БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
ХАНТЫ-МАНСИЙСКОГО АВТОНОМНОГО ОКРУГА-ЮГРЫ
«ЦЕНТР ИМУЩЕСТВЕННЫХ ОТНОШЕНИЙ»

ПРИКАЗ № 13/01-П-85

«27» июня 2023 года г. Ханты-Мансийск

О мерах бюджетного учреждения
Ханты-Мансийского
автономного округа – Югры
«Центр имущественных отношений»,
направленных на
обеспечение защиты информации,
в том числе составляющей персональные данные

Во исполнение требований Федеральных законов от 27 июля 2006 года № 152-ФЗ «О персональных данных» и № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Указа Президента Российской Федерации от 01 мая 2022 года № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации», постановлений Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных», и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказа Роскомнадзора от 28 октября 2022 года № 179 «Об утверждении Требований

к подтверждению уничтожения персональных данных» и в целях приведения локальных нормативных актов бюджетного учреждения Ханты-Мансийского автономного округа – Югры «Центр имущественных отношений» в соответствии с действующим законодательством Российской Федерации и иных нормативных правовых актов в сфере защиты информации,

ПРИКАЗЫВАЮ:

1. Назначить должностных лиц, ответственных за:

1.1. Руководство работами по технической защите информации и обеспечение безопасности конфиденциальной информации в бюджетном учреждении Ханты-Мансийского автономного округа – Югры «Центр имущественных отношений» (далее – Учреждение) – начальника административного отдела Пузанкова Сергея Александровича.

1.2. Обеспечение безопасности персональных данных и другой конфиденциальной информации (администратор информационной безопасности) при их обработке в информационных системах (далее – ИС) Учреждения, за реализацию мероприятий по технической защите информации в Учреждении – техника 1 категории административного отдела Ильина Юрия Вячеславовича.

1.3. Проведение технических работ (техническое сопровождение) в ИС Учреждения (системный администратор) – инженера 1 категории административного отдела Ротаря Юрия Алексеевича.

1.4. Эксплуатацию информационных систем персональных данных - должностные лица, определенные в Приложении 8 к настоящему приказу.

2. Утвердить:

2.1. Регламент ответственного за организацию обработки персональных данных, руководство работами по технической защите информации и обеспечение безопасности конфиденциальной информации в Учреждении (Приложение 1).

2.2. Регламент ответственного за обеспечение безопасности персональных данных и другой конфиденциальной информации (администратор информационной безопасности) при их обработке в ИС Учреждения, за реализацию мероприятий по технической защите информации в Учреждении (Приложение 2).

2.3. Форму обязательства о неразглашении работником Учреждения информации, содержащей персональные данные (Приложение 3).

2.4. Порядок уничтожения персональных данных при достижении целей обработки и (или) при наступлении иных законных оснований (Приложение 4).

2.5. Перечень должностей работников Учреждения, ответственных за выполнение требований по обработке персональных данных (Приложение 5).

2.6. Перечень должностей работников Учреждения, ответственных за проведение мероприятий по обезличиванию персональных данных (Приложение 6).

2.7. Правила работы с обезличенными персональными данными в Учреждении (Приложение 7).

2.8. Перечень информационных систем Учреждения, предназначенных для обработки информации ограниченного доступа (Приложение 8).

2.9. Перечень категорий персональных данных и должностей работников Учреждения, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным, обрабатываемых в том числе в информационных системах Учреждения (Приложение 9).

2.10. Положение об организации режима обеспечения безопасности помещений, в которых размещены информационные системы персональных данных, препятствующего возможности неконтролируемого

проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения (Приложение 10).

2.11. Положение о постоянно действующей технической комиссии по защите информации в Учреждении (Приложение 11).

2.12. Порядок использования паролей в автоматизированных системах Учреждения (Приложение 12).

2.13. Порядок защиты компонентов информационных систем в Учреждении (Приложении 13).

2.14. Инструкцию по установке, модификации, ремонту, техническому обслуживанию и восстановлению работоспособности программного обеспечения и аппаратных средств (Приложение 14).

2.15. Инструкцию по организации парольной защиты в информационных системах Учреждения (Приложение 15).

2.16. Инструкцию по проведению антивирусного контроля информационных систем Учреждения (Приложение 16).

2.17. Инструкцию по работе с инцидентами информационной безопасности в информационных системах Учреждения (Приложение 17).

2.18. Инструкцию по резервному копированию и восстановлению данных в информационных системах Учреждения (Приложение 18).

2.19. Положение пользователя по обеспечению безопасности информации в информационных системах Учреждения (Приложение 19).

2.20. Положение об организации и проведении работ по обеспечению безопасности персональных данных при их обработке в информационных системах Учреждения (Приложение 20).

2.21. План мероприятий по обеспечению безопасности информации, обрабатываемой в информационных системах Учреждения (Приложение 21).

2.22. Регламент ответственного за эксплуатацию информационных систем персональных данных Учреждения (Приложение 22).

2.23. Инструкцию о пропускном и внутриобъектовом режимах Учреждения (Приложение 23).

2.24. Инструкцию по обработке персональных данных без использования средств автоматизации в Учреждении (Приложение 24).

2.25. Инструкцию по обращению со средствами криптографической защиты информации в Учреждении (Приложение 25).

2.26. Правила работы лиц, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими должностных (трудовых) обязанностей (Приложение 26).

2.27. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в Учреждении (Приложение 27).

3. Ответственным лицам, определенных настоящим приказом, а также ответственным за организацию обработки персональных данных в Учреждении организовать выполнение мероприятий по обеспечению требований Федерального закона Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных» и принятых в соответствии с ним нормативных правовых актов Российской Федерации, а также руководствоваться настоящим приказом.

4. Признать утратившими силу приказы Учреждения:

- от 27 марта 2018 года № 13/01-П-27 «О назначении ответственных лиц»;

- от 02 октября 2018 года № 13/01-П-77 «О мерах, направленных на обеспечение выполнения требований Федерального закона «О персональных данных».

5. Начальнику отдела делопроизводства и кадровой работы Муратовой С.С. ознакомить с настоящим приказом работников Учреждения.

6. Контроль за исполнением настоящего приказа возложить на заместителя директора Зарубина А.С.

И.о. директора С.П. Исраилова

Исполнитель:

начальник административного отдела

Пузанков Сергей Александрович

Приложение 1
к приказу бюджетного учреждения
Ханты-Мансийского автономного округа – Югры
«Центр имущественных отношений»
№ 13/01-П-85 от «27» июня 2023 г.

Регламент ответственного за организацию обработки персональных данных, руководство работами по технической защите информации и обеспечение безопасности конфиденциальной информации в бюджетном учреждении Ханты-Мансийского автономного округа – Югры «Центр имущественных отношений» (далее – Регламент)

1. Общие положения

1.1. Регламент определяет обязанности, ответственность и права должностного лица, ответственного за организацию обработки персональных данных, руководство работами по технической защите информации и обеспечение безопасности конфиденциальной информации в бюджетном учреждении Ханты-Мансийского автономного округа – Югры «Центр имущественных отношений» (далее соответственно – ответственный за организацию персональных данных, Учреждение).

1.2. Ответственный за организацию обработки персональных данных назначается локальным нормативным актом Учреждения.

1.3. Ответственный за организацию обработки персональных данных в своей деятельности руководствуется Трудовым кодексом Российской Федерации, Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ), постановлениями Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств

автоматизации», от 01 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», от 21 марта 2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствие с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», иными нормативными правовыми актами Российской Федерации в области обеспечения безопасности персональных данных и локальными нормативными актами Учреждения по обеспечению безопасности персональных данных.

2. Обозначение и сокращение

АС - автоматизированная система;

АРМ - автоматизированное рабочее место;

ВТСС - вспомогательные технические средства и системы;

ИБ - информационная безопасность;

ИС - информационная система;

ИСПДн - информационная система персональных данных;

ОРД - организационно-распорядительная документация;

ОС - операционная система.

ОТСС - основные технические средства и системы;

ПДн - персональные данные;

ПО - программное обеспечение;

ПЭВМ - персональная электронно-вычислительная машина;

СВТ - средства вычислительной техники;

СЗИ - средства защиты информации;

СЗПДн - система (подсистема) защиты персональных данных;

СКЗИ - средства криптографической защиты информации;

УБПДн - угрозы безопасности персональных данных;

НСД - несанкционированный доступ к информации.

3. Обязанности

3.1. Ответственный за организацию обработки персональных данных в Учреждении обязан знать:

- перечень ПДн обрабатываемых в Учреждении;

- перечень ИСПДн Учреждении;

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

- условия и технологический процесс обработки персональных данных в Учреждении;

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

3.2. Ответственный за организацию обработки персональных данных в Учреждении обязан:

- осуществлять внутренний контроль соблюдения Учреждением и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

- довести до сведения работников Учреждения положений законодательства Российской Федерации о персональных данных, локальных актов Учреждения по вопросам обработки персональных данных, требований к защите персональных данных;

- организовать прием и обработку обращений и запросов субъектов персональных данных или их представителей и осуществление контроля приема и обработки таких обращений и запросов.

- уведомить директора Учреждения о выявленных нарушениях обработки персональных данных или требований по их защите, принимаемых мерах и способах устранения выявленных нарушений;

- предоставлять на утверждение руководителю Учреждения перечень должностей работников Учреждения, замещение которых предусматривает осуществление обработки персональных данных, либо осуществление доступа к персональным данным и изменения к нему;

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

- контролировать выполнение мероприятий по защите информации в ИСПДн Учреждения;

- 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 Учреждения о порядке работы с персональными данными и изучение руководящих документов в области обеспечения безопасности ПДн;

- контролировать соблюдение работниками Учреждения локальных нормативных актов, регламентирующих порядок работы с программными, техническими средствами ИСПДн и персональными данными, машинными носителями информации;

- 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 Учреждения при проверках надзорных органов в сфере обработки персональных данных;

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

4. Функции

4.1. Ответственный за организацию обработки персональных данных в Учреждении выполняет следующие функции:

- руководство и координация деятельности по обеспечению безопасности информации в соответствии с требованиями законодательством Российской Федерации, нормативных правовых актов Президента и Правительства Российской Федерации, руководящих и методических документов Федеральной службы по техническому и экспортному контролю (далее - ФСТЭК России) Российской Федерации и Федеральной Службы Безопасности Российской Федерации;

- контроль выполнения работ по информационной безопасности в Учреждении;

- принимает решение о возможности распространения (передачи) персональных данных и иной конфиденциальной информации;

- согласовывает назначение администратора информационной безопасности информационных систем Учреждения;

- представляет на утверждение директору Учреждения перечень должностных лиц, доступ которых к конфиденциальной информации, обрабатываемой в ИС Учреждения, необходим для выполнения ими своих служебных обязанностей;

- осуществляет контроль по поддержанию функционирования системы защиты информации в Учреждении;

- осуществляет контроль соответствия реального состава пользователей матрице доступа;

- осуществляет контроль должностных лиц, допущенных к работе с конфиденциальной информацией в ИС;

- осуществляет согласование документов, определяющих построение, внедрение, модернизацию системы защиты информации в ИС Учреждения;

- осуществляет контроль за уровнем безопасности информации в Учреждении;

- инициирует и организовывает проведение служебных проверок по фактам несоблюдения условий, которые могут привести к нарушению конфиденциальности информации или другим нарушениям, приводящим к снижению уровня защищенности информации;

- осуществляет координацию и руководство работой ПДТК по защите информации.

5. Права

5.1. Ответственный за организацию обработки персональных данных в Учреждении имеет право:

- требовать от работников Учреждения выполнения Федерального закона № 152 и принятых в соответствии с ним нормативных правовых актов, а также локальных нормативных актов Учреждения в части работы с персональными данными;

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

- проводить служебные проверки 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 Учреждения с возложением на них соответствующих обязанностей и закреплением ответственности;

- иметь доступ к информации, касающейся обработки персональных данных в соответствующем структурном подразделении Учреждения 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;

- 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

6.1. Несет персональную ответственность за соблюдение требований Регламента, за качество проводимых им работ по обработке и обеспечению безопасности персональных данных.

6.2. 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.

Приложение 2
к приказу бюджетного учреждения
Ханты-Мансийского автономного округа – Югры
«Центр имущественных отношений»
№ 13/01-П-85 от «27» июня 2023 г.

Регламент ответственного за обеспечение безопасности персональных данных и другой конфиденциальной информации (администратор информационной безопасности) при их обработке в информационной системе бюджетного учреждения Ханты-Мансийского автономного округа – Югры «Центр имущественных отношений», за реализацию мероприятий по технической защите информации в бюджетном учреждении Ханты-Мансийского автономного округа – Югры «Центр имущественных отношений»

(далее – Регламент)

1. Общие положения

1.1. Регламент определяет обязанности, права, ответственность и порядок работы с инцидентами информационной безопасности и должностного лица, ответственного за обеспечение безопасности персональных данных и другой конфиденциальной информации (администратор информационной безопасности) при их обработке в информационной системе бюджетного учреждения Ханты-Мансийского автономного округа – Югры «Центр имущественных отношений», за реализацию мероприятий по технической защите информации в бюджетном учреждении Ханты-Мансийского автономного округа – Югры «Центр имущественных отношений» (далее соответственно – Администратор ИБ, Учреждение).

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

1.3. Администратор ИБ назначается локальным нормативным актом Учреждения из числа штатных работников Учреждения.

1.4. 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.

1.5. 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 Учреждения;

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

- обеспечение необходимого уровня безопасности носителей КИ;

- обеспечение безопасности конфиденциальной информации при ее копировании, размножении;

- резервное копирование, восстановление информации.

2. Обозначение и сокращение

АС - автоматизированная система;

АРМ - автоматизированное рабочее место;

ВТСС - вспомогательные технические средства и системы;

ИБ - информационная безопасность;

ИС - информационная система;

ИСПДн - информационная система персональных данных;

ОРД - организационно-распорядительная документация;

ОС - операционная система.

ОТСС - основные технические средства и системы;

ПДн - персональные данные;

ПО - программное обеспечение;

ПЭВМ - персональная электронно-вычислительная машина;

СВТ - средства вычислительной техники;

СЗИ - средства защиты информации;

СЗПДн - система (подсистема) защиты персональных данных;

СКЗИ - средства криптографической защиты информации;

УБПДн - угрозы безопасности персональных данных;

НСД - несанкционированный доступ к информации.

3. Особенности организации работы в ИСПДнН

3.1. Администратор ИБ должен знать, что: ИСПДн Учреждения относятся к многопользовательским ИС с разными правами доступа пользователей к ресурсам ИСПДн. Группы пользователей, работающих в ИСПДн: администратор информационной безопасности, пользователи ИСПДн. Данные группы пользователей имеют права доступа к ресурсам ИСПДн в соответствии с разрешительной системой доступа пользователей к ресурсам ИСПДн.

4. Обязанности

4.1. Администратор ИБ обязан:

- 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:

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

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

в) запрет доступа к ИС до прохождения процедур аутентификации и идентификации;

г) 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 РТС;

- вести учет съемных машинных носителей конфиденциальной информации;

- 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:

а) 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);

б) 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);

в) 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);

г) 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);

д) 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 ИСУ,

- 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;

- 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 Учреждения;

- 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 в информационных системах»;

- 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.

4.2. 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.

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

4.4. 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 ИС и КИ в Учреждении и любую информацию, которая может создать предпосылки для возникновения канала утечки информации или создания угрозы безопасности информации.

5. Права

5.1. Требовать от пользователей ИСПДн соблюдения установленных технологий обработки информации, выполнения нормативно-

методических документов в области безопасности информации и организационно-распорядительных документов на ИСПДн.

5.2. Участвовать в разработке мероприятий по совершенствованию безопасности персональных данных.

5.3. Давать своему непосредственному руководителю свои предложения по совершенствованию мер защиты в ИСПДн.

6. Ответственность

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

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

7. Порядок работы с инцидентами информационной безопасности

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

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

7.3. 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 Учреждения;

- контроль установки обновлений программного обеспечения рабочих станций и серверов ИС Учреждения.

7.4. 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.

7.5. Журналы аудита СЗИ от НСД и СКЗИ просматриваются администратором ИБ не реже одного раза в две недели.

7.6. О фактах обнаружения инцидентов администратор ИБ Учреждения докладывает непосредственному руководителю, ответственному за организацию обработки персональных данных в Учреждении.

7.7. Управление инцидентами информационной безопасности и реагирование на них в Учреждении осуществляется в соответствии с инструкцией по работе с инцидентами информационной безопасности в информационных системах Учреждения.

Приложение 3

к приказу бюджетного учреждения

Ханты-Мансийского автономного округа – Югры

«Центр имущественных отношений»

№ 13/01-П-85 от «27» июня 2023 г.

Форма

Директору бюджетного учреждения
Ханты-Мансийского
автономного округа – Югры
«Центр имущественных отношений»
адрес: г. Ханты-Мансийск, улица Коминтерна, дом 23
ИНН 8601001003
ОГРН 1028600510421
Ф.И.О
от _____

Обязательства о неразглашении работником бюджетного учреждения Ханты-Мансийского автономного округа – Югры «Центр имущественных отношений» информации, содержащей персональные данные

я,_____
(фамилия, имя, отчество, должность)

являясь работником бюджетного учреждения Ханты-Мансийского автономного округа - Югры «Центр имущественных отношений» (далее - Учреждение) и непосредственно осуществляя обработку персональных данных, ознакомлен(а) с требованиями по соблюдению конфиденциальности обрабатываемых мной персональных данных и обязуюсь в случае расторжения Учреждением со мной трудового договора прекратить обработку персональных данных, ставших мне известными в связи с исполнением должностных обязанностей.

Я предупрежден(а), что разглашение персональных данных, обрабатываемых в Учреждении, утрата носителей персональных данных, передача третьим лицам, публикация без согласия субъекта персональных данных, а также использование для занятия любой деятельностью, которая может нанести ущерб субъекту персональных данных, влечет уголовную, административную, гражданско-правовую или иную ответственность в

соответствии с действующим законодательством, в виде лишения свободы, денежного штрафа и других наказаний.

До моего сведения также доведены с разъяснениями соответствующие положения, инструкции, приказы по обеспечению безопасности персональных данных.

Настоящее обязательство хранится в личном деле работника.

«____»_____202_ г. _____
(Подпись)

Один экземпляр обязательства получил _____
(Подпись, дата)

Приложение 4
к приказу бюджетного учреждения
Ханты-Мансийского автономного округа – Югры
«Центр имущественных отношений»
№ 13/01-П-85 от «27» июня 2023 г.

Порядок
уничтожения персональных данных при достижении целей обработки и (или) при наступлении иных законных оснований
(далее – Порядок)

1. Порядок устанавливает условия, сроки, способы уничтожения персональных данных при достижении целей обработки и (или) при наступлении иных законных оснований, а также способы их фиксации, в соответствии с требованиями приказа Роскомнадзора от 28.10.2022 № 179 «Об утверждении Требований к подтверждению уничтожения персональных данных».

2. Условия и сроки уничтожения персональных данных бюджетным учреждением Ханты-Мансийского автономного округа – Югры «Центр имущественных отношений» (далее – Учреждение):

- достижение цели обработки персональных данных либо утрата необходимости достигать эту цель - в течение 30 дней;

- достижение максимальных сроков хранения документов, содержащих персональные данные, - в течение 30 дней;

- предоставление субъектом персональных данных (его представителем) подтверждения того, что персональные данные получены незаконно или не являются необходимыми для заявленной цели обработки, - в течение семи рабочих дней;

- отзыв субъектом персональных данных согласия на обработку его персональных данных, если их сохранение для цели их обработки более не

требуется - в течение 30 дней.

2.1. При достижении цели обработки персональных данных, а также в случае отзыва субъектом персональных данных согласия на их обработку персональные данные подлежат уничтожению, если:

- иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных;

- Учреждение не вправе осуществлять обработку без согласия субъекта персональных данных на основаниях, предусмотренных Законом о персональных данных или иными федеральными законами;

- иное не предусмотрено другим соглашением между Учреждением и субъектом персональных данных.

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

Уничтожение персональных данных осуществляет комиссия, созданная локальным нормативным актом Учреждения, в присутствии ответственного за организацию обработки персональных данных.

3. При обработка персональных данных осуществляемой Учреждением без использования средств автоматизации, документом, подтверждающим уничтожение персональных данных субъектов персональных данных, является акт об уничтожении персональных данных.

4. При обработке персональных данных осуществляемой Учреждением с использованием средств автоматизации, документами, подтверждающими уничтожение персональных данных субъектов персональных данных, являются акт об уничтожении персональных данных, соответствующий требованиям, содержащимся в пунктах 4 и 5 Порядка, и выгрузка из журнала регистрации событий в информационной

системе персональных данных (далее - выгрузка из журнала).

5. Акт об уничтожении персональных данных должен содержать:

5.1. Наименование (юридического лица) или фамилию, имя, отчество (при наличии) (физического лица) и адрес Учреждения.

5.2. Наименование (юридического лица) или фамилию, имя, отчество (при наличии) (физического лица), адрес лица (лиц), осуществляющего (осуществляющих) обработку персональных данных субъекта (субъектов) персональных данных по поручению Учреждения (если обработка была поручена такому (таким) лицу (лицам).

5.3. Фамилию, имя, отчество (при наличии) субъекта (субъектов) или иную информацию, относящуюся к определенному (определенным) физическому (физическим) лицу (лицам), чьи персональные данные были уничтожены.

5.4. Фамилию, имя, отчество (при наличии), должность лиц (лица), уничтоживших персональные данные субъекта персональных данных, а также их (его) подпись.

5.5. Перечень категорий, уничтоженных персональных данных субъекта (субъектов) персональных данных.

5.6. Наименование уничтоженного материального (материальных) носителя (носителей), содержащего (содержащих) персональные данные субъекта (субъектов) персональных данных, с указанием количества листов в отношении каждого материального носителя (в случае обработки персональных данных без использования средств автоматизации).

5.7. Наименование информационной (информационных) системы (систем) персональных данных, из которой (которых) были уничтожены персональные данные субъекта (субъектов) персональных данных (в случае обработки персональных данных с использованием средств автоматизации).

5.8. Способ уничтожения персональных данных.

5.9. Причину уничтожения персональных данных.

5.10. Дату уничтожения персональных данных субъекта (субъектов)

персональных данных.

6. Акт об уничтожении персональных данных в электронной форме, подписанный в соответствии с законодательством Российской Федерации, признается электронным документом, равнозначным акту об уничтожении персональных данных на бумажном носителе, подписанному собственноручной подписью лиц, указанного в подпункте 5.3 пункта 5 Порядка.

7. Выгрузка из журнала должна содержать:

7.1. Фамилию, имя, отчество (при наличии) субъекта (субъектов) или иную информацию, относящуюся к определенному (определенным) физическому (физическим) лицу (лицам), чьи персональные данные были уничтожены.

7.2. Перечень категорий, уничтоженных персональных данных субъекта (субъектов) персональных данных.

7.3. Наименование информационной системы персональных данных, из которой были уничтожены персональные данные субъекта (субъектов) персональных данных.

7.4. Причину уничтожения персональных данных.

7.5. Дату уничтожения персональных данных субъекта (субъектов) персональных данных.

8. В случае если выгрузка из журнала не позволяет указать отдельные сведения, предусмотренные пунктом 7 Порядка, недостающие сведения вносятся в акт об уничтожении персональных данных.

9. В случае если обработка персональных данных осуществляется Учреждением одновременно с использованием средств автоматизации и без использования средств автоматизации, документами, подтверждающими уничтожение персональных данных субъектов персональных данных, являются акт об уничтожении персональных данных, соответствующий требованиям, установленным пунктами 5 и 6 Порядка, и выгрузка из журнала, соответствующая требованиям, установленным пунктом 7

Порядка.

10. Акт об уничтожении персональных данных и выгрузка из журнала подлежат хранению в течение 3 лет с момента уничтожения персональных данных.

11. Способы уничтожения персональных данных в зависимости от типа носителя (бумажный или электронный):

11.1. Без использования средств автоматизации (бумажный носитель) – измельчаются механическим способом до степени, исключающей возможность прочтения текста (шредерирование) или сжигаются.

11.2. С использование средств автоматизации (электронный носитель) - (удаление файла (docx, rtf, xps, txt, html, xml и pdf, путем стирания (безвозвратно) со средств вычислительной техники (компьютера), в том числе с использованием сертифицированного программного обеспечения, установленного на АРМ с гарантированным уничтожением (в соответствии с заданными характеристиками для установленного программного обеспечения с гарантированным уничтожением)).

11.3. Уничтожение части персональных данных, если это допускается материальным носителем, производится способом, исключающим дальнейшую обработку этих персональных данных, с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (на бумажном носителе - путем обезличивания персональных данных субъекта персональных данных).

Приложение 5
к приказу бюджетного учреждения
Ханты-Мансийского автономного округа – Югры
«Центр имущественных отношений»
№ 13/01-П-85 от «27» июня 2023 г.

Перечень должностей работников бюджетного учреждения Ханты-Мансийского автономного округа – Югры «Центр имущественных отношений, ответственных за выполнение требований по обработке персональных данных

№ п/п	Структурное подразделение	Наименование должности
1.	Административный отдел	Начальник отдела
2.	Отдел бухгалтерского учета и отчетности	Начальник отдела, Главный бухгалтер
3.	Отдел делопроизводства и кадровой работы	Начальник отдела
4.	Юридический отдел	Начальник отдела
5.	Отдел планирования и размещения закупок	Начальник отдела
6.	Отдел обеспечения сохранности и государственного учета документов	Начальник отдела
7.	Отдел инвентаризации и обеспечения совершения сделок с имуществом	Начальник отдела
8.	Отдел сбора и систематизации сведений для государственной кадастровой оценки	Начальник отдела
9.	Отдел определения кадастровой стоимости	Начальник отдела
10.	Отдел актуализации кадастровой стоимости	Начальник отдела
11.	Отдел кадастровых работ, развития и сопровождения геоинформационных систем	Начальник отдела

Приложение 6

к приказу бюджетного учреждения

Ханты-Мансийского автономного округа – Югры

«Центр имущественных отношений»

№ 13/01-П-85 от «27» июня 2023 г.

Перечень должностей работников бюджетного учреждения Ханты-Мансийского автономного округа Югры «Центр имущественных отношений», ответственных за проведение мероприятий по обезличиванию персональных данных

№ п/п	Структурное подразделение	Наименование должности
1.	Административный отдел	Начальник отдела
2.	Отдел бухгалтерского учета и отчетности	Начальник отдела, Главный бухгалтер
3.	Отдел делопроизводства и кадровой работы	Начальник отдела
4.	Юридический отдел	Начальник отдела
5.	Отдел планирования и размещения закупок	Начальник отдела
6.	Отдел обеспечения сохранности и государственного учета документов	Начальник отдела
7.	Отдел инвентаризации и обеспечения совершения сделок с имуществом	Начальник отдела
8.	Отдел сбора и систематизации сведений для государственной кадастровой оценки	Начальник отдела
9.	Отдел определения кадастровой стоимости	Начальник отдела
10.	Отдел актуализации кадастровой стоимости	Начальник отдела
11.	Отдел кадастровых работ, развития и сопровождения геоинформационных систем	Начальник отдела

Приложение 7
к приказу бюджетного учреждения
Ханты-Мансийского автономного округа – Югры
«Центр имущественных отношений»
№ 13/01-П-85 от «27» июня 2023 г.

Правила работы с обезличенными персональными данными в бюджетном учреждении Ханты-Мансийского автономного округа – Югры «Центр имущественных отношений» (далее – Правила)

1. Общие положения

1.1. Правила разработаны в целях обеспечения защиты от несанкционированного использования персональных данных, сохранения возможности обработки персональных данных, ведения статистического учета и отчетности, недопущения снижения уровня защищенности информационных систем бюджетного учреждения Ханты-Мансийского автономного округа – Югры «Центр имущественных отношений» (далее – Учреждение), а также по достижении целей обработки персональных данных или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством Российской Федерации.

1.2. Обезличивание персональных данных осуществляется в соответствии с требованиями:

- Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

- постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее – Постановление № 1119);

- приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

- приказа Роскомнадзора от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных»;

- методических рекомендаций по применению приказа Роскомнадзора от 5 сентября 2013 г. № 996 «Об утверждении требований и методов по обезличиванию персональных данных» (утв. Роскомнадзором 13.12.2013).

1.3. Правила регулируют отношения, возникающие при проведении мероприятий по обезличиванию персональных данных в Учреждении.

1.4. Правила обязательны для исполнения лицам, ответственным за проведение мероприятий по обезличиванию персональных данных в Учреждении.

1.5. Обезличивание персональных данных осуществляется лицами, ответственными за проведение мероприятий по обезличиванию персональных данных в структурных подразделениях Учреждении, определенных приказом Учреждения.

1.6. Контроль за соблюдением требований по обезличиванию персональных данных осуществляется должностным лицом, ответственным за организацию обработки персональных данных в Учреждении.

2. Способы и методы обезличивания персональных данных

2.1. Обезличивание персональных данных осуществляется в соответствии с требованиями и методами по обезличиванию персональных данных, утвержденных приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 05.09.2013 № 996.

2.2. Методы обезличивания должны обеспечивать требуемые свойства обезличенных данных, соответствовать предъявляемым

требованиям к их характеристикам (свойствам), быть практически реализуемыми в различных программных средах и позволять решать поставленные задачи обработки персональных данных.

2.3. К наиболее перспективным и удобным для практического применения относятся следующие методы обезличивания:

метод введения идентификаторов (замена части сведений (значений персональных данных) идентификаторами с созданием таблицы (справочника) соответствия идентификаторов исходным данным). Для реализации метода требуется установить атрибуты персональных данных, записи которых подлежат замене идентификаторами, разработать систему идентификации, обеспечить ведение и хранение таблиц соответствия;

метод изменения состава или семантики (изменение состава или семантики персональных данных путем замены результатами статистической обработки, обобщения или удаления части сведений). Для реализации метода требуется выделить атрибуты персональных данных, записи которых подвергаются изменению, определить набор правил внесения изменений и иметь возможность независимого внесения изменений для данных каждого субъекта. При этом возможно использование статистической обработки отдельных записей данных и замена конкретных значений записей результатами статистической обработки (средние значения, например);

метод декомпозиции (разбиение множества (массива) персональных данных на несколько подмножеств (частей) с последующим раздельным хранением подмножеств). Для реализации метода требуется предварительно разработать правила декомпозиции, правила установления соответствия между записями в различных хранилищах, правила внесения изменений и дополнений в записи и хранилища;

метод перемешивания (перестановка отдельных записей, а также групп записей в массиве персональных данных). Для реализации метода требуется разработать правила перемешивания и их алгоритмы, правила и

алгоритмы деобезличивания и внесения изменений в записи. Метод может использоваться совместно с методами введения идентификаторов и декомпозиции.

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

2.5. В целях обезличивания персональных данных и в случаях наличия необходимости в Учреждении применяется метод изменения состава или семантики в целях представления в установленном порядке статистической информации для заинтересованной стороны в соответствии с требованиями законодательства Российской Федерации.

3. Требования к свойствам получаемых обезличенных данных

3.1. При выполнении обезличивания персональных данных получаемый результат должен обеспечивать:

сохранение полноты (состав обезличенных данных должен полностью соответствовать составу обезличиваемых персональных данных);

сохранение структурированности обезличиваемых персональных данных;

сохранение семантической целостности обезличиваемых персональных данных;

анонимность отдельных данных не ниже заданного уровня (количества возможных сопоставлений, обезличенных данных между собой для деобезличивания).

3.2. Требования к свойствам метода обезличивания:

обратимость (возможность проведения деобезличивания);

возможность обеспечения заданного уровня анонимности;

увеличение стойкости при увеличении объема обезличиваемых персональных данных.

4. Порядок работы с обезличенными персональными данными

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

4.5. 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;

требований Постановления Правительства Российской Федерации от 01.11.2012 г. № 1119.

4.6. При обработке обезличенных персональных данных без использования средств автоматизации, в целях исключения несанкционированного доступа к обезличенным персональным данным, возможности их несанкционированного уничтожения, изменения, блокирования, копирования, распространения, а также иных неправомерных действий, необходимо соблюдение:

правил хранения бумажных носителей;

правил доступа к ним и в помещения, где они хранятся;

4.7. При осуществлении процедур обезличивания не допускается совместное хранение персональных данных и обезличенных персональных данных.

При хранении также обеспечивается конфиденциальность дополнительной (служебной) информации о выбранном методе обезличивания персональных данных и параметрах процедуры обезличивания персональных данных.

4.8. В определённых случаях обезличивание персональных данных субъектов должно производиться Учреждением перед внесением их в информационную систему.

4.9. В процессе обработки обезличенных данных Учреждением, при необходимости, может проводиться деобезличивание.

После обработки персональные данные, полученные в результате такого деобезличивания, уничтожаются.

4.10. Обработка обезличенных данных должна осуществляться в соответствующих формах представления и хранения данных.

5. Ответственность

5.1. Лица, ответственные за проведение мероприятий по обезличиванию персональных данных в структурных подразделениях Учреждении несут персональную ответственность за соблюдение требований настоящих Правил и за качество проводимых работ по обезличиванию персональных данных.

Приложение 8

к приказу бюджетного учреждения

Ханты-Мансийского автономного округа – Югры

«Центр имущественных отношений»

№ 13/01-П-85 от « 27 » июня 2023 г.

Перечень информационных систем бюджетного учреждения

Ханты-Мансийского автономного округа – Югры

«Центр имущественных отношений», предназначенных для обработки

информации ограниченного доступа

№ п/п	Наименование информационной системы персональных данных	Уровень защищенности персональных данных/класс защищенности АС	Принадлежность к структурному подразделению, адрес местонахождения (использования)	Ответственный за эксплуатацию,
1	1 С Предприятие	УЗ 4	Отдел бухгалтерского учёта и отчётности, ул.Чехова, 27А	Главный бухгалтер
2	Контур Экстерн	УЗ 4	Отдел бухгалтерского учёта и отчётности, отдел делопроизводства и кадровой работы, ул.Чехова, 27А	Главный бухгалтер, начальник отдела делопроизводства и кадровой работы
3	Сбербанк Бизнес Онл@йн	УЗ 4	Отдел бухгалтерского учёта и отчётности, ул.Чехова, 27А	Главный бухгалтер
4	Бизнес-портал Открытие	УЗ 4	Отдел бухгалтерского учёта и отчётности, ул.Чехова, 27А	Главный бухгалтер
5	ГАС Правосудие	УЗ 4	Юридический отдел, ул.Чехова 27А	Начальник отдела
6	СЭД Дело	УЗ 4	Структурные подразделения	Начальники отделов
7	Портал ССТУ.РФ	УЗ 4	Отдел делопроизводства и кадровой работы, ул.Чехова 27А	Начальник отдела
8	АИС «МФЦ»	УЗ 4	Отдел инвентаризации и обеспечения совершения сделок с имуществом, Отдел обеспечения сохранности и государственного учёта документов, ул.Чехова 27А	Начальники отдела

9	ГИС Госзаказ	УЗ 4	Отдел планирования и размещения закупок, ул.Чехова 27А	Начальник отдела
10	Единая информационная система в сфере закупок (ЕИС)	УЗ 4	Отдел планирования и размещения закупок, ул.Чехова 27А	Начальник отдела
11	Фабрикант, электронная торговая площадка	УЗ 4	Отдел инвентаризации и обеспечения совершения сделок с имуществом, ул.Чехова 27А	Начальник отдела
12	Исполнение бюджета Информационно-аналитическая система (WEB-Исполнение)	УЗ 4	Отдел бухгалтерского учёта и отчётности, ул.Чехова, 27А	Главный бухгалтер
13	Региональный электронный бюджет ХМАО-Югры	УЗ 4	Отдел бухгалтерского учёта и отчётности, ул.Чехова, 27А	Главный бухгалтер
14	Система исполнения регламентов	УЗ 4	Отдел обеспечения сохранности и государственного учёта документов, ул.Чехова 27А, ул.Коминтерна 23	Начальник отдела
15	ИС «Удостоверяющий центр Федерального казначейства»	УЗ 4	Административный отдел, ул.Чехова, 27А	Начальник отдела
16	Сбербанк-АСТ	УЗ 4	Отдел планирования и размещения закупок, ул.Чехова 27А	Начальник отдела
17	Росэлторг	УЗ 4	Отдел планирования и размещения закупок, ул.Чехова 27А	Начальник отдела
18	РТС-тендер	УЗ 4	Отдел планирования и размещения закупок, ул.Чехова 27А	Начальник отдела
19	Национальная электронная площадка	УЗ 4	Отдел планирования и размещения закупок, ул.Чехова 27А	Начальник отдела
20	Заказ РФ	УЗ 4	Отдел планирования и размещения закупок, ул.Чехова 27А	Начальник отдела
21	РАД Госзакупки	УЗ 4	Отдел планирования и размещения закупок, ул.Чехова 27А	Начальник отдела
22	ЭТП ГПБ Электронная торговая площадка Газпромбанка	УЗ 4	Отдел планирования и размещения закупок, ул.Чехова 27А	Начальник отдела
23	ЭТП ТЭК-Торг	УЗ 4	Отдел планирования и размещения закупок, ул.Чехова 27А	Начальник отдела

Приложение 9
к приказу бюджетного учреждения
Ханты-Мансийского автономного округа – Югры
«Центр имущественных отношений»
№ 13/01-П-85 от «27» июня 2023 г.

Перечень категорий персональных данных и должностей работников бюджетного учреждения Ханты-Мансийского автономного округа – Югры «Центр имущественных отношений», замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным, обрабатываемых в том числе в информационной системе бюджетного учреждения Ханты-Мансийского автономного округа – Югры «Центр имущественных отношений»

№ п/п	Структурное подразделение, должность	Категория обрабатываемых персональных данных
1	Директор, Первый заместитель директора, Заместитель директора	Все категории персональных данных образующихся по всем направлениям деятельности БУ «Центр имущественных отношений» (далее – Учреждение): - сведения о работниках Учреждения, накапливаемых в личных делах работников; - сведения по претендентам на замещение вакантных должностей; - сведения о получателях (физических лицах) государственных услуг, услуг приносящий доход детальности и контрагентах (физических лицах) по контрактам (договорам) по закупке товаров, работ, услуг.

2	Руководители структурных подразделений	Все категории персональных данных обрабатываемых по направлению деятельности структурного подразделения Учреждения: - сведения о работниках вверенного структурного подразделения, накапливаемых в личных делах работников; - сведения о получателях (физических лицах) государственных услуг, услуг приносящий доход детальности и контрагентах (физических лицах) по контрактам (договорам) по закупке товаров, работ, услуг.
3	Юридический отдел, юрист 1 категории	Все категории персональных данных обрабатываемых в рамках юридического сопровождения (претензионная, судебная работа) деятельности Учреждения: - сведения о работниках Учреждения, накапливаемых в личных делах работников; - сведения о получателях (физических лицах) государственных услуг, услуг приносящий доход детальности и контрагентах (физических лицах) по контрактам (договорам) по закупке товаров, работ, услуг.
4	Отдел делопроизводства и кадровой работы: Специалист по кадрам 1, 2 категории, Специалист по охране труда	Все категории персональных данных обрабатываемых в рамках реализации трудовых отношений Учреждения: - сведения о работниках, их близких родственниках Учреждения, накапливаемых в личных делах работников; - сведения о претендентах на замещение вакантных должностей; - сведения о получателях (физических лицах) государственных услуг, услуг приносящий доход детальности и контрагентах (физических лицах) по контрактам (договорам) по закупке товаров, работ, услуг.
5	Отдел делопроизводства и кадровой работы, специалист по охране труда	Все категории персональных данных обрабатываемых в рамках соблюдения требований по охране труда в Учреждении: - сведения о работниках Учреждения, накапливаемых в личных делах работников. - сведения о работниках контрагентов при выполнении работ, услуг в рамках контракта (договора) выполняемых на территории Учреждения (при наличии согласия на обработку персональных данных).

6	Все работники следующих структурных подразделений: - отдел обеспечения сохранности и государственного учета документов; - отдел инвентаризации и обеспечения совершения сделок с имуществом; - отдел кадастровых работ, развития и сопровождения геоинформационных систем; - отдел определения кадастровой стоимости; - отдел актуализации кадастровой стоимости; - отдел сбора и систематизации сведений для государственной кадастровой оценки	Все категории персональных данных обрабатываемых в рамках оказания государственных услуг и услуг, приносящих доход деятельности, в том числе функций реализуемых в целях оказания таких услуг: - сведения о получателях (физических лицах), в том числе о правах на объекты недвижимости.
7	Главный бухгалтер, Все работники отдела бухгалтерского учета и отчетности	Все категории персональных данных обрабатываемых в рамках осуществления финансового обеспечения Учреждения: - сведения о работниках, их близких родственниках Учреждения, накапливаемых в личных делах работников; - сведения о получателях (физических лицах) государственных услуг, услуг приносящий доход детальности и контрагентах (физических лицах) по контрактам (договорам) по закупке товаров, работ, услуг.
8	Все работники отдела планирования и размещения закупок	Все категории персональных данных обрабатываемых в рамках закупок товаров, работ, услуг в Учреждении: - сведения о контрагентах (физических лицах) при выполнении работ, услуг в рамках контракта (договора).
9	Все работники административного отдела	Все категории персональных данных обрабатываемых Учреждением в информационных системах (автоматизированная обработка).

Приложение 10
к приказу бюджетного учреждения
Ханты-Мансийского автономного округа – Югры
«Центр имущественных отношений»
№ 13/01-П-85 от «27» июня 2023 г.

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

1. Общие положения

1.1. Положение регулирует порядок допуска пользователей к работе в информационных системах бюджетного учреждения Ханты-Мансийского автономного округа – Югры «Центр имущественных отношений» (далее – Учреждение) и предназначено для руководящего состава Учреждения, руководителей структурных подразделений Учреждения.

1.2. Обозначение и сокращение

АРМ - автоматизированное рабочее место;

ИСПДн - информационная система персональных данных;

ОТСС - основные технические средства и системы;

ПДн - персональные данные;

ЭВМ - электронно-вычислительная машина.

2. Порядок допуска к ИСПДн и в помещения размещения ОТСС

2.1. Положение направлено на достижение следующих задач:

- допуск к информации, обрабатываемой в ИСПДн, строго определённого перечня лиц;

- самостоятельный допуск в помещения с установленными в них ОТСС ИСПДн строго определённого перечня лиц;

- закрепление за каждым пользователем определённого ему для работы АРМ ИСПДн и определённых ему информационных ресурсов в ИСПДн.

2.2. Для выполнения задач, обозначенных в п. 2.1 Положения, Учреждением принимаются следующие локальные нормативные акты:

- Перечень лиц, имеющих право допуска к обработке сведений, составляющих персональные данные в информационных системах персональных данных Учреждения, содержит перечень лиц (ФИО, отдел, должность), имеющих право допуска к каждому АРМ ИС. Разрабатывается и актуализируется администратором информационной безопасности в порядке, описанном данным Положением. Копия списка находится у руководителя административного отдела в целях исключения допуска к работе с АРМ не закреплённых за ними пользователей;

- Разрешительная система доступа персонала к информационным ресурсам ИСПДн. Разрабатывается и актуализируется (для каждой ИСПДн Учреждения) администратором информационной безопасности в порядке настоящего Положения;

- Перечень лиц, имеющих право доступа (неконтролируемого пребывания) в помещения, в которых ведется обработка персональных данных. Содержит сведения о помещениях и перечень лиц (ФИО, отдел, должность), имеющих право самостоятельного доступа в помещения, снятия помещения с охраны и получения ключей от него. Готовится и поддерживается в актуальном состоянии администратором информационной безопасности.

2.3. Для работы в ИСПДн каждый пользователь должен получить соответствующий допуск. Под допуском к ИСПДн понимается

возможность самостоятельного доступа пользователя к средствам информатизации ИСПДн (средства электронно-вычислительной техники, системы и сети ЭВМ, системы и сети электросвязи, программные средства). Право допуска предоставляется пользователю только после включения его в соответствующий перечень лиц, имеющих право допуска к обработке сведений, составляющих персональные данные в информационных системах персональных данных.

Устные указания кого бы то ни было об установлении права доступа пользователю к ИСПДн либо об изменении его прав доступа не имеют юридической силы и необязательны для исполнения. Администратор информационной безопасности не могут быть наказаны за невыполнение подобного указания от вышестоящего руководства.

Процедура получения (лишения/ограничение) соответствующего права допуска пользователя для работников Учреждения инициируется заявкой руководителя структурного подразделения в адрес директора Учреждения по форме, согласно Приложения (далее – Заявка). Непосредственно допуск/ограничение (лишение) допуска осуществляется после включения работника Учреждения в соответствующий локальный нормативный акт Учреждения, и подписания им обязательства о неразглашении персональных данных. Подписание и хранение обязательства о неразглашении персональных данных в личном деле работника, организуется работниками отдела делопроизводства и кадровой работы.

Администратор информационной безопасности, после получения Заявки, которые впоследствии хранятся у него:

- Вносит соответствующие изменения в локальные нормативные акты, которыми утверждены: перечень лиц, имеющих право допуска к обработке сведений, составляющих персональные данные в информационных системах и разрешительная система доступа персонала к ИСПДн. Указанные изменения утверждаются директором Учреждения.

- После утверждения указанных локальных нормативных актов администратор информационной безопасности обеспечивает:

а) Регистрацию (удаление) персонального имени (учетная запись пользователя) и пароля, под которым пользователь регистрируется и работает в системе в соответствии с Инструкцией по организации парольной защиты в информационных системах Учреждения;

б) Внесение необходимых изменений администратором сети, серверов, баз данных в списки пользователей соответствующих подсистем и СУБД;

в) Настройку средств защиты и программного обеспечения АРМ пользователя, соответствующим категориям защиты.

- Обновлённый «Перечень лиц, имеющих право допуска к обработке сведений, составляющих персональные данные в информационных системах персональных данных» рассылается администратором информационной безопасности заинтересованным работникам Учреждения.

- Вносятся соответствующие изменения и утверждаются локальным нормативным актом Учреждения в «Перечень лиц, имеющих право доступа (неконтролируемого пребывания) в помещения, в которых ведется обработка персональных данных».

- При исключении пользователя ИС из «Перечня лиц, имеющих право допуска к обработке сведений, составляющих персональные данные в информационных системах» руководителям структурных подразделений необходимо направлять заявку в адрес директора Учреждения до момента объявления пользователю о лишении его прав на допуск к ИСПДн. Обязательным является уведомление руководителем структурного подразделения о планируемом лишении прав доступа или изменения полномочий сотрудника по доступу к ресурсам ИСПДн администратора информационной безопасности, в письменной форме. Администратором информационной безопасности принимаются меры по исключению

возможности нарушения данными лицами характеристик безопасности информации ИСПДн.

2.4. В таком же порядке осуществляется включение (исключение) в локальный нормативной акт Учреждения утвержденным перечень лиц, имеющих право доступа (неконтролируемого пребывания) в помещения, в которых ведется обработка персональных данных.

2.5. Локальными нормативными актами Учреждения, которыми утверждены: перечни лиц, имеющих право допуска к обработке сведений, составляющих персональные данные в информационных системах и перечни лиц, имеющих право доступа (неконтролируемого пребывания) в помещения, в которых ведется обработка персональных данных» в своей повседневной деятельности руководствуются руководители структурных подразделений, работники Учреждения (технические специалисты) и администратор информационной безопасности. Администратор информационной системы осуществляет контроль соблюдения правомерного доступа работников в указанных перечнях.

3. Требования по организации режимных мер

3.1. Состав ИС должен соответствовать техническому паспорту. Обработка не учтённых в техпаспорте технических средств запрещается. Все технические средства ИСПДн должны размещаться в соответствии с техническим паспортом.

Изменение состава ОТСС в составе ИСПДн допускается только после согласования с органом по аттестации. В адрес органа по аттестации на соответствие требованиям по защите информации направляется письменное уведомление о планируемых изменениях. Изменения осуществляются после получения рекомендаций органа по аттестации. Ответственным за данные мероприятия является администратор информационной безопасности.

Полный порядок действий при модификации, обновлении программного обеспечения и других изменениях в ИСПДн приведён в Инструкция по установке, модификации, ремонту, техническому обслуживанию и восстановлению работоспособности программного обеспечения и аппаратных средств Учреждения.

Контроль соблюдения данных требований и ведения учета средств информатизации ИСПДН возлагается на администратора информационной безопасности.

3.2. Помещения, в которых размещаются средства информатизации ИСПДн, должны исключать возможность бесконтрольного проникновения в него посторонних лиц. Помещения должны быть оборудованы пожарной сигнализацией, находящейся в работоспособном состоянии. Уборка помещений должна осуществляться в присутствии работников, имеющих право самостоятельного допуска в помещение.

Ключи от кабинетов должны храниться на посту охраны. Работники Учреждения в начале рабочего дня должны получать ключи от кабинетов под роспись. В конце рабочего дня все ключи должны сдаваться на пост охраны. Должен вестись журнал выдачи ключей.

При обнаружении факта несанкционированного проникновения в помещения лиц, не входящих в утверждённый локальным нормативным актом перечень лиц, имеющих право доступа (неконтролируемого пребывания) в помещения, в которых ведется обработка персональных данных Учреждения, администратор информационной безопасности или другие лица (в зависимости от обнаружившего данный факт) обязаны немедленно сообщить о происшедшем ответственному за организацию обработки персональных данных в Учреждении.

По данному происшествию проводится служебная проверка с установлением последствий проникновения для безопасности информации (нарушение целостности, доступности и конфиденциальности), обрабатываемой в ИСПДн.

При утере ключа от помещения работники, имеющие право допуска в помещение, обязаны сообщить о случившемся администратору информационной безопасности. Руководством принимаются меры по исключению возможности хищения носителей информации и ОТСС ИС (замена замков или другие меры).

3.3. Технические средства АРМ в помещении размещаются таким образом, чтобы исключить возможность просмотра экрана видеомонитора и распечаток принтера лицами, не имеющими отношения к обрабатываемой информации. Не допускается перемещение АРМ в другие помещения.

3.4. Ключи от серверной комнаты хранятся на посту охраны и выдаются с обязательной отметкой (дата, получатель, цель получения) о выдаче в журнале свободной формы.

3.5. Техническое обслуживание и ремонт средств информатизации проводится в соответствии с Инструкцией по установке, модификации, ремонту, техническому обслуживанию и восстановлению работоспособности программного обеспечения и аппаратных средств Учреждения.

4. Ответственность за нарушение режимных мер

4.1. Ответственность за обеспечение безопасности информации в ИСПДн, своевременную разработку и осуществление необходимых мероприятий по обеспечению безопасности информации несёт администратор информационной безопасности. Контроль за обеспечением режима безопасности информации и требований настоящего Положения возлагается на администратор информационной безопасности.

4.2. Нарушение требований настоящего Положения является дисциплинарным проступком. По каждому случаю проводится служебная проверка.

Невыполнение требований настоящего Положения рассматривается как нарушение трудовой дисциплины и влечет за собой дисциплинарное взыскание.

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

Форма

Директору бюджетного учреждения
Ханты-Мансийского
автономного округа – Югры
«Центр имущественных отношений»
адрес: г. Ханты-Мансийск, улица Коминтерна, дом 23
ИНН 8601001003
ОГРН 1028600510421

Ф.И.О, наименование должности
(руководителя структурного подразделения)
_____
_____

Заявка на внесение изменений в списки пользователей
ИСПДн _____
(наименование ИСПДн)
и наделение пользователей полномочиями доступа к информационным системам бюджетного учреждения Ханты-Мансийского автономного округа – Югры «Центр имущественных отношений»,

Прошу зарегистрировать пользователем (исключить из списка пользователей, изменить полномочия пользователя) (ненужное зачеркнуть) в ИСПДн

_____
(наименование ИСПДн)
_____
(должность с указанием структурного подразделения)
_____
(фамилия имя и отчество работника)

предоставив ему полномочия, необходимые (лишив его полномочий, необходимых) (ненужное зачеркнуть)
для решения задач:

_____

(список задач: чтение, обработка)

_____

на следующих рабочих местах (АРМ):

_____

(номер помещения)

Обязательство о неразглашении персональных данных, обрабатываемых в ИС, мною проверено и хранится в личном деле работника.

_____20__ г.

_____ _____

(подпись) (ФИО)

Приложение 11
к приказу бюджетного учреждения
Ханты-Мансийского автономного округа – Югры
«Центр имущественных отношений»
№ 13/01-П-85 от «27» июня 2023 г.

Положение о постоянно действующей технической комиссии по защите информации в бюджетном учреждении Ханты-Мансийского автономного округа – Югры «Центр имущественных отношений» (далее – Положение)

1. Общие положения

1.1. Положение разработано в соответствии с Федеральным законом 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 РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», приказом ФСТЭК России от 18.02.2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и иными нормативными правовыми актами

Российской Федерации, регулирующими отношения в области защиты государственной тайны.

1.2. Положение определяет функции, состав и порядок функционирования постоянно действующей технической комиссии по защите информации бюджетного учреждения Ханты-Мансийского автономного округа – Югры «Центр имущественных отношений» (далее соответственно - ПДТК по ЗИ, Комиссия, Учреждение). ПДТК по ЗИ является коллегиальным совещательным органом при директоре Учреждения, 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 также обрабатываемых в информационных системах Учреждения.

1.3. ПДТК по ЗИ вносит директору Учреждения предложения по вопросам защиты, как общедоступной информации, так и информации ограниченного доступа обрабатываемой, циркулирующей, накапливаемой в Учреждении.

1.4. ПДТК по ЗИ в своей работе руководствуется Конституцией Российской Федерации, федеральными законами, указами и распоряжениями Президента Российской Федерации, постановлениями и распоряжениями Правительства Российской Федерации, нормативно методическими документами ФСБ России и ФСТЭК России, решениями Межведомственной комиссии по защите государственной тайны, законами Ханты-Мансийского автономного округа – Югры, постановлениями и распоряжениями Губернатора и Правительства Ханты-Мансийского автономного округа – Югры, распоряжениями и указаниями Аппарата Губернатора Ханты-Мансийского автономного округа - Югры (по вопросам защиты информации), решениями Постоянно действующей технической комиссии по защите государственной тайны и Совета по вопросам

технической защиты информации в Ханты-Мансийском автономном округе – Югре и настоящим Положением.

1.5. 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 защиты информации в Ханты-Мансийском автономном округе - Югре, являющиеся координирующими органами защиты информации в Ханты- Мансийском автономном округе – Югре.

1.6. Ответственность за организацию деятельности ПДТК по ЗИ возлагается на директора Учреждения.

2. Основные функции ПДТК по ЗИ

2.1. Изучает все стороны деятельности Учреждения в области защиты информации.

2.2. Вырабатывает рекомендации руководству Учреждения, направленные на обеспечение решения следующих вопросов:

- надежное и эффективное управление системой защиты информации в Учреждении;

- разработку проектов локальных нормативных документов Учреждения 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;

- изучение и анализ возможностей иностранных технических разведок с учетом полномочий Учреждения и оперативной обстановки, определение видов и средств разведки, которым необходимо осуществлять противодействие;

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

- организации и координации работ по технической защите информации;

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

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

2.4. Проводит классификацию информационных систем в Учреждении.

2.5. Осуществляет контроль и координацию работ по обеспечению безопасности общедоступной информации в соответствии с требованиями Указа Президента Российской Федерации от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена», приказа Министерства связи и массовых коммуникаций Российской Федерации от 25.08.2009 № 104 «Об утверждении Требований по обеспечению целостности, устойчивости функционирования и безопасности информационных систем общего пользования» и совместного приказа ФСБ России и ФСТЭК России от 31.08.2010 № 416/489 «Об утверждении Требований о защите информации, содержащихся в информационных системах общего пользования».

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

2.7. Осуществляет в соответствии с требованиями Межведомственной комиссии по защите государственной тайны от 24.01.2012 № 225 «Рекомендациями по проведению экспертизы материалов, предназначенных к открытому опубликованию» одобренных решением Межведомственной комиссии по защите государственной тайны, Федеральным законом от 27.07. 2006 г. № 149-ФЗ «Об информации,

информационных технологиях и о защите информации» экспертизу материалов, предназначенных для открытого опубликования.

3. Состав и порядок работы ПДТК по ЗИ

3.1. Численность и персональный состав ПДТК по ЗИ определяется локальным нормативным актом Учреждения.

В состав ПДТК по ЗИ могут включаться:

- руководители структурных подразделений Учреждения, работники которых непосредственно обрабатывают информацию ограниченного доступа;

- должностные лица, назначенное ответственным за обработку персональных данных и обеспечение безопасности конфиденциальной информации в Учреждении (структурном подразделении Учреждения);

- руководитель структурного подразделения по защите информации в Учреждении (административный отдел).

Состав комиссии формируется из числа должностных лиц, согласно Приложения к настоящему Положению и утверждается локальным нормативным актом Учреждения, перед заседанием Комиссии.

3.2. Председателем ПДТК по ЗИ назначается заместитель директора - ответственный за руководство работами по обеспечению безопасности конфиденциальной информации в Учреждении.

3.3. Председатель ПДТК по ЗИ несет ответственность за планирование и организацию работы Комиссии.

3.4. Из членов ПДТК по ЗИ назначается заместитель (заместители) председателя Комиссии и секретарь Комиссии.

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

3.6. Деятельность ПДТК по ЗИ организуется и проводится в соответствии с планом работы Комиссии на календарный год.

3.7. План работы ПДТК по ЗИ формируется под руководством председателя (заместителя председателя) Комиссии и утверждается директором Учреждения.

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

3.8. Заседания ПДТК по ЗИ проводятся не реже одного раза, в полгода. При необходимости на заседания Комиссии могут приглашаться специалисты (консультанты, эксперты) из числа работников или иных лиц, компетентных в рассматриваемых на заседаниях Комиссии вопросах.

3.9. 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.

3.10. Материалы к обсуждению на заседаниях ПДТК по ЗИ готовятся секретарем или по его поручению иными специалистами административного отдела.

3.11. По результатам заседаний ПДТК по ЗИ секретарем оформляются протоколы, которые подписываются председателем (заместителем председателя) и секретарем Комиссии.

3.12. ПДТК по ЗИ правомочна принимать решения при присутствии на заседании не менее 2/3 ее состава.

3.13. Решение считается принятым при голосовании за него большинством голосов членов комиссии присутствующих на заседании, путем открытого голосования.

3.14. При равенстве голосов решающим является голос председателя комиссии, который голосует последним.

3.15. В случае несогласия с принятым решением члены комиссии вправе отразить в протоколе особое мнение.

3.16. Члены ПДТК по ЗИ имеет право:

- знакомиться в установленном порядке с документами и материалами, необходимыми для выполнения возложенных на нее задач;

- 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;

- вносить директору Учреждения предложения об отмене, внесении изменений в локальные нормативные акты Учреждения, противоречащих законодательным и иным нормативным правовым актам, по вопросам, отнесенным к компетенции ПДТК по ЗИ;

- рассматривать проекты локальных нормативных актов Учреждения по вопросам защиты информации ограниченного доступа.

4. Контроль за работой ПДТК по ЗИ

4.1. ПДТК по ЗИ подотчетна директору Учреждения.

4.2. Председатель ПДТК по ЗИ периодически, но не реже одного раза в год, заслушивается директором Учреждения об итоге работы Комиссии и реализации ее предложений и рекомендаций.

Приложение к Положению о постоянно
Действующей технической комиссии по защите
информации в бюджетном учреждении
Ханты-Мансийского автономного округа – Югры
«Центр имущественных отношений»

Перечень должностей, работников бюджетного учреждения Ханты-Мансийского автономного округа – Югры «Центр имущественных отношений», для формирования состава постоянно действующей технической комиссии по защите информации в бюджетном учреждении Ханты-Мансийского автономного округа – Югры «Центр имущественных отношений»

Председатель комиссии: Заместитель директора

Члены комиссии:

Начальник административного отдела,

Начальник отдела делопроизводства и кадровой работы;

Главный бухгалтер;

Начальник отдела инвентаризации и обеспечения совершения сделок с имуществом;

Начальник отдела планирования и размещения закупок;

Начальник отдела обеспечения сохранности и государственного учета документов;

Начальник отдела сбора и систематизации сведений для государственной кадастровой оценки;

Начальник отдела актуализации кадастровой стоимости;

Начальник отдела определения кадастровой стоимости;

Начальник отдела кадастровых работ, развития и сопровождения геоинформационных систем;

Начальник юридического отдела.

Приложение 12
к приказу бюджетного учреждения
Ханты-Мансийского автономного округа – Югры
«Центр имущественных отношений»
№ 13/01-П-85 от «27» июня 2023 г.

Порядок использования паролей в автоматизированных системах бюджетного учреждения Ханты-Мансийского автономного округа - Югры «Центр имущественных отношений» (далее – Порядок)

1. Термины и сокращения

1.1. Для целей настоящего документа использованы термины:

Автоматизированная система - система, состоящая из работников и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Аутентификация - проверка принадлежности субъекту доступа предъявленного им идентификатора и установление (подтверждение) его подлинности.

Доступ к информации (доступ) - ознакомление с информацией, её обработка, в частности, копирование, модификация или уничтожение информации.

Доступность (санкционированная доступность) информации - состояние информации, характеризуемое способностью технических средств и информационных технологий обеспечивать беспрепятственный доступ к информации субъектов, имеющих на то полномочия.

Идентификация - присвоение субъектам и объектам доступа личного идентификатора (имени, названия) или проверка его соответствия одному из значений в заданном для системы перечне идентификаторов.

Информационные ресурсы - отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках и базах данных, других информационных системах).

Защита от несанкционированного доступа - предотвращение или существенное затруднение несанкционированного доступа к информации.

Компрометация (для целей данного документа):

а) разглашение парольной информации;

б) безвозвратная или долговременная утеря аппаратного идентификатора.

Несанкционированный доступ к информации - доступ к информации или действия с ней, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых автоматизированными системами.

Пароль - набор символов, который используется в качестве кода доступа к автоматизированной системе, программе или информационному ресурсу; наиболее распространённое средство аутентификации субъектов доступа.

Правила разграничения доступа - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Объект доступа - единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

Субъекты доступа - лицо или процесс, действия которого регламентируются правилами разграничения доступа.

1.2. Используемые в тексте сокращения:

Сокращение	Термин
АИБ	администратор информационной безопасности
АС	автоматизированная система
АРМ	автоматизированное рабочее место

ГМД	гибкий магнитный диск
ИС	информационная система
ЛВС	локальная вычислительная сеть
НСД	несанкционированный доступ к информации
ОС	операционная система
ПО	программное обеспечение
ПРД	правила разграничения доступа
ПЭВМ	персональная электронно-вычислительная машина
РСД	разрешительная система допуска (к документам и сведениям)
СВТ	средство (средства) вычислительной техники
СЗИ	система защиты информации

2. Общие положения

2.1. Порядок представляет с собой набор правил, которыми необходимо руководствоваться всем работникам бюджетного учреждения Ханты-Мансийского автономного округа – Югры «Центр имущественных отношений» (далее – Учреждения) при защите с помощью паролей информации, обрабатываемой в автоматизированных системах Учреждения.

2.2. Целями Порядка являются:

- создание и неуклонное применение комплекса организационных мер, программных и технических средств защиты, применяемых при создании, использовании, уничтожении парольной информации;

- контроль за выполнением различными категориями пользователей мер по применению и безопасности парольной информации.

2.3. Доступ к информационным ресурсам, размещённым в АС Учреждения, должен быть авторизованным.

2.4. С целью предотвращения несанкционированного доступа к информационным ресурсам, размещенным в АС, а также его разграничения в Учреждении установлена единая система паролирования.

2.5. Единая система паролирования предусматривает, что доступ к информационным ресурсам АС для всех пользователей возможен только через установленные процедуры идентификации и аутентификации.

2.6. Организационное и техническое обеспечение процессов создания, использования, смены и прекращения действия паролей и контроль за работой пользователей с паролями в АС Учреждения возлагается на администратора информационной безопасности.

2.7. Ознакомление с требованиями настоящего Порядка и инструктирование по правилам использования паролей всех работников, допущенных к информационным ресурсам Учреждения, проводит администратор информационной безопасности, о чём делается запись в специальном заведённом журнале. При ознакомлении с настоящим Порядком работник Учреждения должен быть предупреждён об ответственности за нарушение правил использования паролей, в первую очередь за добровольное разглашение парольной информации.

2.8. Повторное инструктирование работников Учреждения проводится администратором информационной безопасности при обнаружении грубых нарушений ими правил использования паролей.

2.9. Администратором информационной безопасности инструктирование работников Учреждения осуществляется, в том числе в целях закрепления знаний настоящего Порядка, путем проведения соответствующего обучения (подготовка занятий).

2.10. При вынужденном неисполнении требований настоящего Порядка (в нештатных ситуациях) пользователи АС Учреждения (при необходимости во взаимодействии с администратором информационной безопасности) обязаны принять безотлагательные и достаточные меры к восстановлению установленного режима применения парольной информации. Непринятие таких мер расценивается как грубое должностное нарушение.

2.11. Порядок (или вносимые в него изменения) утверждает директор Учреждения по представлению администратора информационной безопасности. Вносимые изменения не должны противоречить другим положениям Порядка. Изменения Порядка отражаются в Листе регистрации изменений, согласно Приложению, к настоящему Порядку.

3. Требование к составлению и обеспечению безопасности паролей

3.1. В целях авторизации доступа к информационным ресурсам каждому работнику, допущенному к информационным ресурсам АС Учреждения, должно присваиваться пользовательское имя, которое составляется системным администратором и сообщается пользователю.

3.2. Первоначальные пароли формируются системным администратором для разрешения (реализации) первого входа пользователей в АС (доступа к ИР). Первое подключение пользователя к АС (доступ к ИР) осуществляется с паролем, назначенным администратором безопасности АС. Во время процедуры первого входа в сеть пользователь обязан назначить новый пароль с учётом нижеперечисленных требований:

Параметр пароля	Для всех пользователей	Исключения для администра - торов
Минимальная длина пароля (количество символов)	7	10
Максимальная длина пароля (количество символов)	16	32
Наличие в пароле букв верхнего и нижнего регистра (русских, английских)	да	
Наличие в пароле цифр	да	
Наличие в пароле специальных символов (не буквы и не цифры)	да	
Наличие в пароле наборов символов, имеющих значение сведений о реально существующих объектах окружающего мира, а также общепринятых сокращений	нет	

Наличие в пароле сочетаний символов, полученных путём набора на клавиатуре русских слов при английской раскладке клавиатуры, и наоборот	нет	
Наличие в пароле сочетаний из символов, соответствующих клавишам, расположенным в одном горизонтальном или вертикальном ряду клавиатуры	нет	
Наличие в пароле сочетаний из нескольких однообразных или одинаковых символов	нет	
Требование не повторяемости паролей	24 хранимых пароля	
Минимальное отличие нового пароля от предыдущего	6 позиций	
Максимальный срок действия паролей	30 дней	
Минимальный срок действия паролей	1 день	
Пороговое значение блокировки учётной записи при ошибочных вводах паролей	7 ошибок	
Период блокировки учётной записи при ошибочных вводах паролей / сброс счётчика блокировки	15 минут	
Напоминание пользователям ЛВС об окончании срока действия пароля	за 5 дней	

3.3. В целях обеспечения тайны пароля категорически не рекомендуется записывать личный пароль пользователя на доступных другим лицам носителях информации

3.4. Плановая смена паролей проводится до истечения 30 дней от назначения пароля. Предложение пользователю сменить пароль производится операционной системой автоматически заблаговременно за 5 календарных дней до истечения срока действия пароля, в течение которых его необходимо сменить. Сетевое имя пользователя, не сменившего пароль в течение предоставленного ему срока, блокируется сетевыми службами. Снятие блокировки одновременно с принудительной сменой пароля производится администратором АС (по распоряжению начальника его структурного подразделения).

3.5. В случае компрометации его личного (сетевого) пароля пользователем должны быть немедленно приняты меры по смене пароля.

При подозрении на наличие фактов злоупотреблений, связанных с компрометацией личного (сетевого) пароля, пользователь обязан сообщить об этом руководителю своего структурного подразделения, а тот, в свою очередь, администратору информационной безопасности.

3.6. При отсутствии возможности использования действующего пароля пользователь должен обратиться к администратору информационной безопасности (к администратору АС) для принятия мер по восстановлению его прав доступа к ресурсам АС.

3.7. Ответственность за действия в отношении информационных ресурсов несёт пользователь, от чьего имени они производились.

3.8. Допускается хранение резервных копий паролей (на случай утери или забывания пользователями паролей) системных администраторов, администраторов информационных ресурсов и информационной безопасности, а также пользователей АС. Копии должны сдаваться в отдельном опечатанном конверте администратору информационной безопасности Учреждения, который хранит их в специально отведённом сейфе.

3.9. Намеренное разглашение (компрометация) личных паролей, использование не своих или своих, но скомпрометированных, паролей, не допускается и расценивается как грубое должностное нарушение.

3.10. Скомпрометированные пароли должны незамедлительно выводиться из действия путём их смены через установленную процедуру.

3.11. Отдел делопроизводства и кадровой работы обязан документально (например, через обходной лист, выдаваемый сотруднику) информировать администратора информационной безопасности об увольнении или ином изменении кадрового статуса работников Учреждения.

3.12. Учётные записи уволенных работников должны блокироваться, их доступ ко всем информационным ресурсам должен прекращаться.

3.13. Допускается блокировка учётных записей работников Учреждения, длительное время отсутствующих на рабочем месте.

3.14. При прекращении полномочий администратора парольной защиты (системного администратора) должна производиться внеплановая общая смена паролей всех пользователей.

4. Организация и контроль выполнения требований Порядка

4.1. Организация выполнения требований Порядка, контрольных и проверочных мероприятий по вопросам парольной защиты возлагается на администратора информационной безопасности.

4.2. Доведение требований Порядка до работников Учреждения, обеспечение условий и повседневный (текущий) контроль за их выполнением возлагается на руководителей структурных подразделений Учреждения, применяющих СВТ, работники Учреждения которых получают доступ к защищаемым информационным ресурсам Учреждения.

4.3. Ответственность за соблюдение требований Порядка возлагается на всех работников Учреждения, использующих доступ к защищаемым информационным ресурсам Учреждения.

4.4. Проведение периодического контроля за действиями пользователей АС при работе с паролями, соблюдением порядка их смены и использования возлагается на администратора информационной безопасности. О результатах контроля докладывается директору Учреждения.

4.5. Обо всех случаях компрометации паролей пользователи обязаны докладывать руководителю своего структурного подразделения и администратору информационной безопасности для определения причин произошедшего, возможного ущерба от компрометации и принятия мер по устранению угроз информационным ресурсам.

4.6. Злостное нарушение требований Порядка (халатное отношение к ним) должно разбираться (расследоваться) с принятием руководством

Учреждения решения о дальнейшем допуске виновных должностных лиц к защищаемой информации.

Приложение к Порядку использования паролей
в автоматизированных системах
бюджетного учреждения
Ханты-Мансийского автономного округа - Югры
«Центр имущественных отношений»

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Наименование локального нормативного акта	Основание (дата, номер локального нормативного акта)

Приложение 13
к приказу бюджетного учреждения
Ханты-Мансийского автономного округа – Югры
«Центр имущественных отношений»
№ 13/01-П-85 от «27» июня 2023 г.

Порядок защиты компонентов информационных систем в бюджетном учреждении Ханты-Мансийского автономного округа – Югры «Центр имущественных отношений» (далее – Порядок)

1. Термины и сокращения

1.1. Для целей настоящего документа использованы термины:

Автоматизированная система - система, состоящая из работников и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Администратор АС - лицо, ответственное за функционирование автоматизированной системы в установленном штатном режиме работы.

Администратор безопасности информации АС - лицо, ответственное за защиту АС от несанкционированного доступа к информации.

Антивирусная программа (антивирусное программное средство) - программа, предназначенная для противодействия вредоносным программам (компьютерным вирусам).

Антивирусная программа-детектор - программа, позволяющая обнаруживать файлы, поражённые компьютерным вирусом, известным разработчикам антивирусной программы.

Антивирусная программа-доктор - программа, удаляющая программный код компьютерного вируса из объектов, в которых он был

обнаружен, восстанавливая их в том состоянии, в котором они находились до поражения вирусом.

Антивирусная программа-ревизор - программа, записывающая сведения о состоянии файловой системы, а затем периодически сравнивающая текущее её состояние с исходным и сообщающая пользователю об обнаруженных изменениях.

Антивирусная программа-фильтр - программа, находящаяся резидентно в оперативной памяти компьютера, анализирующая обращения программ к операционной системе и определяющая те обращения, которые могут использоваться вирусами.

Антивирусный контроль (в более широком смысле: противостояние вредоносным программам) - комплекс мероприятий, проводимых в целях предотвращения воздействия или ликвидации последствий воздействия вредоносных программ (компьютерных вирусов) на его автоматизированные системы и информационные ресурсы.

Вирусная активность - выявление пользователем путём плановой или внеочередной проверки, а также через посредство оповещений активизированных антивирусных программ наличия вредоносных программ на эксплуатируемой АС, а также признаков их активности.

Вирусная эпидемия - в данном документе: распространение вредоносных программ на два и более компьютера (иных компонентов объекта информатизации Учреждения).

Вредоносная программа (malware) - компьютерная программа или переносной код, предназначенный для реализации угроз информации, хранящейся в компьютерной системе, либо для скрытого нецелевого использования ресурсов компьютерной системы, либо иного воздействия, препятствующего нормальному функционированию автоматизированной системы. К вредоносным программам относятся компьютерные вирусы, трояны, сетевые черви и др. Этот термин может обозначать любое нежелательное программное обеспечение.

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

Информационные ресурсы - отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках и базах данных, других информационных системах).

Инцидент - любое непредвиденное или нежелательное событие, нарушившее штатный режим функционирования информационной системы или какого-либо её компонента.

Компьютерный вирус (программа-вирус) - программа, способная создавать свои копии (необязательно совпадающие с оригиналом) и внедрять их в файлы, системные области компьютера, компьютерных сетей, а также осуществлять иные деструктивные действия. При этом копии сохраняют способность дальнейшего распространения. Компьютерный вирус относится к вредоносным программам.

Пользователь - сотрудник, непосредственно использующий аппаратное и программное обеспечение для выполнения служебных обязанностей.

Рабочее место - персональный компьютер и машинные носители информации, которые используются пользователем при его работе.

1.2. Используемые в тексте сокращения:

Сокращение	Термин
АС	автоматизированная система
БД	база данных
ВП	вредоносная программа
ГМД	гибкий магнитный диск
ИР	информационный ресурс (информационные ресурсы)

ИС	информационная система (информационные системы)
ИТКС	информационно-телекоммуникационная система
ЛВС	локальная вычислительная сеть
МНИ	машинные носители информации
НСД	несанкционированный доступ к информации
ОС	операционная система
ПО	программное обеспечение
ПЭВМ	персональная электронно-вычислительная машина, компьютер
СВТ	средство вычислительной техники
СУБД	система управления базами данных

2. Общие положения

2.1. Порядок определяет общие принципы противодействия вредоносным программам (системой антивирусной защиты), устанавливает единые процедуры и правила выбора методов и средств борьбы с вредоносными программами в информационных системах бюджетного учреждения Ханты-Мансийского автономного округа – Югры «Центр имущественных отношений» (далее – Учреждение).

2.2. Целями функционирования системы антивирусной защиты Учреждения являются:

- сохранение работоспособности информационных систем при воздействии различного рода вредоносных программ;

- защита информации (сведений, данных) от потери конфиденциальности, блокированиядоступа к ней, утраты, модификации, а также от иных неправомерных действий.

2.3. Основополагающими требованиями к системе антивирусной защиты Учреждения являются:

- противодействие вредоносным программам должно осуществляться непрерывно в течение всей работы информационных систем;

- реакция на воздействие (обнаружение) вредоносных программ должна быть немедленной;

- противодействие вредоносным программам должно основываться на предположениях, что они могут быть занесены в информационные системы и о них, их структуре и возможных действиях ничего не известно;

- Учреждение может использовать для противодействия вредоносным программам только лицензионные антивирусные программные средства, имеющие техническую поддержку (сопровождение) производителя, предусматривающие оперативное получение обновлений вирусных баз данных, совместимые с другими применяемыми в налоговом органе программными средствами;

- антивирусные программные средства должны быть настроены на еженедельное автоматическое проведение полных проверок компьютеров пользователей и серверов локальных вычислительных сетей;

- обновление вирусных баз данных антивирусных программных средств пользователей должно производиться с заданной максимально возможной частотой, но не реже 1 раза в 2 рабочих дня;

- установка антивирусных программных средств на компьютерах (автоматизированных системах), настройка их параметров осуществляется системным администратором Учреждения в соответствии с руководящими документами и техническими руководствами по применению конкретных антивирусных средств;

- системный администратор Учреждения обеспечивает непрерывный контроль над всеми возможными путями проникновения вредоносных программ в ИС, мониторинг антивирусной безопасности и обнаружение активности вредоносных программ на всех объектах ИС;

- системный администратор Учреждения проводит анализ, определение степени опасности и предотвращение угроз распространения

(воздействия) вредоносных программ путем выявления уязвимостей используемых в АС ОС, программного обеспечения и сетевых устройств;

- системный администратор Учреждения проводит устранение выявленных угроз распространения (воздействия) вредоносных программ в соответствии с рекомендациями специализированных антивирусных служб и поставщиков антивирусных программ, а также путём установки обновлений, предоставляемых разработчиками общесистемного и прикладного ПО;

- системный администратор организует профилактические мероприятия по предотвращению и ограничению массового поражения вредоносными программами, включающие загрузку и развертывание специальных правил нейтрализации (отражению, изоляции и ликвидации) вредоносных программ на основе рекомендаций по контролю атак, подготавливаемых разработчиком средств защиты от вредоносных программ и другими специализированными экспертными антивирусными службами до того, как будут выпущены файлы исправлений, признаков и антивирусных сигнатур;

- съёмные машинные носители информации, используемые для транспортировки электронных данных или программ, перед применением в составе автоматизированных систем обязательно проверяются пользователями на отсутствие компьютерных вирусов;

- антивирусными программами должны проверяться файлы, заархивированные файлы, входящие и исходящие почтовые сообщения, а также файлы, предназначенные для помещения в архив электронных документов;

- антивирусная программа при обнаружении поражённого объекта должна автоматически препятствовать дальнейшему его использованию, оповещая пользователя (рекомендуется: и администратора) об обнаружении вирусной активности и предлагая ему оптимальные действия

по нейтрализации компьютерного вируса (лечение, при невозможности лечения - удаление) или же проделывая эти действия автоматически.

2.4. Объектом атак, осуществляемых с помощью вредоносных программ, могут быть государственные информационные ресурсы, формируемые в Учреждении при осуществлении его деятельности. Информационные ресурсы сосредотачиваются в Учреждения, в том числе в электронном виде (массивы документов в информационных системах: файлы, электронные архивы, базы и банки данных; общесистемное и специализированное программное обеспечение, управляющее работой аппаратных средств и обеспечивающее обработку электронных данных).

2.5. В Учреждении основными объектами для атак вредоносными программами и в силу этого объектами обязательной антивирусной защиты являются:

- автоматизированные системы, в том числе: локальные вычислительные сети, серверы и рабочие станции локальных вычислительных сетей, серверы почтовых систем, активное коммутационное оборудование ЛВС, отдельные ПЭВМ, переносные ПЭВМ, применяемые как для временного подключения к локальным вычислительным сетям, так и используемые локально;

- общесистемное и прикладное программное обеспечения автоматизированных систем;

- электронные данные, массивы данных (файлы);

- сообщения электронной почты и вложенные в них файлы.

2.6. Предполагаемыми субъектами, способными проводить атаки вредоносными программами, являются:

- работники Учреждения, непреднамеренно вводящие вредоносные программы в автоматизированные системы Учреждения;

- работники Учреждения, при наличии у них соответствующих прав преднамеренно вводящие вредоносные программы в автоматизированные системы Учреждения или отключающие антивирусные средства;

- лица, не являющиеся работниками Учреждения, преднамеренно вводящие вредоносные программы в автоматизированные системы Учреждения посредством несанкционированного доступа к ним;

- преступные группировки или отдельные лица;

- специальные службы иностранных государств.

2.7. Основными направлениями деятельности Учреждения по борьбе с ВП считаются:

- выбор средств и способов противодействия ВП;

- методологическое обеспечение противодействия ВП;

- предотвращение внедрения вредоносных программ в информационные системы;

- выявление и безопасное удаление ВП в случае их внедрения в информационные системы;

- анализ уязвимостей информационных систем со стороны ВП;

- внедрение новых, появляющихся на рынке технологий противодействия вредоносным программам;

- контроль за эффективным использованием работниками антивирусных программных средств.

2.8. В целях повышения устойчивости ИС к воздействию ВП в Учреждении должны предприниматься дополнительные (косвенные) меры:

- регулярная проверка целостности критически важных программ и данных на наличие

«лишних» файлов и признаков несанкционированного внесения изменений в их состав;

- определение (ограничение) состава программного обеспечения, используемого сотрудниками Учреждения в автоматизированных системах;

- применение в информационных системах только программного обеспечения, имеющего лицензию на его использование в Учреждении, а

также дистрибутивов к нему, полученных от производителей программ или с их официальных сайтов;

- ограничение состава доступных пользователям ресурсов сети Интернет только теми, что используются в основной деятельности Учреждения;

- запрет на распространение официальных адресов электронной почты в открытых ресурсах сети Интернет;

- отрицательное отношение к всплывающим сообщениям на Интернет-сайтах («баннерам»), избирательное отношение к сообщениям от неизвестных адресатов и прикреплённым к ним файлам;

- создание системы резервного копирования и восстановления критически важных электронных данных и программ;

- обучение работников правилам противодействия вредоносным программам.

3. Ответственность структурных подразделений.

Обязанности должностных лиц. Осуществление контроля

3.1. Ответственность за ведение антивирусного контроля в структурном подразделении, использующем информационные системы Учреждения, возлагается на руководителя соответствующего подразделения.

3.2. Периодический контроль состояния антивирусной защиты в АС, соблюдения установленного порядка антивирусного контроля работниками структурных подразделений осуществляется администратором информационной безопасности.

3.3. Ответственность за организацию защиты ИС Учреждения от вредоносных программ в структурных подразделениях Учреждения и соблюдение требований настоящего Порядка возлагается на администратора информационной безопасности, который:

- разрабатывает проекты локальных нормативных актов по организации и осуществлению защиты ИС Учреждения от вредоносных программ;

- планирует мероприятия по защите ИС Учреждения от вредоносных программ;

- анализирует состояние защиты ИС Учреждения от вредоносных программ и вносит предложения по её совершенствованию;

- проводит разбирательство инцидентов, нанесших существенный или необратимый ущерб информационным ресурсам Учреждения;

- контролирует соблюдение Порядка структурными подразделениями Учреждения.

3.4. Администратор антивирусных программ (далее - Администратор) назначается из числа работников Учреждения. Функции Администратора могут быть распределены между несколькими работниками административного отдела его начальником.

3.5. В своей деятельности Администратор руководствуется требованиями действующих федеральных законов, общегосударственных и ведомственных руководящих и нормативных документов по защите информации от вредоносных программ и добивается их исполнения пользователями АС.

3.6. Для реализации поставленных задач и возложенных на него функций Администратор обязан:

- сопровождать внедрённые в Учреждении средства защиты информационных ресурсов и АС от вредоносных программ, в том числе получать текущие обновления антивирусных баз и программного обеспечения;

- управлять системой защиты от ВП в течение рабочего времени;

- устанавливать антивирусные программы (комплексы) на компьютеры локальной вычислительной сети и отдельные рабочие станции,

настраивать в программах функции автозагрузки и удалённого администрирования;

- обеспечивать пользователей инструкциями по противодействию вредоносным программам и использованию антивирусных программ;

- вести всеобщий и полный контроль за вирусной активностью и состоянием антивирусной защиты, безотлагательно реагировать на полученные сообщения об угрозах или других инцидентах в локальной вычислительной сети;

- своевременно (до нанесения ущерба) обнаруживать и устранять инциденты;

- инструктировать сотрудников Учреждения о профилактических мерах при угрозе вирусной эпидемии;

- вести учёт инцидентов в Журнале регистрации инцидентов с компьютерными вирусами, по форме согласно Приложения к настоящему Порядку;

- обеспечить хранение статистической информации об инцидентах (вирусной активности);

- оперативно разбираться в причинах инцидентов и докладывать о них начальнику административного отдела;

- осуществлять проверку работоспособности системы защиты от ВП при изменении конфигурации (обновлении) аппаратно-программных средств АС;

- производить первичный (при установке антивирусных программ) инструктаж пользователей о правилах работы с используемыми на их рабочих местах средствами защиты от ВП, в дальнейшем инструктировать пользователей по необходимости (инциденты, нарушение Порядка);

- по поручению начальника административного отдела проводить занятия с персоналом по тематике противодействия ВП;

- производить анализ защищенности АС от ВП, используя специальное программное обеспечение, свои наблюдения и опыт;

- участвовать в служебных проверках по выявлению (выявленным) нарушений установленных требований обеспечения антивирусного контроля в Учреждении.

3.7. Администратору запрещено:

- предоставлять права администрирования антивирусных средств другим лицам без разрешения начальника административного отдела;

- использовать ставшие доступными в ходе исполнения его обязанностей идентификационные данные пользователей (сетевое имя, пароль, ключи и т.п.) для маскирования своих действий;

- выключать антивирусные средства или изменять их базовые настройки без согласования с начальником административного отдела;

- производить действия, приводящие к сбою, остановке, замедлению работы АС, блокированию доступа, потере информации без санкции руководства и предупреждения пользователей;

- нарушать правила эксплуатации аппаратно-программного обеспечения АС;

- корректировать, удалять, подменять журналы аудита вирусной активности.

3.8. Администратор имеет право:

- получать доступ к программным и аппаратным средствам АС пользователей для осуществления мероприятий антивирусного контроля;

- требовать от пользователей АС выполнения требований руководящих документов по защите информации в АС от вредоносных программ;

- осуществлять оперативное вмешательство в работу пользователя при явной угрозе безопасности информации в результате несоблюдения установленной технологии антивирусного контроля и невыполнения требований по информационной безопасности с последующим докладом начальнику административного отдела;

- предлагать начальнику административного отдела меры по совершенствованию антивирусной защиты.

3.9. Администратор несёт ответственность за:

- реализацию системы антивирусной защиты, для противодействия вредоносным программам;

- регулярность и качество проводимых им работ по обеспечению защиты от ВП в соответствии с функциональными обязанностями.

3.10. При выполнении работ на АС пользователь обязан:

- строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами АС, правила работы и порядок регистрации в АС, доступа к информационным ресурсам АС;

- знать и строго выполнять правила работы со средствами антивирусной защиты информации, установленными на его автоматизированном рабочем месте;

- выполнять требования настоящего Порядка;

- немедленно и неукоснительно выполнять предписания администратора антивирусных программ по противодействию вредоносным программам;

- предоставлять своё автоматизированное рабочее место Администратору для антивирусного контроля (по его просьбе);

- приостанавливать работу на АС и безотлагательно сообщать администратору антивирусных программ и руководителю своего подразделения о появлении сообщений (подозрений) о вирусной активности на своём или чужом автоматизированном рабочем месте, а также отклонений от нормы в работе системных и прикладных программных средств, затрудняющих их применение;

- запускать внеочередную проверку ПЭВМ на отсутствие компьютерных вирусов при появлении сообщений о вирусной активности или подозрений на неё;

- анализировать необходимость дальнейшего использования поражённых компьютерными вирусами файлов;

- производить с помощью антивирусных программ лечение (очистку) или удаление поражённых файлов;

- приступать к дальнейшей эксплуатации АС (ПЭВМ), только убедившись в полной ликвидации вирусной активности.

3.11. Пользователю запрещается:

- использовать программное и аппаратное обеспечение АС в неслужебных целях;

- самовольно вносить какие-либо изменения в состав, размещение, конфигурацию аппаратно-программных средств АС или устанавливать дополнительно программные и аппаратные средства;

- выключать или деинсталлировать антивирусные программные средства, установленные на его автоматизированном рабочем месте, самовольно вносить изменения в их настройки;

- использовать на служебном автоматизированном рабочем месте какие-либо сменные машинные носители информации, кроме прошедших проверку на отсутствие компьютерных вирусов и регламентированных технологическим процессом на его рабочем месте;

- продолжать работу на АС, игнорируя сообщения (предупреждения) антивирусных средств о вирусной активности на его автоматизированном рабочем месте;

- использовать в работе на АС заведомо поражённые вредоносными программами сменные машинные носители информации;

- осуществлять рассылку ложных, беспокоящих или угрожающих сообщений.

3.12. Требования Порядка обязательны для исполнения всеми пользователями, которые должны быть предупреждены о возможной ответственности за их нарушение.

4. Управление системой защиты от вредоносных программ

4.1. В связи со значительным количеством ПЭВМ, входящих в её состав, рекомендуемым в локальной вычислительной сети общего назначения является централизованное управление антивирусной защитой.

4.2. Общее руководство защитой от вредоносных программ осуществляет администратор информационной безопасности. Ему подчиняются администраторы антивирусных программ (комплексов), осуществляющие централизованное управление системой защиты от вредоносных программ.

4.3. Централизованное управление системой защиты от вредоносных программ должно реализовывать следующие функции и возможности:

- непрерывность управления системой в течение рабочего времени;

- установка антивирусных программ (комплексов) на компьютеры локальной вычислительной сети, настройка в программах функций автозагрузки при включении компьютеров и удалённого администрирования;

- удалённое (со своего рабочего места) обслуживание администратором всех входящих в его ведение рабочих станций и сетевых серверов, в том числе: настройка политики антивирусной безопасности; запуск проверки объектов защиты на наличие в них компьютерных вирусов; включение или выключение постоянной защиты; централизованное обновление вирусных баз, в том числе (по необходимости) внеплановое; контроль наличия и работоспособности антивирусных программ на рабочих станциях пользователей; запрещение пользователям самим менять какие-либо настройки антивирусных программ;

- всеобщий и полный контроль за вирусной активностью и состоянием антивирусной защиты, получение администратором сообщений об угрозах или других инцидентах в логической сети;

- хранение статистической информации об инцидентах (вирусной активности) и доступ администратора к ней;

- своевременное обнаружение и устранение всех инцидентов с компьютерными вирусами;

- учёт инцидентов с вредоносными программами, нанесших существенный или необратимый ущерб информационным ресурсам Учреждения;

- обеспечение оперативного разбирательства с достоверным определением причин поражения автоматизированных систем и информационных ресурсов вредоносными программами, а также виновных в нанесении им ущерба.

4.4. Система удалённого централизованного управления должна состоять из отдельных программных компонентов:

- клиентской антивирусной программы, то есть антивирусного комплекса для рабочих станций или серверов;

- сервера администрирования;

- консоли администрирования, устанавливаемой на рабочем месте администратора.

4.5. В целях обеспечения возможности ведения расследования инцидентов с компьютерными вирусами, анализа состояния противодействия вредоносным программам и выработки решений по его усовершенствованию система защиты от вредоносных программ должна реализовывать функцию сбора статистики. Источниками статистических данных при этом являются файловые серверы, рабочие станции пользователей, в том числе администраторов системы защиты от вредоносных программ, на которых установлены клиентские антивирусные программы. Получателем статистических данных является сервер администрирования, управляющий базой данных статистики.

4.6. Администраторы антивирусных программ осуществляют ежедневный (в рабочие дни) мониторинг работы антивирусных средств на объектах ЛВС.

4.7. Объектами мониторинга являются:

- клиентские антивирусные программы (их активация, настройки, статистика выявления вредоносных программ);

- сервер администрирования (его работоспособность, размещённая на нём база данных статистики).

4.8. На развёрнутых для работы ПЭВМ, не входящих в общую ЛВС, управление защитой от вредоносных программ осуществляется локально. При этом требования Порядка относятся и к таким (отдельно развёрнутым) ПЭВМ.

4.9. Антивирусный комплекс для защиты электронной почты должен осуществлять:

- автоматическую антивирусную проверку в режиме реального времени всей проходящей через почтовую систему корреспонденции;

- автоматическую антивирусную проверку в режиме реального времени файлов, запрашиваемых пользователями из своих почтовых ящиков;

- антивирусную проверку (полную или выборочную) по команде администратора хранимых на сервере файлов почтового формата, прикреплённых к сообщениям файлов (информации в ящиках пользователей);

- обновление антивирусных баз.

5. Предотвращение атак информационных ресурсов и систем вредоносными программами, реагирование на них и устранение их последствий

5.1. Предотвращение атак на информационные ресурсы и системы является первой из важнейших задач противодействия вредоносным программам. Оно достигается:

- постоянной активностью антивирусных программных средств в работающих автоматизированных системах Учреждения;

- определяемыми собственными инструкциями оптимальными настройками антивирусных программных средств, позволяющими проводить непрерывную и всеобъемлющую проверку обрабатываемой электронной информации;

- контролем со стороны ответственных структурных подразделений за работоспособностью антивирусных программных средств и вирусной активностью в автоматизированных системах;

- своевременным и адекватным реагированием пользователей на извещения о вирусной активности в закреплённых за ними автоматизированных системах;

- ограничением состава используемых в работе с автоматизированными системами съёмных носителей, содержащих информационные массивы (файлы), полученные из внешних источников и обязательной принудительной проверкой таких носителей на наличие вредоносных программ;

- выявлением и устранением угроз поражения информационных ресурсов и автоматизированных систем вредоносными программами;

- оптимальным использованием функции эвристического анализа обрабатываемой на автоматизированных системах информации.

5.2. Основные обязанности по предотвращению атак информационных ресурсов и систем вредоносными программами, реагированию на них и устранению их последствий лежат на пользователях и администраторах антивирусных программ.

5.3. При подозрении на вирусную активность пользователь самостоятельно или (при необходимости) вместе с администратором

антивирусных программ должен провести внеочередную проверку своей рабочей станции на отсутствие компьютерных вирусов.

5.4. При обнаружении вирусной активности на своей ПЭВМ пользователь обязан:

- приостановить работу;

- безотлагательно сообщить об этом руководителю своего подразделения и администратору антивирусных программ;

- запустить внеочередную проверку ПЭВМ на отсутствие компьютерных вирусов, если она непосредственно перед этим не проводилась;

- проанализировать (при необходимости с привлечением администраторов антивирусных программ и прикладных программных средств) необходимость дальнейшего использования поражённых компьютерными вирусами файлов;

- произвести с помощью антивирусных программ лечение (очистку) или уничтожение поражённых файлов;

- убедившись (при необходимости с привлечением администратора антивирусных программ) в полной ликвидации вирусной активности, приступить к дальнейшей эксплуатации ПЭВМ.

5.5. Ликвидация администратором последствий (ущерба) поражения АС или информационных ресурсов вредоносными программами содержит следующие мероприятия:

- сканирование антивирусными программами всех информационных массивов, вероятность поражения которых была определена;

- выявление и анализ в Диспетчере задач ОС Windows подозрительных (нештатных) процессов или программ;

- завершение подозрительных процессов или программ;

- анализ состояния открытых портов;

- при необходимости анализ необходимых ветвей и ключей в реестре ОС Windows и их восстановление;

- поиск инфицированных файлов по имени на основе данных анализа процессов операционной системы и данных анализа реестра;

- лечение (очистка), удаление или замена инфицированных файлов;

- перезагрузка компьютера.

5.6. После выполнения описанных в п. 5.5 настоящего Порядка процедур администратором проводится контрольный анализ процессов, ключей реестра, открытых портов. Если подозрительных процессов не обнаружено, а ключи реестра ОС Windows не изменились, то ликвидацию последствий атак вредоносными программами можно считать успешной, в противном случае указанные процедуры необходимо повторять.

5.7. Учитывая, что ряд современных вредоносных программ (черви, трояны) могут использовать технологии, присущие вирусам, а также устанавливать компоненты, затрудняющие процедуру анализа и обнаружения своих файлов, администратору после перезагрузки компьютера рекомендуется осуществлять полную принудительную проверку компьютера антивирусным средством.

5.8. По фактам обнаружения вирусной активности администратором антивирусных программ проводится разбирательство, целью которого является выявление предположительных источников (отправителей, владельцев, сайтов, носителей и т.п.) поражённых файлов, их типа, характера содержащейся в них информации, групп и наименований вредоносных программ, применённых антивирусных средств. Эти сведения об инцидентах с вредоносными программами заносятся в данные учёта.

5.9. При наличии халатного или злонамеренного характера действий пользователей, приведших к вирусной активности в автоматизированных системах, а также нанесших существенный или необратимый ущерб информационным ресурсам, результаты разбирательства представляются руководству Учреждения для принятия решения.

5.10. Если обнаружена ВП, не поддающаяся лечению применяемыми антивирусными средствами, то поражённый ею файл (файлы) направляется

организации (производителю), с которой заключен договор о технической поддержке антивирусной программы.

Приложение

к Порядку защиты компонентов информационных систем

в бюджетном учреждении

Ханты-Мансийского автономного округа – Югры

«Центр имущественных отношений»

ЖУРНАЛ РЕГИСТРАЦИИ ИНЦИДЕНТОВ С КОМПЬЮТЕРНЫМИ ВИРУСАМИ

№ п/п	Дата и время обнаружения	Содержание события и другие сведения. Результаты анализа регистрационной информации, причина инцидента. Последствия воздействия вредоносных программ.	Решение Администратора антивирусных программ по факту воздействия вредоносных программ, его подпись, дата и время	Меры, принятые ответственным за защиту информации

Приложение 14

к приказу бюджетного учреждения

Ханты-Мансийского автономного округа – Югры

«Центр имущественных отношений»

№ 13/01-П-85 от «27» июня 2023 г.

Инструкция

по установке, модификации, ремонту, техническому обслуживанию и восстановлению работоспособности программного обеспечения и аппаратных средств (далее – Инструкция)

1. Обозначения и сокращения:

ИСПДн - информационная система персональных данных;

СВТ - средства вычислительной техники.

2. Настоящая Инструкция регламентирует проведение любых модификаций и изменений в составе технических средств и программного обеспечения ИСПДн, технического обслуживания и устранения нештатных ситуаций в работе СВТ, входящих в состав ИСПДн.

3. Все изменения конфигурации технических и системных программных средств ИСПДн, ремонт, модификация, а также неконтролируемое со стороны администратора информационной безопасности техническое обслуживание технических средств и систем, входящих в состав ИСПДн, должны производиться только на основании письменных заявок (Приложение к настоящей Инструкции) администратору информационной безопасности. Ответственность за выполнение данного требования несёт работник бюджетного учреждения Ханты-Мансийского автономного округа – Югры «Центр имущественных отношений» (далее – Учреждение), эксплуатирующий данные средства информатизации.

4. При всех вышеуказанных работах на объектах информатизации работниками структурных подразделений Учреждения (или сторонних организаций), занимающихся ремонтом, модификацией программных и аппаратных средств, инженерных коммуникаций, кабельных линий и систем

объекта и выступающих в качестве инициаторов данных действий в соответствии с планом работ либо внепланово, руководитель соответствующего структурного подразделения либо пользователь ИСПДн допускает указанных исполнителей к данным работам только по согласованию с администратором информационной безопасности.

5. Передача СВТ в другое структурное подразделение или в распоряжение другой организации для ремонта или решения иных задач осуществляется только после того, как администратор информационной безопасности снимет средства защиты и предпримет необходимые меры для затирания или резервного копирования (при необходимости) защищаемой информации, которая хранилась на дисках.

6. О факте выполнения всех без исключения, вышеуказанных работ администратором информационной безопасности делается соответствующая отметка в Журнале учета нештатных ситуаций, выполнения профилактических и ремонтных работ на объекте, установки и модификации аппаратных и программных средств ИСПДн, который ведётся в отношении каждой ИСПДн.

Формат записей Журнала учета нештатных ситуаций, выполнения профилактических и ремонтных работ на объекте, установки и модификации аппаратных и программных средств ИСПДн:

N п/п	Дата записи	Краткое описание выполненной работы, основание	Дата и время начала работы	Дата и время окончания работы	ФИО исполнителей работ и их подписи	Подпись администратора информационной безопасности	Примечание
1	2	3	4	5	6	7	8

7. Пользователям и администратору информационной безопасности необходимо знать, что контролю со стороны администратора информационной безопасности и регистрации в журнале подлежат:

- замена (модификация) средств вычислительной техники, входящих в состав ИСПДн в соответствии с техническим паспортом на ИСПДн, в том числе изменения линий локально - вычислительной сети и т.п.;

- замена, изъятие, добавление средств информатизации ИСПДн (средства электронно-вычислительной техники, комплектующие, системы и сети ИСПДн , системы и сети электросвязи, программные средства);

- техническое обслуживание и ремонт СВТ без замены комплектующих и составных частей;

- обновление (замена) на конкретном автоматизированном рабочем месте или сервере программных средств, необходимых для решения определенной задачи (обновление версий, используемых для решения определенной задачи программ);

- изменение местоположения СВТ и вспомогательных средств и систем, указанных в схеме технического паспорта.

После внесения изменений в состав ИСПДн администратором информационной безопасности делается пометка в техническом паспорте на ИСПДн.

Приложение к Инструкции по установке,
модификации, ремонту, техническому
обслуживанию и восстановлению работоспособности
программного обеспечения и аппаратных средств

На имя ответственного за руководство
работами по технической защите информации и
обеспечение безопасности конфиденциальной
информации в бюджетном учреждении
Ханты-Мансийского автономного округа – Югры
«Центр имущественных отношений»

Заявка по установке, модификации, ремонту, техническому обслуживанию и восстановлению работоспособности программного обеспечения и аппаратных средств

Прошу разрешения на установку (модификацию, ремонт, техническое обслуживание, восстановление работоспособности программного обеспечения и аппаратных средств) в помещении №_____структурного подразделения_____
_____

рабочее
место_____
(ФИО)

_____
(должность)

Краткое описание необходимых работ и
обоснование_____

_____

_____

Дата_____20___

_____ _____ _____
(должность) (подпись) (ФИО)

Приложение 15
к приказу бюджетного учреждения
Ханты-Мансийского автономного округа – Югры
«Центр имущественных отношений»
№ 13/01-П-85 от «27» июня 2023 г.

Инструкция
по организации парольной защиты в информационных системах
бюджетного учреждения
Ханты-Мансийского автономного округа – Югры
«Центр имущественных отношений»
(далее – Инструкция)

1. Обозначения и сокращения:

АРМ- автоматизированное рабочее место;

ИСПДн - информационная система персональных данных.

2. Настоящая Инструкция регламентирует организационно-техническое обеспечение процессов смены и прекращения действия паролей в ИСПДн бюджетного учреждения Ханты-Мансийского автономного округа – Югры «Центр имущественных отношений» (далее – Учреждения).

3. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей возлагается на администратора информационной безопасности.

4. Личный пароль должен генерироваться и распределяться централизованно либо выбираться пользователем ИСПДн самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 6 символов;

- в числе символов пароля обязательно должны присутствовать буквы в верхнем или нижнем регистрах, цифры и/или специальные символы (@, #, $, &, *, % и т.п.);

- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

- личный пароль пользователь не имеет права сообщать никому.

5. Администратор информационной безопасности имеет доступ к АРМ ИСПДн только под своей учётной записью и своим паролем.

6. Плановая смена паролей пользователя должна проводиться регулярно, не реже одного раза в 3 месяца.

7. Внеплановая смена личного пароля или удаление учетной записи пользователя в случае прекращения его полномочий (увольнение, переход на другую работу внутри Управления и т.п.) должна производиться немедленно после окончания последнего сеанса работы данного пользователя с системой.

8. В случае компрометации личного пароля пользователя ИСПДн должны быть немедленно предприняты меры в соответствии с пунктом 7 настоящей Инструкции в зависимости от полномочий владельца скомпрометированного пароля.

Приложение 16
к приказу бюджетного учреждения
Ханты-Мансийского автономного округа – Югры
«Центр имущественных отношений»
№ 13/01-П-85 от «27» июня 2023 г.

Инструкция
по проведению антивирусного контроля информационных систем бюджетного учреждения Ханты-Мансийского автономного округа – Югры
«Центр имущественных отношений»
(далее – Инструкция)

1. Обозначения и сокращения

АРМ — автоматизированное рабочее место;

ИСПДн — информационная система персональных данных;

ПДн — персональные данные;

СВТ — средства вычислительной техники.

2. На АРМ ИСПДн запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации на АРМ. К использованию в ИСПДн допускаются только лицензионные антивирусные средства.

3. Администратор информационной безопасности еженедельно осуществляет проверку статистики обновлений вирусных баз, обновляет базу вручную в случае необходимости, контролирует обеспечение проверки жесткого диска на наличие вирусов не реже 1 раза в две недели.

4. Администратор информационной безопасности в случае обнаружения вирусов или сообщения об обнаружении от пользователей

принимает меры по выявлению и уничтожению вредоносных программ и недопущению их дальнейшего распространения. При этом в обязательном порядке устанавливает источник (носитель) заражения для принятия соответствующих мер.

5. Настройка параметров, режимов и функций средств антивирусного контроля осуществляется администратором информационной безопасности в соответствии с руководствами по применению конкретных антивирусных средств.

6. В случае обнаружения не поддающегося лечению вируса, ответственный за обеспечение безопасности ПДн обязан удалить инфицированный файл и проверить работоспособность СВТ. В случае отказа СВТ произвести восстановление соответствующего программного обеспечения.

7. Ответственность за организацию антивирусного контроля в соответствии с требованиями настоящей Инструкции возлагается на руководителя структурного подразделения, эксплуатирующего ИСПДн.

8. Ответственность за проведение мероприятий антивирусного контроля на своих рабочих станциях и соблюдение требований настоящей Инструкции возлагается на всех пользователей ИСПДн.

9. Периодический контроль за состоянием антивирусной защиты в ИСПДн, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции пользователями осуществляется ответственным за организацию обработки персональных данных в бюджетном учреждении Ханты-Мансийского автономного округа – Югры «Центр имущественных отношений».

Приложение 17
к приказу бюджетного учреждения
Ханты-Мансийского автономного округа – Югры
«Центр имущественных отношений»
№ 13/01-П-85 от «27» июня 2023 г.

Инструкция
по работе с инцидентами информационной безопасности в информационных системах бюджетного учреждения Ханты-Мансийского автономного округа – Югры «Центр имущественных отношений»
(далее – Инструкция)

1. Обозначения и сокращения

ИБ – информационная безопасность;

ИСПДн – информационная система персональных данных;

ОРД – информационно-распорядительные документы;

ПДн – персональные данные;

СЗИ – средства защиты информации;

ПО – программное обеспечение.

2. Ответственность за выявление инцидентов ИБ и реагирование на них в бюджетном учреждении Ханты-Мансийского автономного округа – Югры «Центр имущественных отношений» (далее – Учреждение) возлагается на администратора информационной безопасности.

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

4. Администратор информационной безопасности обязан вести журнал учёта инцидентов ИБ (событий, действий, повлекших за собой риски безопасности защищаемой информации и создающие предпосылки к нарушению критериев безопасности информации). К инцидентам ИБ относятся нарушения пользователями положений организационно-распорядительных документов, установленных порядков и технологии работы в ИСПДн, разглашение защищаемой информации и любые действия, направленные на это, не антропогенные инциденты (сбои ПО, стихийные бедствия).

В журнале в свободной форме описывается инцидент с указанием следующих данных:

- даты и времени;

- причин (умышленные и неумышленные действия, не антропогенные инциденты и т.п.) и описания инцидента и задействованных лиц;

- информации о последствиях;

- информации о возможных последствиях (экономические убытки (в связи с заменой СЗИ, переаттестации; временные и трудозатраты на устранение последствий, нарушение работы пользователей, ущерб субъектам ПДн и юридические последствия для Учреждения и т.п.).

Журнал с данным отчётом об инциденте предоставляется на ознакомление ответственному за организацию обработки персональных данных в Учреждении для принятия мер по предотвращению рецидива (возникновения повторного инцидента).

5. В случае возникновения рецидива со стороны пользователя или администратора информационной безопасности, по ходатайству ответственного за организацию обработки персональных данных директором Учреждения накладывается дисциплинарное взыскание.

6. Сокрытие нарушений и инцидентов ИБ, вызванных любыми должностными лицами Учреждения, является грубым нарушением трудовой дисциплины. Сокрытие нарушений и инцидентов ИБ, вызванных действиями администратора информационной безопасности и ответственным за организацию обработки персональных данных, является грубейшим нарушением дисциплины.

7. 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.

8. Ответственный за организацию обработки персональных данных не может требовать от администратора информационной безопасности действий, направленных на нарушение настоящего руководства и других ОРД Учреждения, требовать сокрытия инцидентов ИБ, вызванных любыми должностными лицами, требовать сообщения ему паролей на СЗИ и нарушения установленного разграничения прав по допуску к информационным ресурсам, установленным матрицей доступа к информационным ресурсам ИСПДн.

Приложение 18
к приказу бюджетного учреждения
Ханты-Мансийского автономного округа – Югры
«Центр имущественных отношений»
№ 13/01-П-85 от «27» июня 2023 г.

Инструкция
по резервному копированию и восстановлению данных
в информационных системах бюджетного учреждения
Ханты-Мансийского автономного округа – Югры
«Центр имущественных отношений»
(далее – Инструкция)

1. Обозначения и сокращения

АРМ - автоматизированное рабочее место;

НСД - несанкционированный доступ;

ПДн - персональные данные.

2. За осуществление резервного копирования баз данных на серверах бюджетного учреждения Ханты-Мансийского автономного округа – Югры «Центр имущественных отношений» (далее – Учреждение) ответственность несет администратор информационной безопасности. Резервное копирование ПДн, хранящихся локально на АРМ пользователей осуществляют пользователи, закрепленные за данным АРМ.

3. Резервное копирование центральной базы данных, расположенной на сервере информационной системы персональных данных, осуществляется еженедельно на сервере в автоматическом режиме стандартными механизмами.

4. Резервное копирование критичных элементов, важных областей и директорий, расположенных на сервере контроллера домена Учреждения, осуществляется ежедневно на логический диск данного сервера в

автоматическом режиме и ежемесячно в ручном режиме на учтенный съемный носитель информации.

5. Резервное копирование ПДн, обрабатываемых локально на АРМ пользователей, осуществляется вручную пользователями на логический диск операционной системы АРМ пользователей с установленной периодичностью один раз в месяц.

6. Мониторинг резервного копирования осуществляется путем просмотра логов копирования данных на сервере, на котором установлена ИСПДн.

7. Регистрация фактов восстановления данных осуществляется в журнале Учета восстановления данных, который ведется для каждой ИСПДн по следующей форме:

Дата резервного копирования данных	**Дата резервного восстановления данных**	**Подпись ответственного лица**
1	2	3

8. Ответственный за организацию обработки персональных данных в Учреждении проверяет правильность ведения журнала и своевременного резервного копирования.

9. Восстанавливать ПДн из резервных копий необходимо в случае утраты/случайного удаления, или выхода из строя накопителя на жестких магнитных дисках АРМ или сервера.

Приложение 19
к приказу бюджетного учреждения
Ханты-Мансийского автономного округа – Югры
«Центр имущественных отношений»
№ 13/01-П-85 от «27» июня 2023 г.

Положение
пользователя по обеспечению безопасности информации в информационных системах бюджетного учреждения Ханты-Мансийского автономного округа – Югры «Центр имущественных отношений» (далее – Положение)

1. Общие положения

1.1. Положение определяет основные обязанности, права и ответственность работника бюджетного учреждения Ханты-Мансийского автономного округа – Югры «Центр имущественных отношений» (далее – Учреждение), эксплуатирующего информационные системы Учреждения (далее - Пользователь), информационные системы обработки информации ограниченного доступа, не содержащих сведений, составляющих государственную тайну, в том числе персональные данные (далее - ИС) Учреждения.

1.2. Пользователем ИС является работник Учреждения, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИС, в соответствии с Перечнем категорий персональных данных и должностей работников Учреждения, замещение которых предусматривает осуществление обработки персональных данных либо осуществление

доступа к персональным данным, обрабатываемых в том числе в информационных системах Учреждения.

1.3. 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.

1.4. Положение обязательно для исполнения всеми пользователями.

Все пользователи должны быть ознакомлены под роспись с настоящим Положением и предупреждены о персональной ответственности за его нарушения.

1.5. 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 Учреждения;

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

- обеспечение необходимого уровня безопасности носителей КИ;

- обеспечение безопасности конфиденциальной информации при ее копировании, размножении;

- резервное копирование, восстановление информации.

1.6. Обозначения и сокращения, применяемые в Положении:

АРМ - автоматизированное рабочее место;

ОТСС - основные технические средства и системы;

НСД - несанкционированный доступ;

СВТ - средства вычислительной техники;

ИСПДн – информационная система персональных данных.

2. Права, обязанности и ответственность пользователей

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

2.2. 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, а также настоящее Положение;

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

располагать ОТСС в соответствии с техническим паспортом;

хранить в тайне свой пароль (пароли), парольную защиту организовывать в соответствии с Инструкцией по организации парольной защиты в информационных системах Учреждения;

выполнять требования Инструкции по проведению антивирусного контроля информационных систем Учреждения;

немедленно вызывать администратора информационной безопасности и ставить в известность руководителя подразделения при подозрении компрометации личных ключей и паролей или при обнаружении фактов совершения в его отсутствие попыток НСД к основным техническим средствам и ИС;

в случае появления у пользователя сведений или подозрений о фактах нарушения настоящего Положения, а в особенности о фактах или попытках НСД к информации, обрабатываемой в ИС, пользователь должен немедленно сообщить об этом администратору информационной 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 должностные обязанности (служебные задания);

при отсутствии необходимости работы выключить (блокировать) компьютер;

при работе в ИС использовать только учтенные съемные носители информации, 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 информационной 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 по установке, модификации, ремонту, техническому обслуживанию и восстановлению работоспособности программного обеспечения и аппаратных средств;

сохранность оборудования и физической целостности системных блоков компьютеров;

блокировать свою учетную запись в случае кратковременного оставления АРМ (нажатием клавиш Windows+L);

обязательно выключать компьютер после завершения работы.

2.3 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 информационной 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 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.

2.4. Права пользователя:

участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения информационной безопасности, НСД, утраты, порчи защищаемой информации и технических компонентов РТС, 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.

2.5. Ответственность Пользователя:

Пользователь несет персональную ответственность за соблюдение установленных требований во время работы. Пользователь, виновный 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 Российской Федерации;

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
Подготовка к обработке информации		
1	Получение допуска к работе	Допуск работников Учреждения к ИС осуществляется в соответствии с Перечнем категорий персональных данных и должностей работников Учреждения, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным, обрабатываемых в том числе в информационных системах Учреждения 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 6 символов.
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 со съемных носителей информации.
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.
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 АРМ ИС, регистрация и контроль доступа к ним осуществляется средствами защиты информации.
3	Передача носителей информации и распечатанных документов	В соответствии с требованиями локальными нормативными актами Учреждения
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 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.

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

Печать производится на принтере, входящем в состав ОТСС ИС.

Размножение (копирование) документов, содержащих информацию ограниченного доступа, осуществляется только на принтерах, многофункциональных устройствах, входящих в состав аттестованного

АРМ или на аттестованном средстве изготовления и размножения документов (копир) Учреждения.

Приложение 20
к приказу бюджетного учреждения
Ханты-Мансийского автономного округа – Югры
«Центр имущественных отношений»
№ 13/01-П-85 от «27» июня 2023 г.

Положение
об организации и проведении работ по обеспечению безопасности персональных данных при их обработке в информационных системах бюджетного учреждения Ханты-Мансийского автономного округа – Югры «Центр имущественных отношений»
(далее - Положение)

1. Общие положения

1.1. Настоящее Положение об организации и проведении работ по обеспечению безопасности персональных данных при их обработке в информационных системах бюджетного учреждения Ханты-Мансийского автономного округа – Югры «Центр имущественных отношений» (далее – Учреждение, Оператор) определяет основные требования к порядку создания системы защиты персональных данных (далее - СЗ ПДН), в целях обеспечения безопасности персональных данных (далее - ПДн) при их обработке в информационных системах персональных данных с использованием средств автоматизации и без использования таковых.

1.2. Персональными данными является любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Специальные категории персональных данных определяются Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» (далее – Федеральный закон «О персональных данных»).

1.3. Понятия, используемые в настоящем Положении:

Безопасность персональных данных - состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Вирус (компьютерный, программный) исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Вспомогательные технические средства и системы - технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные, системы персональных данных.

Защищаемая информация - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационная система персональных данных информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Контролируемая зона - пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Межсетевой экран - локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Недекларированные возможности функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) - доступ к информации или действия с информацией, нарушающие правила

разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных,

Оператор - организация, организующая и (или) осуществляющая обработку персональных данных, а также определяющая цели и содержание обработки персональных данных.

Перехват (информации) неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Побочные электромагнитные излучения и наводки электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Пользователь информационной системы персональных данных - лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа - совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка - код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) блокировать аппаратные средства.

Программное (программно-математическое) воздействие - несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Ресурс информационной системы - именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Средства вычислительной техники - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) - лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технический канал утечки информации - совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми

добывается защищаемая информация.

Угрозы безопасности персональных данных - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Утечка (защищаемой) информации по техническим каналам - неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уполномоченное оператором лицо - лицо, которому на основании договора оператор поручает обработку персональных данных.

Целостность информации - способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

2. Система защиты персональных данных

2.1. Обеспечение безопасности ПДн осуществляется путем выполнения комплекса организационных и технических мероприятий, реализуемых в рамках создаваемой системы защиты персональных данных (далее - СЗ ПДн), которая включает в себя организационные меры и технические средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки ПДн), а также используемые в информационной системе информационные технологии.

2.2. СЗ ПДн строится следующим образом:

2.2.1. Инвентаризация ресурсов - анализ (аудит) всех эксплуатируемых информационных систем и традиционных хранилищ данных, выявление, где присутствуют и обрабатываются ПДн.

2.2.2. Оценка наличия предусмотренных законом оснований для обработки ПДн, в случаях, когда они отсутствуют - получение согласия субъекта ПДн на их обработку.

2.2.3. Формирование перечня ПДн.

2.2.4. Определение срока обработки ПДн и срока хранения ПДн исходя из сроков требований законодательства Российской Федерации.

2.2.5. Перечень должностей, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным.

2.2.6. Формирование модели угроз ПДн.

2.2.7. Классификация ИС ПДн.

2.2.8. Организация мероприятий по техническому обеспечению безопасности ПДн, обрабатываемых в ИСПД, с обязательной сертификацией (аттестацией) по требованиям безопасности.

2.3. Создание СЗ ПДн включает в себя следующие стадии:

2.3.1. Предпроектная стадия включает в себя:

2.3.1.1. При обследовании ИС ПДн:

устанавливается необходимость обработки ПДн в ИС ПДн;

определяется перечень ПДн, подлежащих защите от несанкционированного доступа;

определяются условия расположения ИС ПДн относительно границ контролируемой зоны (далее - КЗ);

определяются конфигурация и топология ИС ПДн в целом и ее отдельных компонентов, физические, функциональные и технологические связи как внутри этих систем, так и с другими системами различного уровня и назначения;

определяются технические средства и системы, предполагаемые к использованию в разрабатываемой ИС ПДн, условия их расположения, общесистемные и прикладные программные средства, имеющиеся и предлагаемые к разработке;

определяется класс ИС ПДн;

уточняется степень участия персонала в обработке ПДн, характер их взаимодействия между собой;

определяются (уточняются) угрозы безопасности ПДн к конкретным условиям функционирования (разработка частной модели угроз), модели нарушителя.

2.3.1.2. Анализ правовых актов, регламентирующих порядок обработки и защиты ПДн на предмет соответствия требованием нормативных правовых актов, действующих в области безопасности информации.

2.3.1.3. Определение перечня ПДн, подлежащих защите, а также используемых средств защиты ПДн, оценка их соответствия требованиям законодательства Российской Федерации.

2.3.1.4. Определение перечня ИС ПДн, обрабатывающих ПДн.

На данном этапе определяется перечень ИС ПДн и их основные свойства, такие как: структура ИС, подключение к сетям общего доступа, режим обработки ПДн, режим разграничения прав доступа пользователей РТС, местонахождение технических средств информационной системы, характеристики безопасности персональных данных, обрабатываемых в ИС.

2.3.1.5. Определение степени участия работников Учреждения в обработке ПДн, порядка взаимодействия работников между собой.

2.3.1.6. По результатам предпроектного обследования, с учетом установленного класса ИС ПДн задаются конкретные требования по обеспечению безопасности ПДн, включаемые в техническое (частное техническое) задание на разработку СЗ ПДн.

Техническое (частное техническое) задание на разработку СЗ ПДн должно содержать:

обоснование разработки СЗ ПДн;

исходные данные создаваемой (модернизируемой) ИС ПДн в техническом, программном, информационном и организационном аспектах;

класс ИС ПДН;

ссылку на нормативные правовые акты, с учетом которых будет разрабатываться СЗ ПДн и приниматься в эксплуатацию ИСПДн;

конкретизацию мероприятий и требований к СЗ ПДн;

перечень предполагаемых к использованию сертифицированных средств защиты информации.

2.3.2. На стадии проектирования и реализации ИС ПДн, включающей разработку СЗ ПДн в составе ИС ПДн, осуществляется:

2.3.2.1. Производится разработка задания и проекта на строительные, строительно-монтажные работы (или реконструкцию) ИС ПДн в

соответствии с требованиями технического (частного технического) задания на разработку СЗ ПДн.

2.3.2.2. Разработка раздела технического проекта на ИС ПДн в части защиты информации.

2.3.2.3. Строительно-монтажные работы в соответствии с проектной документацией.

2.3.2.4. Использование серийно выпускаемых технических средств обработки, передачи и хранения информации.

2.3.2.5. Разработка мероприятий по защите ПДн в соответствии с предъявляемыми требованиями.

2.3.2.6. Использование сертифицированных технических, программных и программно-технических средств защиты ПДн и их установка.

2.3.2.7. Разработка и реализация разрешительной системы доступа пользователей к обрабатываемой в ИС ПДн информации.

2.3.3. Стадия ввода в действие СЗ ПДн, включает в себя:

2.3.3.1. Выполнение генерации пакета прикладных программ в комплексе с программными средствами защиты информации.

2.3.3.2. Опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИС ПДн и отработки ПДн.

2.3.3.3. Приемо-сдаточные испытания средств защиты информации по результатам опытной эксплуатации.

2.3.3.4. Оценка соответствия ИС ПДн требованиям безопасности ПДн.

3. Порядок проведения классификации информационных систем персональных данных.

3.1. Классификация ИС ПДн проводится в соответствии с утвержденными Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных

информационных системах Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 1 1 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

3.2. Целью классификации ИС ПДн является определение по её результатам перечня организационных и технических мероприятий, позволяющих выполнить требования по обеспечению безопасности ПДн при их обработке в ИС ПДн.

3.3. Результаты классификации ИС ПДн оформляются соответствующим актом классификации, утверждаемым директором Учреждения

3.4. Из всей совокупности обрабатываемой информации комиссией определяются информационные ресурсы, содержащие в себе персональные данные, а также технические средства, позволяющие осуществлять обработку ПДн, к которым относятся: средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных).

3.5. По результатам анализа составляется перечень ИС ПДн, подлежащих, защите, утверждаемый руководителем.

4. Порядок организации и основные мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных

4.1. Под организацией обеспечения безопасности ПДн при их обработке в ИС ПДн понимается осуществление мероприятий, направленных на предотвращение (нейтрализацию) и устранение угроз безопасности ПДн в ИС ПДн, на восстановление нормального функционирования ИС ПДн после нейтрализации угрозы. Обеспечение безопасности ПДн при их обработке в автоматизированных ИС ПДн должно проводиться путем выполнения комплекса организационных и технических мероприятий, в рамках системы (подсистемы) защиты персональных данных.

4.2. Порядок организации обеспечения безопасности ПДн в ИС ПДн должен предусматривать:

4.2.1. Оценку обстановки на основе результатов комплексного обследования ИС ПДн, в ходе которого, прежде всего, проводится определение защищаемой информации и ее категорирование по важности.

При оценке обстановки определяется необходимость обеспечения безопасности ПДн от угроз:

уничтожения, хищения аппаратных средств ИС ПДн носителей информации путем физического доступа к элементам ИС ПДн;

утечки по каналам побочных электромагнитных излучений и наводок (далее - ПЭМИН) перехвата при передаче по проводным (кабельным) линиям связи;

хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (далее - НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий);

воспрепятствования функционированию ИС ПДн путем преднамеренного электромагнитного воздействия на ее элементы;

непреднамеренных действий пользователей и нарушений безопасности функционирования ИС ПДн и СЗ ПДн в ее составе из-за сбоев

в программном обеспечении, а также от угроз не антропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера.

При оценке обстановки должна учитываться степень ущерба, который может быть причинен в случае неправомерного использования соответствующих ПДн.

4.2.2. Обоснование требований по обеспечению безопасности ПДн и формулирование задач защиты ПДн - проводится в соответствии с нормативными и методическими документами уполномоченных федеральных органов исполнительной власти.

4.2.3. Выбор целесообразных способов (мер и средств) защиты ПДн в соответствии с задачами защиты - необходимо определить организационные и технические меры (аппаратные, программные и программно-аппаратные) средства защиты. При выборе технических средств защиты следует использовать сертифицированные средства защиты информации.

4.2.4. Решение вопросов управления обеспечением безопасности ПДн в динамике изменения обстановки и контроля эффективности защиты. К основным вопросам управления относятся:

распределение функций управления доступом к данным и их обработкой между должностными лицами;

определение порядка изменения правил доступа к защищаемой информации и резервируемым информационным и аппаратным ресурсам.

Решение основных вопросов обеспечения защиты ПДн должно предусматривать подготовку кадров, выделение необходимых финансовых и материальных средств, закупку и разработку программного и аппаратного обеспечения.

4.2.5. Планирование мероприятий по защите ПДн.

4.2.6. Организацию и проведение работ по созданию СЗ ПДн в рамках разработки (модернизации) ИС ПДн, в том числе с привлечением специализированных сторонних организаций к разработке и развертыванию СЗ ПДн или ее элементов в ИС ПДн, решение основных задач взаимодействия, определение функций на различных стадиях создания и эксплуатации ИС ПДн.

4.2.7. Разработку документов, регламентирующих вопросы организации обеспечения безопасности ПДн и эксплуатации СЗ ПДн в ИС ПДн.

4.2.8. Ввод в эксплуатацию СЗ ПДн в ИС ПДн.

4.3. Обработка персональных данных без использования средств автоматизации осуществляется в соответствии с постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

4.4. Мероприятия по обеспечению безопасности ПДн реализуются в рамках следующих подсистем СЗ ПДн:

- управления доступом;
- регистрации и учёта;
- обеспечения целостности;
- криптографической защиты;
- антивирусной защиты;
- обнаружения вторжений;
- защиты от утечки за счёт ПЭМИН (для ИС 1 и 2 классов).

Конкретный состав мероприятий по защите ПДн в рамках каждой информационной системы определяется в зависимости от класса ИС ПДн и результатов моделирования угроз, а также результатов обследования ИС ПДн в соответствии с Приказом ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических

мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

4.5. С целью обеспечения возможности незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним в ИС ПДн применяется резервное копирование баз данных.

4.6. С целью защиты ИС ПДн от разрушающего воздействия компьютерных вирусов в Учреждении используются только лицензионные антивирусные средства, имеющие соответствующие сертификаты ФСТЭК России по требованиям безопасности.

4.7. Обязанности по реализации необходимых мероприятий для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также иных неправомерных действий с ними, возлагается на специалиста по информационной безопасности.

4.8. Все магнитные, оптические и другие машинные носители ПДн подлежат обязательному учету. На носители информации наносится маркировка, позволяющая идентифицировать и организовать их учет.

Уничтожение информации с магнитных носителей информации должно осуществляться средствами гарантированного уничтожения информации.

Оператором должна быть организована периодическая проверка наличия, сохранности и соблюдения правил хранения машинных носителей ПДн с оформлением соответствующих актов проверки.

5. Порядок привлечения специализированных организаций к разработке и эксплуатации ИС ПДн и СЗ ПДн.

5.1. Учреждение на основании договора может привлекать организации для формирования и сопровождения баз данных и информационного взаимодействия (центры обработки информации),

выполняющие функции операторов и администраторов системы централизованной обработки данных. В этом случае безопасность ПДн обеспечивает привлекаемая организация. При этом существенным условием договора является обязанность организации обеспечить конфиденциальность ПДн и безопасность ПДн при их обработке в ИС ПДн, а также наличие у такой организации лицензии ФСТЭК России и ФСБ России на:

деятельность по технической защите конфиденциальной информации;

разработку и (или) производство средств защиты конфиденциальной информации (при необходимости);

деятельность по распространению шифровальных (криптографических) средств;

деятельность по техническому обслуживанию шифровальных (криптографических) средств:

предоставление услуг в области шифрования информации.

5.2. Практические аспекты проведения анализа ИС ПДн и построения СЗ ПДн при привлечении специализированных сторонних организаций.

5.2.1. Основные мероприятия необходимые для проведения работ по анализу ИС ПДн:

разработка регламента, устанавливающего порядок и рамки проведения работ по анализу ИС ПДН;

сбор информации об ИС ПДн Учреждения.

5.2.2. Методы сбора исходных данных:

заполнение опросных листов работниками Учреждения;

интервьюирование работников Учреждения, обладающих необходимой информацией;

анализ существующей организационно-технической документации, используемой Учреждением;

использование специализированных программных средств;

инвентаризация сетевых сервисов ИС ПДн;

идентификация и анализ технологических уязвимостей ИС ПДн.

5.2.3. Особенности использования инструментальных средств для сбора информации:

- заранее оговариваются рамки проведения инструментального аудита;

- результаты анализируются и интерпретируются экспертами;

- производится фильтрация полученных данных;

- используется несколько средств анализа защищённости;

- проверка критически важных систем проводится во внерабочие часы, в присутствии администратора с обязательным резервным копированием информации.

5.2.4. Подготовка отчётных материалов:

- итоговый отчёт;

- границы проведения аудита безопасности;

- описание ИС ПДн Учреждения;

- методы и средства проведения аудита;

- результаты классификации ИС ПДн;

- частная модель угроз безопасности ПДн;

- требования по защите персональных данных;

- рекомендации по совершенствованию СЗ ПДн;

- план мероприятий по созданию СЗ ПДн.

5.3. Результаты анализа являются основой для проведения дальнейших работ по повышению информационной безопасности:

совершенствование организационно-правового обеспечения Учреждения;

обучение работников Учреждения.

5.4. Пути минимизации затрат на создание СЗ ПДн (снижения уровня требований):

- максимальное использование возможностей уже имеющихся в ИС средств защиты информации;

- принятие дополнительных мер, позволяющих снизить требования к части ИС ПДн или сегментам сети, где такие ИС ПДн расположены;

- сокращение количества работников Учреждения, обрабатывающих ПДн, разделение функций, минимизирующие возможность одновременной обработки ПДн из разных систем;

- обезличивание части ИС ПДн (переход на абонентские и табельные номера, номера лицевых счетов и т.п.);

- разделение ИС сертифицированными межсетевыми экранами на отдельные сегменты, классификация каждого сегмента и снижения требований к части из них;

- организация терминального доступа к ИС ПДн;

- исключение из ИС ПДн части ПДн, хранение их на бумажных или иных носителях вне ИСПДн.

6. Контроль эффективности защиты ПДн

6.1. Контроль эффективности средств (систем) защиты информации предусматривает инструментальную проверку функционирования технических средств на соответствие установленным требованиям и нормам безопасности. Контроль заключается в проверке выполнения требований нормативных документов по защите информации, а также в оценке обоснованности и эффективности принятых мер. Он может проводиться оператором или на договорной основе сторонними организациями, имеющими лицензии на деятельность по технической защите конфиденциальной информации.

6.2. Контроль СЗ ПДн выполняет функцию обратной связи, позволяющей определить истинное состояние уровня защиты обследуемого

объекта, величину возможного ущерба, вызванного нарушениями требований и норм по защите, а также дает качественную оценку уровню защиты объекта на период проведения проверок (испытаний).

6.3. Проводимые в Учреждении контрольно-проверочные мероприятия должны включать следующие основные мероприятия:

систематическую проверку технического состояния средств, систем и комплексов защиты, а также мер, предотвращающих несанкционированный доступ к ним и нарушение режимов их эксплуатации;

комплексную проверку эффективности системы защиты информации с составлением протоколов (актов);

контроль эффективности защиты объектов информатизации, аттестованных на соответствие требованиям по безопасности информации, включающий проведение объектовых испытаний (специсследования, спецпроверка) организацией, имеющей лицензию на оказание таких услуг и аттестат аккредитации ФСТЭК России.

Приложение 21

к приказу бюджетного учреждения

Ханты-Мансийского автономного округа – Югры

«Центр имущественных отношений»

№ 13/01-П-85 от «27» июня 2023 г.

План мероприятий по обеспечению безопасности информации, обрабатываемой в информационных системах бюджетного учреждения Ханты-Мансийского автономного округа – Югры «Центр имущественных отношений»

№ п/п	Мероприятия	Срок исполнения	Ответственное лицо	Отчетный документ
1	Организация и проведение занятий с сотрудниками Учреждения по изучению законодательства, локальных актов в сфере защиты информации.	Каждое полугодие, не позднее 5 числа месяца следующего за отчетным периодом	Начальник административного отдела Администратор информационной безопасности	Отчет по проведенному занятию, содержащий: - дату проведения занятия; - список присутствующих на занятии сотрудников; - темы, освещенные на занятии.
2	Организация и проведение проверок соблюдения условий обработки информации требованиям законодательства Российской Федерации в области защиты информации.	Каждое полугодие, не позднее 27 числа последнего месяца отчетного периода	Начальник административного отдела Администратор информационной безопасности	Отчет по проверке, содержащий: - дату проведения проверки; - мероприятия, вошедшие в проверку; - результаты проверки.

3	Проверка неизменности состава информационной системы (отсутствия замен основных технических средств и систем в составе информационных систем).	Ежеквартально, не позднее 27 числа последнего месяца отчетного периода	Администратор информационной безопасности	Отчет по проверке, содержащий: - в случае обнаружения изменений, занесение в журнал инцидентов информационной безопасности).
4	Проверка неизменности состава установленного на АРМ пользователей программного обеспечения разрешенного к установке в соответствии с п. 3 Разрешительной системы доступа персонала к сведениям конфиденциального характера в информационной системе.	Ежемесячно, не позднее 25 числа каждого месяца	Администратор информационной безопасности	Отчет (если выявлены изменения), содержащий: - выявленные изменения или их отсутствие (в случае обнаружения изменений, занесение в журнал инцидентов информационной
5	Анализ защищенности информационных системы, в том числе сканирование АРМ ИС	Ежеквартально, не позднее 25 числа последнего месяца	Администратор информационной безопасности	Отчет (если выявлены уязвимости), содержащий: - выявленные уязвимости; - план устранения выявленных уязвимостей.
6	Проверка работоспособности средств защиты информации	Ежемесячно, не позднее 25 числа каждого месяца	Администратор информационной безопасности	Отчет по проверке, содержащий: - выявленные нарушения в работе средств защиты информации или их отсутствие.
7	Выявление инцидентов и событий информационной безопасности.	Постоянно	Администратор информационной безопасности	Журнал инцидентов информационной безопасности

Приложение 22
к приказу бюджетного учреждения
Ханты-Мансийского автономного округа – Югры
«Центр имущественных отношений»
№ 13/01-П-85 от «27» июня 2023 г.

Регламент ответственного за эксплуатацию информационных систем персональных данных бюджетного учреждения Ханты-Мансийского автономного округа – Югры «Центр имущественных отношений» (далее – Регламент)

1. Общие положения

1.1. Настоящий Регламент определяет основные функции, обязанности, права и ответственность ответственного за эксплуатацию информационных систем персональных данных (далее - ИСПДн) бюджетного учреждения Ханты-Мансийского автономного округа – Югры «Центр имущественных отношения» (далее – Учреждение) по вопросам защиты персональных данных (далее - ПДн) в ИСПДн.

1.2. Ответственный за эксплуатацию ИСПДн Учреждения назначается приказом директора.

1.3. Ответственный за эксплуатацию ИСПДн осуществляет контроль за соблюдением порядка работы пользователей ИСПДн, на которых проводится обработка ПДн, дополнительно к своим непосредственным обязанностям.

1.4. Ответственный за эксплуатацию ИСПДн непосредственно подчиняется ответственному за организацию обработки ПДн в Учреждении в части, касающейся защиты ПДн в ИСПДн Учреждения, и осуществляет контроль за выполнением требований локальных нормативных актов по обеспечению безопасности ПДн при их обработке в ИСПДн Учреждения.

2. Основные функции ответственного за эксплуатацию информационной системы персональных данных

1.5. Функции ответственного за эксплуатацию ИСПДн:

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

2.1.2. Ежедневный контроль над отсутствием в период обработки защищаемой информации в помещении, где осуществляется обработка, посторонних лиц, не допущенных к обрабатываемой информации.

1.6. Обязанности ответственного за эксплуатацию ИСПДн:

2.2.1. Знать:

- перечень ПДн, обрабатываемых в ИСПДн Учреждения;
- перечень и состав ИСПДн Учреждения;
- перечень должностей работников Учреждения, доступ которых к ПДн, в том числе обрабатываемым в ИСПДн, необходим для выполнения ими должностных (трудовых) обязанностей;
- условия и технологический процесс обработки ПДн в ИСПДн.

2.2.2. Знать и выполнять требования действующих нормативных и руководящих документов, а также локальных нормативных актов Учреждения, регламентирующих порядок действий по защите ПДн.

2.2.3. Осуществлять внутренний контроль за соблюдением работниками ИСПДн требований законодательства Российской Федерации в области ПДн.

2.2.4. Обеспечивать контроль соблюдения работниками локальных нормативных актов Учреждения, регламентирующих порядок работы с программными, техническими средствами ИСПДн и ПДн, машинными носителями ПДн.

2.2.5. Осуществлять контроль за выполнением работниками ИСПДн мероприятий по защите ПДн в ИСПДн.

2.2.6. Осуществлять контроль за хранением документов, содержащих ПДн, и отсутствием несанкционированного доступа к данным документам, их уничтожение по достижению целей обработки либо контроль процедуры их уничтожения.

2.2.7. Участвовать в определении полномочий пользователей ИСПДн (оформлении разрешительной системы доступа), минимально необходимых для выполнения должностных (трудовых) обязанностей.

2.2.8. При появлении новой должности или исключении существующей должности из списка должностей в ИСПДн, которым необходим доступ к ПДн, своевременно предоставить данные ответственному за организацию обработки ПДн для внесения изменений в перечень должностей в Учреждении, доступ которых к ПДн, в том числе обрабатываемым в ИСПДн, необходим для выполнения ими должностных (трудовых) обязанностей.

2.2.9. Обеспечивать функционирование ИСПДн в пределах, возложенных на него функций.

2.2.10. Своевременно реагировать на попытки несанкционированного доступа к ПДн.

2.2.11. Немедленно сообщить ответственному за организацию обработки ПДн в части, касающейся защиты ПДн, об обнаруженных фактах (попытках) несанкционированного доступа к ПДн и автоматизированным рабочим местам (далее - АРМ), и принимать необходимее меры по пресечению нарушений.

2.2.12. Немедленно прекращать работы на АРМ при несоблюдении установленной технологии обработки информации и невыполнении требований по безопасности ПДн.

2.2.13. Блокировать доступ к ПДн при обнаружении нарушений порядка их обработки.

2.2.14. Осуществлять взаимодействие по обеспечению безопасности ПДн с администратором информационной безопасности ИСПДн и ответственным за организацию обработки ПДн.

2.2.15. 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 вследствие неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения ПДн, а также от иных неправомерных действий в отношении ПДн.

3. Права ответственного за эксплуатацию информационной системы персональных данных

3.1. Ответственный за эксплуатацию ИСПДн имеет право требовать от сотрудников ИСПДн выполнения федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и принятых в соответствии с ним нормативных правовых актов, а также локальных нормативных актов Учреждения в части работы с ПДн.

3.2. Ответственный за эксплуатацию ИСПДн имеет право требовать от пользователей ИСПДн соблюдения установленных технологий обработки информации в соответствии с документом «Описание технологического процесса обработки персональных данных в информационной системе персональных данных» и выполнения инструкций по обеспечению безопасности ПДн в ИСПДн.

3.3. Ответственный за эксплуатацию ИСПДн имеет право инициировать проведение служебных расследований по фактам нарушения требований защиты ПДн, утвержденных соответствующими инструкциями,

несанкционированного доступа, утраты, порчи защищаемых ПДн и технических компонентов ИСПДн.

3.3. Ответственный за эксплуатацию ИСПДн имеет право давать свои предложения по совершенствованию организационных и технических мер защиты ПДн.

3.4. Блокировать доступ к ПДн любых пользователей, если это необходимо для предотвращения нарушения режима защиты ПДн.

3.5. Проводить служебные расследования и опрашивать пользователей по фактам несоблюдения условий хранения носителей ПДн, 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 ПДн.

3.6. Иметь доступ к информации, касающейся обработки ПДн в соответствующей ИСПДн и включающей:

- цели обработки ПДн;
- категории обрабатываемых ПДн;
- категории субъектов, ПДн которых обрабатываются;
- правовые основания обработки ПДн;
- перечень действий с ПДн, общее описание используемых в Учреждении способов обработки ПДн;
- дату начала обработки ПДн;
- срок или условия прекращения обработки ПДн;
- сведения о наличии или об отсутствии трансграничной передачи ПДн в процессе их обработки;
- сведения об обеспечении безопасности ПДн в соответствии с требованиями к защите ПДн, установленными Правительством Российской Федерации.

4. Ответственность ответственного за эксплуатацию информационных

систем персональных данных

4.1. Ответственный за эксплуатацию ИСПДн несет ответственность за свои действия и действия работников вверенной ИСПДн в соответствии с действующим законодательством РФ.

4.2. На ответственного за эксплуатацию ИСПДн возлагается персональная ответственность за качество проводимых им работ в ИСПДн. Ответственный за эксплуатацию ИСПДн несет ответственность в соответствии с действующим законодательством Российской Федерации.

Приложение 23
к приказу бюджетного учреждения
Ханты-Мансийского автономного округа – Югры
«Центр имущественных отношений»
№ 13/01-П-85 от «27» июня 2023 г.

Инструкция о пропускном и внутриобъектовом режимах бюджетного учреждения Ханты-Мансийского автономного округа – Югры «Центр имущественных отношений» (далее – Инструкция)

1. Общие положения

1.1. Инструкция регламентирует условия и порядок осуществления пропускного и внутриобъектового режимов в бюджетном учреждении Ханты-Мансийского автономного округа – Югры «Центр имущественных отношений» (далее – Учреждение), в целях обеспечения предотвращения несанкционированного доступа к персональным данным (далее – ПДн).

1.2. Обеспечение доступа лиц на территорию Учреждения предусматривает комплекс специальных мер, направленных на поддержание и обеспечение установленного порядка деятельности структурных подразделений и определяет порядок пропуска работников Учреждения, сотрудников иных организаций и учреждений и граждан.

1.3. Пропускной режим устанавливается в целях:

– исключения фактов хищений собственности Учреждения;

– исключение фактов вандализма со стороны недобросовестных посетителей;

– исключения возможности несанкционированного доступа работников и посетителей в помещения Учреждения.

1.4. Внутриобъектовый режим устанавливается в целях:

– соблюдения работниками и посетителями правил внутреннего трудового распорядка и пожарной безопасности;

– установления порядка допуска работников в помещения ограниченного доступа Учреждения;

– исключения возможности бесконтрольного передвижения посетителей по территории Учреждения.

1.5. Надёжность пропускного и внутриобъектового режимов достигается:

– осуществлением охраны помещений с помощью охранной сигнализации и видеонаблюдения;

– контролем за состоянием технических средств охраны, который осуществляется частным охранным предприятием на договорной основе;

– контролем электронного пропускного режима (прокси-карты).

1.6. Ответственным за организацию пропускного и внутриобъектового режимов в Учреждении является заместитель директора Учреждения, курирующий административный отдел.

1.7. Ответственным за соблюдение правил внутреннего трудового распорядка, установленного режима функционирования, порядка содержания служебных помещений и мер противопожарной безопасности на объекте является ответственный за организацию обработки ПДн, по курируемому направлению.

1.8. Ответственным за реализацию организационно-технических мероприятий, связанных с осуществлением пропускного и внутриобъектового режимов в Учреждении является администратор информационной безопасности ИСПДн.

2. На территории Учреждения запрещено

2.1. На территории Учреждения запрещается:

– проводить без разрешения руководства фото-, кино-, видеосъемки, в том числе с использованием мобильных телефонов;

– 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 технических средств охраны и пожарной сигнализации;

– заниматься торговой деятельностью;

– вносить химические, взрывчатые и легковоспламеняющиеся вещества и иные предметы и средства, наличие либо применение (использования) которых может представлять угрозу для безопасности окружающих;

– вносить боеприпасы, оружие всех видов и патроны к нему (кроме лиц, которым законодательством Российской Федерации разрешено ношение, хранение и применение оружия для исполнения возложенных на них обязанностей);

– иметь при себе крупногабаритные предметы, в том числе хозяйственные сумки, рюкзаки, вещевые мешки, чемоданы (за исключением папок, портфелей, кейсов для документов).

3. Порядок входа на территорию Учреждения

3.1. Для обеспечения пропускного режима на территорию устанавливаются следующие виды документов:

Заявка на вход на территорию для работы в выходные (праздничные) дни (Таблица 1 к Инструкции);

Заявка на внос (вынос) материальных ценностей на (с) территорию (ии) (Таблица 2 к Инструкции).

3.2. Вход на территорию для работников разрешается с 8:00 до 21:00 в рабочие дни, в субботу с 8:00 до 21:00, воскресенье выходной.

3.3. Вход на территорию работников разрешается с 8:00 до 20:00 в рабочие дни, в субботу с 8:00 до 20:00, в предпраздничные дни на один час короче.

3.4. Вход на территорию разрешается круглосуточно в рабочие, выходные и праздничные дни:

- Директору;
- Первому заместителю;
- Заместителям директора;
- Главному бухгалтеру;
- Руководителям структурных подразделений.

3.5. Вход на территорию для работы в выходные (праздничные) дни осуществляется на основании заявки работника, которая согласовывается с ответственным за реализацию организационно-технических мероприятий. При выполнении строительно-ремонтных работ на территории в заявке обязательно указывается фамилия, имя и отчество, должность, рабочий телефон ответственного должностного лица, который будет присутствовать при проведении этих работ и осуществлять контроль над их проведением.

4. Порядок вноса (выноса) материальных ценностей на (с) территорию (ии) Учреждения

4.1. Внос (вынос) материальных ценностей, замена мебели, оборудования, инвентаря осуществляется на основании заявки по форме, согласно Таблице 2 к настоящей Инструкции, которая подается на имя ответственного за реализацию организационно-технических мероприятий, связанных с осуществлением пропускного режима и сдается на пост охраны после вноса (выноса) указанных в ней материальных ценностей.

4.2. Оформление заявки не требуется на доставку канцелярских товаров, писчей бумаги и иных письменных принадлежностей, товаров хозяйственно-бытового назначения в небольших упаковках.

5. Порядок доставки (отправления) корреспонденции и посылок на территорию Учреждения

5.1. Доставка (отправление) специальной, а также почтовой корреспонденции осуществляется через центральный вход здания.

5.2. Подача заявки на доставку (отправление) специальной, а также почтовой корреспонденции не требуется.

6. Порядок выдачи ключей от служебных помещений Учреждения

6.1. В ведении сотрудника охраны находятся ключи от служебных кабинетов, центрального входа и запасных выходов, электрощитовой.

6.2. Уборка помещений, в которых расположены ИСПДн, осуществляется только в присутствии пользователей ИСПДн.

6.3. Запрещается выдача ключей от служебных кабинетов работникам, не имеющим допуска к ИСПДн.

6.4. Сотрудник охраны перед началом работы пользователя ИСПДн, допущенного к обработке персональных данных в ИСПДн, выдаёт ему ключи от помещения, в котором расположено техническое средство ИСПДн (автоматизированное рабочее место). Факт выдачи ключа фиксируется им в соответствующем журнале и подтверждается личной подписью пользователя ИСПДн.

6.5. В случае утраты ключей от служебного кабинета или по другой причине об этом уведомляется ответственный за реализацию организационно-технических мероприятий, связанных с осуществлением пропускного режима, и выдача дубликата ключа сотрудником охраны производится с его разрешения.

Таблица 1
к Инструкции о пропускном и
внутриобъектовом режимах бюджетного
учреждения Ханты-Мансийского
автономного округа – Югры
«Центр имущественных отношений»

Форма

Директору
_____

З А Я В К А

на вход на территорию бюджетного учреждения Ханты-Мансийского автономного округа – Югры «Центр имущественных отношений» в выходные (праздничные) дни

Прошу Вашего разрешения пропустить меня на территорию ***бюджетного учреждения Ханты-Мансийского автономного округа – Югры «Центр имущественных отношения»*** для работы в выходные (праздничные) дни в связи с
_____
_____
(Обоснование необходимости выполнения работы или наименование мероприятия)

с ___ часов ___ минут «___» _____ 20 __ г. до ___ часов ___ минут «___» _____ 20 __ г.

Должность_____

И.О. Фамилия_____

Подпись_____

« ___ » _____ 20 __ г.

Таблица 2
к Инструкции о пропускном и
внутриобъектовом режимах бюджетного
учреждения Ханты-Мансийского
автономного округа – Югры
«Центр имущественных отношений»
Форма

Директору
_____

З А Я В К А
на внос (вынос) материальных ценностей на (с) территорию (ии)
бюджетного учреждения Ханты-Мансийского автономного округа – Югры
«Центр имущественных отношений»

Прошу разрешить

_____
(полное наименование организации, должность, фамилия, имя, отчество)

внос (вынос) «___» _____ 20 __ г.

в связи _____
(указать цель вноса (выноса)

следующих материальных ценностей:

1._____
(наименование материальных ценностей, серийный номер изделия (если таковой имеется) или инвентарный номер)

Всего в заявку внесено _____ (_____) наименований.

Должность_____
И.О. Фамилия_____
Подпись_____
« ___ » _____ 20 __ г.

Отметка сотрудника охраны

«___»_____ 20__г. в __ час. ___мин. внос (вынос), ввоз (вывоз) осуществлен

_____ _____
(подпись) (расшифровка подписи)

Приложение 24
к приказу бюджетного учреждения
Ханты-Мансийского автономного округа – Югры
«Центр имущественных отношений»
№ 13/01-П-85 от «27» июня 2023 г.

Инструкция по обработке персональных данных без использования средств автоматизации в бюджетном учреждении Ханты-Мансийского автономного округа – Югры «Центр имущественных отношений» (далее – Инструкция)

1. Общие положения

1.1. Персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому гражданину, обратившемуся в бюджетном учреждении Ханты-Мансийского автономного округа – Югры «Центр имущественных отношений» (далее – Учреждение), или работнику (далее – субъекту персональных данных) Учреждения.

1.2. Обработка персональных данных, содержащихся в информационных системах персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

1.3. Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационных системах персональных данных либо были извлечены из нее.

1.4. Правила обработки персональных данных, осуществляемой без использования средств автоматизации, установленные настоящим Положением, должны применяться с учетом требований Постановления Правительства Российской Федерации «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15 сентября 2008 г. № 687, а также требований нормативных правовых актов федеральных органов исполнительной власти.

2. Особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации

2.1. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее – материальные носители), в специальных разделах или на полях форм (бланков).

2.2. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

2.3. Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе работники Учреждения или лица, осуществляющие такую обработку по договору с Учреждением), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется Учреждением без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления

такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти, а также локальными нормативными актами Учреждения.

2.4. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее – типовая форма), должны соблюдаться следующие условия:

– типовая форма или связанные с ней документы должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, наименование и адрес Учреждения, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых Учреждением способов обработки персональных данных;

– типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации,– при необходимости получения письменного согласия на обработку персональных данных;

– типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных.

2.5. При ведении журналов (журналов регистрации, журналов посещений), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных в помещения

Учреждения или в иных аналогичных целях, должны соблюдаться следующие условия:

– необходимость ведения такого журнала должна быть предусмотрена локальным нормативным актом Учреждения, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способах фиксации и составе информации, запрашиваемой у субъектов персональных данных, перечне лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроках обработки персональных данных;

– копирование содержащейся в таких журналах информации не допускается;

– персональные данные каждого субъекта персональных данных могут заноситься в такой журнал не более одного раза в каждом случае пропуска субъекта персональных данных.

2.6. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, зачеркивание, стирание).

2.7. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя – путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

3. Меры по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации

3.1. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

3.2. Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

3.3. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

3.4. Перечень мест хранения материальных носителей ПДн приведен в приложении к настоящей инструкции.

Приложение 25
к приказу бюджетного учреждения
Ханты-Мансийского автономного округа – Югры
«Центр имущественных отношений»
№ 13/01-П-85 от «27» июня 2023 г.

Инструкция по обращению со средствами криптографической защиты информации в бюджетном учреждении Ханты-Мансийского автономного округа – Югры «Центр имущественных отношений» (далее – Инструкция)

1. Общие положения

1.1. Настоящая инструкция регламентирует порядок обращения с шифровальными средствами (средствами криптографической защиты информации, СКЗИ), предназначенными для защиты информации, не содержащей сведений, составляющих государственную тайну, в процессе их получения, транспортировки, учета, хранения, уничтожения, встраивания в прикладные системы, тестирования, а также порядок допуска к работам с шифровальными средствами.

1.2. Перечень должностей, допущенных к работе с СКЗИ, приведен в Таблице 1 к настоящей Инструкции.

1.3. Ответственным за эксплуатацию СКЗИ является ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных (далее - администратор информационной безопасности ИСПДн).

1.4. Работы с СКЗИ должны проводиться с учетом приказа ФСБ от 09.02.2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»

и приказом ФСБ России от 10 июля 2014 года № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности», а также эксплуатационной и технической документации к ним.

2. Ответственные лица

2.1. В бюджетном учреждении Ханты-Мансийского автономного округа – Югры «Центр имущественных отношений» (далее – Учреждении), эксплуатирующей сертифицированные СКЗИ, контроль за обеспечением безопасности при работе с СКЗИ осуществляется администратором информационной безопасности ИСПДн.

2.2. Основные обязанности администратора информационной безопасности ИСПДн:

- обеспечение корректного и безопасного функционирования СКЗИ;
- обеспечение корректной и безопасной эксплуатации СКЗИ;
- ознакомление пользователей с настоящей инструкцией;
- контроль работоспособности и соблюдения правил эксплуатации СКЗИ.

2.3. Основные обязанности пользователей СКЗИ:

- ознакомиться с данной инструкцией под подпись и строго выполнять требования настоящей инструкции в части, их касающейся, а также строго выполнять требования нормативных правовых актов Российской Федерации, относящихся к деятельности с СКЗИ, нормативных и методических документов лицензирующего органа
- соблюдение правил корректной и безопасной эксплуатации СКЗИ;

– обеспечение режима сохранности СКЗИ, ЭТД и ключевых документов, переданных им.

2.4. Администратор информационной безопасности ИСПДн и Пользователи СКЗИ допускаются к работе с СКЗИ только после инструктажа и обучения правилам работы с СКЗИ. Для администратора информационной безопасности ИСПДн инструктаж и обучение проводит Лицензиат. Пользователей инструктирует и обучает администратор информационной безопасности ИСПДн.

3. Требования по размещению, оборудованию и охране помещений

3.1. Размещение, оборудование, охрана и режим в помещениях, в которых проводятся работы с СКЗИ (далее – помещения), должны обеспечивать безопасность СКЗИ, сведение к минимуму возможности неконтролируемого доступа посторонних лиц. Доступ сотрудников в эти помещения должен быть ограничен в соответствии со служебной необходимостью и определяться перечнем должностей, представленном в Таблице 1 к настоящей Инструкции.

3.2. Обеспечения постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода и оборудование помещений пожарной сигнализацией и соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии помещений.

3.3. Помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время. Окна помещений должны быть защищены от НСД посторонних лиц (в случае, если окна на первом этаже, либо рядом с пожарными лестницами) металлическими решетками, а также от визуального просмотра извне окна помещений работ (жалюзи, шторы и т.п.).

4. Порядок обращения с СКЗИ

4.1. Пользователи криптосредств обязаны:

– не разглашать информацию о ключевых документах;

– не допускать вывод ключевых документов на дисплей (монитор) или принтер;

– не допускать установки ключевых документов в другие ПЭВМ.

4.2. Все поступающие СКЗИ, инсталлирующие СКЗИ носители, эксплуатационная и техническая документация (при наличии) к ним должны браться на поэкземплярный учет в «Журнале учета средств криптографической защиты информации». Ведет журналы администратор информационной безопасности ИСПДн.

4.3. Единицей поэкземплярного учета СКЗИ является:

– для аппаратных и программно-аппаратных СКЗИ - конструктивно законченное техническое устройство;

– для программных СКЗИ – инсталлирующий СКЗИ носитель (дискета, компакт-диск (CD-ROM) и т.п.).

4.4. Должны быть приняты организационные меры с целью исключения возможности несанкционированного копирования СКЗИ.

4.5. Хранение съемных машинных носителей должно осуществляется в сейфах (металлических шкафах – при наличии), оборудованных внутренними замками с двумя или более дубликатами ключей и приспособлениями для опечатывания замочных скважин или кодовыми замками. В случае если на съемном машинном носителе хранятся только персональные данные в зашифрованном с использованием СКЗИ виде, допускается хранение таких носителей вне сейфов (металлических шкафов).

4.6. Хранение инсталлирующих СКЗИ носителей допускается в одном хранилище с другими документами при условиях, исключающих непреднамеренное их уничтожение или иное, не предусмотренное правилами пользования СКЗИ применение.

4.7. В случае отсутствия у работника индивидуального хранилища инсталлирующие СКЗИ носители по окончании рабочего дня должны сдаваться администратору информационной безопасности ИСПДн.

4.8. В случае утери носителя СКЗИ или вероятном копировании сотрудник обязан немедленно сообщить об этом администратору информационной безопасности ИСПДн.

4.9. Администратор информационной безопасности ИСПДн должен проводить контроль сохранности и работоспособности установленного СКЗИ, а также всего используемого совместно с СКЗИ программного обеспечения для предотвращения внесения программно-аппаратных закладок и вирусов с периодичностью раз в месяц.

4.10. Используемые СКЗИ должны иметь сертификат соответствия ФСБ и должны быть класса КС1 и выше.

5. Ответственность за нарушение требований Инструкции

5.1. За нарушение требований настоящей Инструкции виновные лица несут дисциплинарную либо материальную ответственность в зависимости от характера нарушения и тяжести наступивших отрицательных последствий.

Таблица 1

к Инструкции по обращению со средствами криптографической защиты информации в бюджетном учреждении Ханты-Мансийского автономного округа – Югры «Центр имущественных отношений»

Перечень должностей, допущенных к работе с СКЗИ

	Должность
1.	Начальник административного отдела
2.	Техник 1 категории (ИТ-специалист) административного отдела
3.	Инженер 1 категории административного отдела

Приложение 26
к приказу бюджетного учреждения
Ханты-Мансийского автономного округа – Югры
«Центр имущественных отношений»
№ 13/01-П-85 от «27» июня 2023 г.

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

1. Общие положения

1.1. Лицами, участвующими в рамках своих функциональных обязанностей в процессах обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным информационных систем персональных данных (далее - ИСПДн) являются работники бюджетного учреждения Ханты-Мансийского автономного округа – Югры «Центр имущественных отношений» (далее – Учреждение) в соответствии с утвержденным Перечнем должностей в Учреждении, доступ которых к персональным данным, в том числе обрабатываемым в ИСПДн, необходим для выполнения ими должностных (трудовых) обязанностей (далее - Пользователи).

1.2. Пользователи должны принимать все необходимые меры по защите персональных данных (далее - ПДн) и контролю за соблюдением прав доступа к ней.

1.3. Пользователи ИСПДн в своих должностных (трудовых) обязанностях обязаны руководствоваться настоящей Инструкцией и должны быть ознакомлены под роспись с настоящим документом и предупреждены об индивидуальной ответственности за его нарушение.

1.4. Основными задачами при обработке ПДн в ИСПДн являются:

– обеспечение исполнения требований нормативных правовых актов, руководящих документов, регламентирующих защиту ПДн в Российской Федерации в процессе создания, хранения, передачи и удаления документов, содержащих ПДн в ИСПДн Учреждения;

– обеспечение в ИСПДн необходимого уровня безопасности обработки, хранения и передачи ПДн;

– обеспечение необходимого уровня безопасности носителей ПДн;

– обеспечение безопасности ПДн при ее копировании, размножении.

2. Обязанности лиц, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими должностных (трудовых) обязанностей

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

2.2. Каждый пользователь ИСПДн, имеющий доступ к автоматизированному рабочему месту (далее - АРМ), программному обеспечению (далее - ПО) и данным ИСПДн, несет персональную ответственность за свои действия и обязан:

– строго соблюдать установленные правила обеспечения безопасности ПДн при работе с программными и техническими средствами ИСПДн, в том числе положения настоящих Правил;

– знать и строго выполнять правила работы со средствами защиты информации, установленными на АРМ;

– при работе в ИСПДн выполнять только те обязанности, которые прописаны в должностной инструкции;

– не разглашать известные им ПДн лицам, не имеющим допуска к этим ПДн;

– располагать во время работы экран монитора в помещении так, чтобы исключалась возможность ознакомления с отображаемой на нем информацией посторонними лицами, и основные технические средства, и системы (далее – ОТСС) в соответствии с Техническим паспортом на ИСПДн;

– помнить свой идентификатор и пароль;

– держать свой пароль в тайне, а именно не сообщать, не разглашать и любым другим способом не доводить до чьего-либо сведения (в том числе других работников Учреждения, в т.ч. руководителей) личный пароль;

– осуществлять ввод пароля только в условиях, исключающих его просмотр;

– не хранить записки-памятки с личным паролем на видном и/или в легко доступном месте: на столе, на мониторе, под клавиатурой, в верхнем ящике стола и т.п.;

– своевременно сообщать ответственному за обеспечение безопасности ПДн в ИСПДн (далее - администратор информационной безопасности ИСПДн) о фактах компрометации пароля (когда пароль стал или может быть известен ещё кому - либо кроме его владельца), об утере или повреждении аппаратного идентификатора и в этих случаях не использовать ИСПДн до специального разрешения администратора информационной безопасности ИСПДн;

– немедленно известить администратора информационной безопасности ИСПДн в случае утери электронного идентификатора или при подозрении компрометации личных ключей и паролей, а также при обнаружении:

а) несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации АРМ;

б) 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;

в) некорректного функционирования установленных на АРМ технических средств защиты;

г) непредусмотренных отводов кабелей и подключенных устройств.

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

– при работе со съемными машинными носителями ПДн 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 в ИСПДн;

– выполнять требования Инструкции по организации антивирусной защиты в ИСПДн в полном объеме;

– осуществлять установленным порядком уничтожение ПДн с машинных носителей ПДн (с помощью средства защиты информации от несанкционированного доступа (далее - НСД));

– немедленно выполнять предписания администратора информационной безопасности ИСПДн в части обеспечения безопасности ПДн;

– соблюдать установленный режим разграничения доступа к информационным ресурсам;

– все изменения конфигурации технических и программных средств ИСПДн, ремонт, модификация и техническое обслуживание технических средств и систем, входящих в состав ИСПДн, производить только по согласованию с администратором информационной безопасности ИСПДн;

– обеспечить сохранность оборудования и физической целостности системных блоков компьютеров;

– при отсутствии необходимости работы компьютера выключить (блокировать нажатием клавиш Windows+L) его.

3. Права лиц, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими должностных (трудовых) обязанностей

3.1. Пользователь ИСПДн имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн. При этом для обработки, хранения и транспортировки ПДн разрешается использовать в ИСПДн только те машинные носители ПДн, которые учтены в «Журнале учета машинных носителей персональных данных».

3.2. Пользователь ИСПДн имеет право участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения информационной безопасности, НСД, утраты, порчи ПДн и технических компонентов ИСПДн, если данное нарушение произошло под его идентификационными данными.

3.3. Своевременно получать доступ к информационным ресурсам ИСПДн, необходимым ему для выполнения своих должностных обязанностей.

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

4. Лицам, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими должностных (трудовых) обязанностей, запрещается

4.1. Пользователю ИСПДн категорически запрещается:

– самостоятельно устанавливать, тиражировать или модифицировать ПО, изменять установленный алгоритм функционирования технических и программных средств, устанавливать или удалять установленные администратором информационной безопасности ИСПДн сетевые программы на компьютерах, вскрывать компьютер, сетевое и периферийное оборудование, подключать к компьютеру дополнительное оборудование;

– запускать любые системные или прикладные программы, не входящие в состав ПО;

– 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 ПО АРМ;

– записывать и хранить ПДн на неучтенных машинных носителях ПДн (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 свой электронный идентификатор, машинные носители ПДн и распечатки, содержащие ПДн;

– умышленно использовать недокументированные свойства и ошибки в ПО или в настройках средств защиты ПДн;

– размещать средства ИСПДн так, чтобы с них существовала возможность визуального считывания информации, содержащей ПДн;

– осуществлять попытки НСД 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;

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

– отключать (блокировать) средства защиты информации;

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

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

– выполнять работы с документами, содержащими ПДн, на дому, выносить их за пределы контролируемой зоны;

– вводить в ОТСС ПДн под диктовку или с микрофона;

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

– передавать свои учетные носители кому-либо;

– запускать файлы-вложения, которые содержатся в спам-письмах.

5. Действия при обнаружении попыток несанкционированного доступа

5.1. К попыткам НСД 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 ПДн;

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

5.2. При выявлении факта несанкционированного доступа (далее - НСД) лицо, выявившее факт НСД (пользователь, ответственный за организацию обработки ПДн, ответственный за эксплуатацию ИСПДн, администратор информационной безопасности ИСПДн) обязан:

– законными способами прекратить НСД к ПДн;

– известить администратора информационной безопасности ИСПДн о факте НСД;

– известить руководителя пользователя, от имени учетной записи которого была осуществлена попытка НСД, о факте НСД;

– известить директора Учреждения.

6. Порядок модификации конфигураций технических и программных средств ИСПДн

6.1. Право внесения изменений в конфигурацию аппаратно-программных средств защиты ИСПДн предоставляется администратору информационной безопасности ИСПДн:

– в отношении системных и прикладных программных средств - по согласованию (в случае, если проводилась аттестация) с аттестационной комиссией, проводившей аттестацию данной ИСПДн;

– в отношении аппаратных средств, а также в отношении программно-аппаратных средств защиты - по согласованию (в случае, если

проводилась аттестация) с аттестационной комиссией, проводившей аттестацию данной ИСПДн.

6.2. Изменение конфигурации аппаратно-программных средств ИСПДн кем-либо, кроме вышеперечисленного уполномоченного работника, запрещено.

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

6.4. 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).

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

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

6.7. После чего заявка передается администратору информационной безопасности ИСПДн для непосредственного исполнения работ по внесению изменений в конфигурацию компьютера, указанного в заявке ИСПДн.

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

6.9. Установка и обновление ПО (системного, тестового и т.д.) на компьютерах производится только с оригинальных лицензионных дистрибутивных носителей, полученных установленным порядком, прикладного ПО - с эталонных копий программных средств, полученных из архива дистрибутивов установленного ПО.

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

6.12. После установки (обновления) ПО, администратор информационной безопасности ИСПДн должен произвести требуемые настройки средств управления доступом к компонентам компьютера и проверить работоспособность ПО, правильность их настройки и произвести соответствующую запись в «Журнале учета выполнения профилактических

работ, установки и модификации программных средств на компьютерах ИСПДн», делает отметку о выполнении (на обратной стороне заявки) и в Техническом паспорте на ИСПДн.

6.13. При возникновении ситуаций, требующих передачи технических средств в сервисный центр с целью ремонта, ответственный за эксплуатацию ИСПДн докладывает об этом администратору информационной безопасности ИСПДн, который в свою очередь связывается с аттестационной комиссией (в случае, если проводилась аттестация) и в дальнейшем действует согласно их инструкциям. В данном случае администратор информационной безопасности ИСПДн обязан предпринять необходимые меры для удаления ПДн с помощью средства защиты информации от НСД, которые хранились на компьютере. 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 выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн» у администратор информационной безопасности ИСПДн для:

– восстановления конфигурации ИСПДн после аварий;

– контроля правомерности установки на ИСПДн средств для решения соответствующих задач при разборе конфликтных ситуаций;

– проверки правильности установки и настройки средств защиты информации, факта уничтожения ПДн, находившихся на компьютере, который оформляется актом и подписывается администратором информационной безопасности ИСПДн и ответственным за эксплуатацию ИСПДн.

7. Порядок учета, хранения и выдачи машинных носителей персональных данных

7.1. Порядок хранения и учета машинных носителей ПДн:

– машинные носители, содержащие ПДн, подлежат обязательному учёту администратором информационной безопасности ИСПДн. Учёт осуществляется с помощью «Журнала учёта машинных носителей ПДн»;

– учёт машинных носителей ПДн включает присвоение регистрационных (учетных) номеров носителям. В качестве регистрационных номеров могут использоваться идентификационные (серийные) номера машинных носителей, присвоенных производителями этих машинных носителей, номер инвентарного учета и иные номера;

– носители должны храниться в сейфе, расположенном в помещении Учреждения, и изыматься только для выполнения должностных обязанностей;

– при поступлении нового машинного носителя, который будет использоваться для хранения или передачи ПДн, администратор информационной безопасности ИСПДн регистрирует его в «Журнале учёта машинных носителей ПДн».

7.2. Порядок регистрации выдачи машинных носителей ПДн:

– учет выдачи машинных носителей ПДн ведётся в «Журнале учёта машинных носителей ПДн», в котором указывается регистрационный (учетный) номер машинного носителя ПДн, дата, время, фамилия, имя и отчество должностного лица, получившего машинный носитель ПДн, его роспись;

– в случае возврата должностным лицом машинного носителя ПДн в «Журнале учёта машинных носителей ПДн» администратором информационной безопасности ИСПДн проставляется отметка о возврате с указанием даты, времени возврата, личных подписей передающей и принимающей стороны.

7.3. Доступ к машинным носителям ПДн осуществляется в соответствии с перечнем должностей, физический доступ которых к ПДн

необходим для выполнения ими должностных обязанностей, который представлен в приложении 9 к настоящему приказу.

8. Порядок работы с файлами документов, внесение корректировок, уничтожение, хранение документов

№ п.п.	Этап	Описание этапа
Подготовка к обработке информации		
1	Получение допуска к работе	Допуск сотрудников к ИСПДн осуществляется в соответствии с Перечнем должностей в Учреждении, доступ которых к ПДн, в том числе обрабатываемым в ИСПДн, необходим для выполнения ими должностных (трудовых) обязанностей и Разрешительной системе доступа пользователей к сведениям конфиденциального характера ИСПДн. Для работы в ИСПДн каждый пользователь должен получить соответствующий допуск, сведения о котором фиксируются в «Журнале учета лиц, допущенных к работе с ПДн в ИСПДн». Права по доступу к информационным ресурсам должны быть определенны утверждённой Разрешительной системой доступа пользователей к сведениям конфиденциального характера ИСПДн.
2	Получение исходной информации для обработки в системе	Исходная информация, обработка которой осуществляется в ИСПДн, может находиться на бумажных носителях.
3	Вход пользователя в систему	Авторизация пользователя осуществляется средствами защиты информации от несанкционированного доступа по имени и с использованием его персонального пароля длиной не менее 6 символов.
Обработка информации		
1	Регистрация времени начала работы	Осуществляется штатными средствами прикладного ПО и средствами защиты информации от несанкционированного доступа.
2	Ввод обрабатываемых исходных данных в систему	Ввод в систему обрабатываемых ПДн производится вручную с клавиатуры.
3	Обработка текстовой информации	Пользователь обязан принять меры по исключению возможности просмотра обрабатываемых ПДн с экрана монитора и с бумажных носителей (в том числе распечатываемых материалов) лицами, не допущенными к ПДн.
4	Временное хранение обрабатываемой информации между сеансами работы пользователя в системе	Хранение ПДн между сеансами работы в ИСПДн осуществляется в каталогах на жестком диске ПЭВМ, выделенных в ИСПДн для ПДн. Контроль доступа к ним осуществляется соответствующими средствами защиты информации.
Сохранение результатов обработки информации		

№ п.п.	Этап	Описание этапа
1	Распечатка документов	Распечатка документов (данных) производится на принтере, входящем в состав ОТСС объекта информатизации, при этом не ведется учет распечатанных документов.
2	Сохранение окончательных результатов работы	Готовые данные в электронном виде хранятся на АРМ пользователя и на учтенном съемном носителе ПДн. Готовые данные в бумажном виде хранятся в кабинетах здания.
3	Передача носителей ПДн и распечатанных документов	В соответствии с требованиями организационно-распорядительных документов.
4	Очистка остаточной (удаленной) информации	Гарантированная очистка удаляемых ПДн с машинных носителей ПДн (без возможности ее восстановления) осуществляется средствами системы защиты информации от НСД.
5	Регистрация времени работы и действий пользователя в системе	Осуществляется штатными средствами прикладного ПО.
6	Завершение работы	После окончания работы с ИСПДн пользователь обязан на своем рабочем месте завершить работу всех программ, входящих в состав специализированного ПО и выключить компьютер (перегрузить). При необходимости оставить свое рабочее место на непродолжительное время пользователь обязан его заблокировать (дальнейшая работа может быть продолжена пользователем только после ввода его логина и пароля). После окончания рабочего дня необходимо закрыть окна и форточки, выключать электроприборы и запереть и опечатать дверь.

9. Ответственность лиц, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими должностных (трудовых) обязанностей

9.1. Персональную ответственность за соблюдение установленных требований настоящих Правил несут пользователи ИСПДн и администратор информационной безопасности ИСПДн.

9.2. За разглашение ПДн и нарушение порядка обращения с машинными носителями ПДн администратор информационной безопасности ИСПДн, а также пользователи ИСПДн, работающие с этими машинными носителями ПДн, могут быть привлечены к дисциплинарной и иной, предусмотренной законодательством Российской Федерации, ответственности.

9.3. 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.

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

9.5. Нарушение данных Правил, повлекшее уничтожение, блокирование, модификацию либо копирование ПДн, нарушение работы компьютеров пользователей ИСПДн или ИСПДн в целом, может повлечь ответственность в соответствии с действующим законодательством РФ.

Приложение 27
к приказу бюджетного учреждения
Ханты-Мансийского автономного округа – Югры
«Центр имущественных отношений»
№ 13/01-П-85 от «27» июня 2023 г.

Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в бюджетном учреждении Ханты-Мансийского автономного округа – Югры «Центр имущественных отношений»
(далее – Правила)

1. Общие положения

1.1. Настоящие Правила, разработаны в соответствии с Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных» и устанавливают процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере обработки персональных данных, а также определяют основания, порядок и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям законодательства Российской Федерации.

2. Порядок осуществления внутреннего контроля соответствия обработки персональных данных к требованиям защиты персональных данных

1.2. В целях осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям к защите персональных данных в бюджетном учреждении Ханты-Мансийского автономного округа – Югры «Центр имущественных отношений» (далее – Учреждение) организовывается проведение ежегодных проверок.

1.3. Проверки проводятся ответственным за организацию обработки персональных данных совместно с ответственным за обеспечение безопасности персональных данных в информационных системах персональных данных и ответственным за эксплуатацию информационной системы персональных данных.

1.4. Плановые проверки условий обработки персональных данных проводятся на основании утвержденного директором Учреждения ежегодного плана внутренних проверок режима защиты персональных данных (плановые проверки).

1.5. Внеплановые проверки проводятся на основании поступившей информации о нарушениях правил обработки персональных данных, по инициативе ответственного за организацию обработки персональных данных, либо ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных. Проведение внеплановой проверки организуется в течение 10 (десяти) рабочих дней со дня поступления информации о нарушениях правил обработки персональных данных.

1.6. В проведении проверки условий обработки персональных данных не могут участвовать работники Учреждения, прямо или косвенно заинтересованные в ее результате.

1.7. Проверки условий обработки персональных данных осуществляются непосредственно на месте обработки персональных данных путем опроса либо, при необходимости, путем осмотра служебных мест работников Учреждения, участвующих в процессе обработки персональных данных.

1.8. 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 Учреждения;

– 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 соблюдения парольной защиты;

– порядок и условия соблюдения антивирусной защиты;

– порядок и условия обеспечения резервного копирования;

– эффективность принимаемых мер по обеспечению безопасности персональных данных до их ввода в ИСПДн;

– условия соблюдения режима защиты при подключении к информационно-телекоммуникационным сетям;

– порядок и условия обновления программного обеспечения и единообразия применяемого программного обеспечения на всех элементах ИСПДн;

– порядок и условия применения средств защиты информации;

– соблюдение учета носителей персональных данных;

– соблюдение правил доступа к персональным данным;

– соблюдение порядка доступа в помещения, в которых ведется

обработка персональных данных;

– наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;

– мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

1.9. Ответственный за организацию обработки персональных данных и ответственный за обеспечение безопасности персональных данных в ИСПДн, а также ответственный за эксплуатацию ИСПДн в ходе проверки имеют право:

– запрашивать у работников информацию, необходимую для реализации своих полномочий;

– требовать от уполномоченных на обработку персональных данных работников 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.

1.10. Проверка условий обработки персональных данных должна быть завершена не позднее чем через тридцать календарных дней со дня принятия решения о ее проведении.

По результатам проведенной проверки условий обработки персональных данных ответственный за организацию обработки

персональных данных предоставляет директору Учреждения письменное заключение с указанием мер, необходимых для устранения выявленных нарушений.