРНАЛ
уничтожения носителей персональных данных

№ п/п	Наименование ИСПДн, в которой уничтожаются персональные данные	Ф.И.О. субъекта, персональные данные которого подлежат уничтожению	Обоснование уничтожения	Наименование файла, и его месторасположение	Дата уничтожения	Ф.И.О. и подпись Исполнителя	Ф.И.О. и подпись ответственного за обработку персональных данных

Приложение 33
к приказу Департамента промышленности
Ханты-Мансийского автономного округа – Югры
от 25.08.2017 №38-П-139

АКТ

определения уровня защищенности информационной системы
Департамента промышленности Ханты-Мансийского автономного округа – Югры

Председатель комиссии _____
Члены комиссии _____
_____
_____

Рассмотрев исходные данные информационной системы _____
_____
(наименование информационной системы или сегмента)
Департамента промышленности Ханты-Мансийского автономного округа – Югры (далее - ИС), комиссия определила:

- Категории персональных данных обрабатываемых в ИС: в сегменте информационной системе обрабатываются_____;
(категория обрабатываемых Пдн)

- Категории субъектов: персональные данные субъектов персональных данных, (работники/не работники) Департамента;

- Объем обрабатываемых персональных данных: менее _____;

- Тип актуальных угроз: для сегмента информационной системы актуальны угрозы N-го типа;

- Уровень значимости информации: информация имеет *(низкий уровень значимости (УЗ 3), средний уровень значимости (УЗ 2), высокий уровень значимости (УЗ 1);

- Масштаб сегмента информационной системы: сегмент информационной системы имеет объектовый масштаб.

Комиссия решила, в соответствии с Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а также в соответствии с приказом ФСТЭК Российской Федерации от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и на основании анализа исходных данных, необходимо обеспечить *(первый, второй, третий уровень защищенности (УЗ 1,2,3)) персональных данных и установить *(первый, второй, третий класс защищенности сегмента информационной системы (К 1,2,3).

Результат оценки вреда:

Для информационной системы актуальны угрозы *(1,2,3-го типа).

Уровень значимости информации определен степенью возможного ущерба для обладателя информации от нарушения конфиденциальности (неправомерные доступ, копирование, предоставление или распространение), целостности (неправомерные уничтожение или модифицирование) или доступности (неправомерное блокирование) информации, руководствуясь следующей формулой:

УЗ = [(конфиденциальность, степень ущерба) (целостность, степень ущерба) (доступность, степень ущерба)], где степень возможного ущерба определяется обладателем информации.

Комиссия утвердила следующее:

УЗ = [(конфиденциальность, низкая степень ущерба) (целостность, низкая степень ущерба) (доступность, низкая степень ущерба)] – таким образом, комиссия установила *(низкий, средний, высокий уровень значимости (УЗ 3,2,1) (возможны незначительные негативные последствия).

Председатель комиссии _____

Члены комиссии

_____

_____

_____

«__»_____2017 г.

*-выбирается по актуальности

Приложение 34
к приказу Департамента промышленности
Ханты-Мансийского автономного округа – Югры
от 25.08.2017 №38-П-139

АКТ

классификации информационной системы
Департамента промышленности Ханты-Мансийского автономного округа – Югры

Комиссия в составе:

Председатель комиссии _____
Члены комиссии _____
_____
_____

Рассмотрев исходные данные информационной системы _____
_____
(наименование информационной системы или сегмента)

Департамента промышленности Ханты-Мансийского автономного округа – Югры, условия ее эксплуатации (многопользовательский с разными правами доступа к информации), с учетом характера обрабатываемой информации (персональные данные) и в соответствии с руководящими документами Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» и «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)»,

РЕШИЛА

Установить информационной системы класс защищенности_____
_____
(наименование информационной системы или сегмента)

Департамента промышленности Ханты-Мансийского автономного округа – Югры **Класс защищенности 1Г**.

Председатель комиссии _____
Члены комиссии _____
_____
_____

«__»_____2017 г.

Приложение 35
к приказу Департамента промышленности
Ханты-Мансийского автономного округа – Югры
от 25.08.2017 №38-П-139

АКТ

об уничтожении персональных данных субъектов персональных данных

Комиссия в составе:

Роль	ФИО	Должность
Председатель		
Члены комиссии		

Установила, что на основании достижения цели обработки персональных данных, в соответствии с требованиями Федерального закона Российской Федерации от 27 июля 2006 г. №152-ФЗ «О персональных данных» гл. 2, ст. 5, пункт 7, подлежат уничтожению сведения, составляющие персональные данные:

№ п/п	Сведения, содержащие персональные данные	Место хранения	Кол-во ед. хранения	Примечание

Указанные персональные данные уничтожены путем_____

_____

(удаления с помощью средств гарантированного удаления информации, уничтожения носителя и т.п.)

Председатель комиссии:

_____ _____
подпись расшифровка

Члены комиссии:

_____ _____
подпись расшифровка

_____ _____
подпись расшифровка