ПРОЕКТ

МЕСТНОЕ САМОУПРАВЛЕНИЕ
Г. ТАГАНРОГ РОСТОВСКОЙ ОБЛАСТИ
КОНТРОЛЬНО-СЧЕТНАЯ ПАЛАТА ГОРОДА ТАГАНРОГА

ПРЕДСЕДАТЕЛЬ КОНТРОЛЬНО-СЧЕТНОЙ ПАЛАТЫ ГОРОДА ТАГАНРОГА

ПРИКАЗ

_____ № ____

Об утверждении инструкций и форм документов в сфере обработки персональных данных и защиты информации

В целях осуществления организационных мер по обеспечению безопасности персональных данных при их обработке в информационной системе персональных данных Контрольно-счетной палаты города Таганрога, а также обеспечения реализации требований предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и Постановлением Правительства РФ от 21.03.2012 № 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»,

ПРИКАЗЫВАЮ:

1. Утвердить следующие инструкции в сфере обработки персональных данных и защиты информации:

1.1. Инструкция администратора информационной системы персональных данных Контрольно-счетной палаты города Таганрога (приложение 1);

1.2. Инструкция администратора информационной безопасности информационной системы персональных данных Контрольно-счетной палаты города Таганрога (приложение 2);

1.3. Инструкция пользователя информационной системы персональных данных Контрольно-счетной палаты города Таганрога (приложение 3);

1.4. Инструкция по организации резервного копирования и восстановления защищаемой информации в информационной системе персональных данных Контрольно-счетной палаты города Таганрога (приложение 4);

1.5. Инструкция по организации антивирусной защиты информационной системы персональных данных Контрольно-счетной палаты города Таганрога (приложение 5);

1.6. Инструкция по организации парольной защиты в информационной системе персональных данных Контрольно-счетной палаты города Таганрога (приложение 6);

1.7. Инструкция по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационной системы персональных данных Контрольно-счетной палаты города Таганрога (приложение 7);

1.8. Инструкция по учету средств защиты, документации и электронных носителей персональных данных в Контрольно-счетной палате города Таганрога (приложение 8);

1.9. Инструкция по действиям пользователей информационной системы персональных

данных Контрольно-счетной палаты города Таганрога в нештатных ситуациях (приложение 9).

2. Утвердить следующие формы журналов учета в сфере обработки персональных данных и защиты информации:

2.1. Журнал учета письменных запросов граждан на доступ к своим персональным данным в Контрольно-счетной палате города Таганрога (приложение 10);

2.2. Журнал учета носителей персональных данных в Контрольно-счетной палате города Таганрога (приложение 11);

2.3. Журнал поэкземплярного учета средств защиты информации, эксплуатационной и технической документации к ним (приложение 12);

2.4. Журнал учета проведения инструктажей по вопросам защиты информации в Контрольно-счетной палате города Таганрога (приложение 13);

2.5. Журнал учета проведения полного резервного копирования в Контрольно-счетной палате города Таганрога (приложение 14);

2.6. Журнал учета работ по восстановлению защищаемой информации в информационной системе персональных данных Контрольно-счетной палаты города Таганрога (приложение 15);

2.7. Журнал учета ключевых носителей информации, выданных уполномоченным лицам (работникам) Контрольно-счетной палаты города Таганрог (приложение 16);

2.8. Журнал учета нештатных ситуаций в Контрольно-счетной палате города Таганрога (приложение 17);

2.9. Журнал учета технических средств, участвующих в обработке персональных данных в Контрольно-счетной палате города Таганрога (приложение 18);

2.10. Журнал учета работ по уничтожению персональных данных в Контрольно-счетной палате города Таганрога (приложение 19).

3. Утвердить следующие формы документов в сфере обработки персональных данных и защиты информации:

3.1. Акт об уничтожении персональных данных (приложение 20);

3.2. Акт проверки соответствия обработки персональных данных требованиям к защите персональных данных (приложение 21).

4. Установить следующие требования к ведению журналов учета, предусмотренных пунктом 1 настоящего приказа (далее – журналы учета):

4.1. журналы учета должны быть прошиты, пронумерованы, скреплены подписью лица, ответственного за организацию обработки персональных данных в Контрольно-счетной палате города Таганрога, и скреплен печатью «Для документов»;

4.2. журналы учета заполняются шариковой или гелевой ручкой синего цвета;

4.3. не допускается написание более одной строчки текста в строке журнала учета, то есть при необходимости текст переносится на следующую строку журнала учета;

4.4. все даты в журналах учета пишутся в формате ЧЧ.ММ.ГГГГ;

4.5. не допускаются в процессе заполнения журнала учета исправления, в том числе с использованием корректирующих средств (жидкость, лента и др.), помарки и подчистки. В случаях, если были допущены ошибки (описки), неверно написанная информация зачеркивается одной чертой, под ней пишется правильная информация, проставляется фраза «Исправленному верить.», должность и подпись лица, внесшего исправление, дата внесения исправлений, а также печать «Для документов».

5. Лицам, указанным в пункте 6 настоящего приказа:

5.1.осуществить ознакомление работников Контрольно-счетной палаты города Таганрога с инструкциями, утвержденными пунктом 1 настоящего приказа, в соответствии с требованиями соответствующих инструкций;

5.2.осуществлять ознакомление вновь принятых на работу работников Контрольно-счетной палаты города Таганрога с инструкциями, утвержденными пунктом 1 настоящего приказа, в соответствии с требованиями соответствующих инструкций;

5.3. осуществлять ведение журналов учета, по формам и в соответствии с требованиями, установленными настоящим приказом, с учетом соответствующих инструкций в сфере обработки персональных данных и защиты информации, предусмотренных пунктом 1 настоящего приказа.

6. Ознакомить лицо, ответственное за организацию обработки персональных данных в Контрольно-счетной палате города Таганрога (Шарафутдинова Т.А.), администратора информационной системы персональных данных Контрольно-счетной палаты города Таганрога (Акименко К.С.) и администратора информационной безопасности информационной системы персональных данных Контрольно-счетной палаты города Таганрога (Лаптева М.Ю.) с настоящим приказом под подпись.

7. Настоящий приказ вступает в силу со дня принятия.

8. Контроль за исполнением настоящего приказа возложить на заместителя председателя Контрольно-счетной палаты города Таганрога Шарафутдинову Т.А.

Председатель Контрольно-счетной
палаты города Таганрога **О.В. Субботина**

Начальник отдела правового, методологического,
кадрового и материального обеспечения
Контрольно-счетной палаты города Таганрога М.Ю. Лаптева

Приложение 1
к приказу председателя
Контрольно-счетной палаты
города Таганрога от
от _____ № ____

ИНСТРУКЦИЯ
администратора информационной системы персональных данных
Контрольно-счетной палаты города Таганрога

1. Общие положения

1. Инструкция администратора информационной системы персональных данных Контрольно-счетной палаты города Таганрога (далее – Инструкция) устанавливает основные обязанности, права и ответственность администратора информационной системы персональных данных Контрольно-счетной палаты города Таганрога (далее также ИСПДн, Палата).

2. Администратор ИСПДн Палаты назначается распоряжением председателя Палаты и функционально подчиняется лицу, ответственному за организацию обработки персональных данных в Палате.

3. Администратор ИСПДн Палаты руководствуется требованиями нормативных правовых актов Российской Федерации, нормативных правовых актов Палаты, настоящей Инструкцией, а также другими распорядительными документами в части, его касающейся.

4. Работники Палаты, задействованные в обеспечении функционирования ИСПДн Палаты, могут быть ознакомлены с настоящей Инструкцией по мере необходимости.

5. Ознакомление администратора ИСПДн Палаты с требованиями настоящей Инструкции, осуществляет лицо, ответственное за организацию обработки персональных данных в Палате под подпись в листе ознакомления с выдачей копии Инструкции непосредственно для повседневного использования в работе.

6. В случае увольнения администратор ИСПДн Палаты обязан передать все носители защищаемой информации Палаты, которые находились в его распоряжении во время работы в Палате, администратору информационной безопасности ИСПДн Палаты или лицу, ответственному за организацию обработки персональных данных в Палате.

2. Обязанности администратора ИСПДн Палаты

7. Администратор ИСПДн Палаты обязан:

1) обеспечивать работоспособность средств вычислительной техники ИСПДн Палаты, проводить организационно-технические мероприятия по их обслуживанию;

2) осуществлять настройку компонентов ИСПДн Палаты, включая прикладное программное обеспечение и специальное программное обеспечение;

3) рассматривать целесообразность применения новых технологий для повышения эффективности функционирования ИСПДн Палаты;

4) подготавливать обоснования и спецификации для закупки новых элементов ИСПДн Палаты и расходных материалов;

5) поддерживать резерв расходных материалов;

6) изучать рынок программных средств и представлять рекомендации по приобретению и внедрению системного и прикладного программного обеспечения;

7) выполнять своевременное обновление программного обеспечения элементов ИСПДн Палаты и системы защиты информации (в пределах своей компетенции) по мере появления новых версий;

8) выполнять учет информации ИСПДн Палаты;

9) выполнять резервное копирование информации ИСПДн Палаты и, в случае необходимости – восстановление данных в соответствие с требованиями Инструкции по

организации резервного копирования и восстановления защищаемой информации в информационной системе персональных данных Контрольно-счетной палаты города Таганрога;

10) фиксировать факты осуществления резервного копирования в Журнале учета проведения полного резервного копирования в Контрольно-счетной палате города Таганрога;

11) фиксировать факты восстановления данных должны в Журнале учета восстановлений информации утраченной (уничтоженной, поврежденной) вследствие нештатных ситуаций в Контрольно-счетной палате города Таганрога;

12) проводить инструктаж пользователей по внедряемым и используемым технологиям или прикладному программному обеспечению, если это требует от пользователей дополнительных навыков и знаний;

13) совместно с администратором информационной безопасности ИСПДн Палаты обеспечивать контроль выполнения пользователями положений Инструкции пользователя информационной системы персональных данных Контрольно-счетной палаты города Таганрога;

14) вести учет всех технических средств, на которых осуществляется обработка персональных данных в Журнале учета технических средств, участвующих в обработке персональных данных в Контрольно-счетной палате города Таганрога;

15) оказывать помощь администратору информационной безопасности ИСПДн Палаты при анализе работы элементов ИСПДн или средств защиты персональных данных с целью выявления и устранения неисправностей, а также оптимизации их функционирования;

16) оказывать помощь администратору информационной безопасности ИСПДн Палаты в осуществлении контроля действий пользователей ИСПДн Палаты по работе с паролями;

17) предоставлять администратору информационной безопасности ИСПДн Палаты любую затребованную им информацию о настройках, конфигурации, составу и структуре ИСПДн Палаты и механизмов защиты информации ИСПДн Палаты;

18) выполнять действия по изменению элементов ИСПДн Палаты, необходимость в которых определяется согласованным решением, определенным совместно с администратором информационной безопасности ИСПДн Палаты;

19) участвовать совместно с администратором информационной безопасности ИСПДн Палаты в проведении служебных расследований фактов нарушения или угрозы нарушения безопасности защищаемой информации;

20) сопровождать исполнителей по муниципальным контрактам (договорам гражданско-правового характера), которые выполняют работы по обслуживанию ИСПДн Палаты;

21) в случае обнаружения попытки несанкционированного доступа в отношении защищаемой информации со стороны пользователей ИСПДн Палаты или третьих лиц, оповещать администратора информационной безопасности ИСПДн Палаты;

22) осуществлять контроль технологических процессов обработки защищаемой информации;

23) осуществлять при необходимости совместно с лицом, ответственным за организацию обработки персональных данных в Палате периодические проверки состояния защиты персональных данных (в соответствии Правилами осуществления внутреннего контроля соответствия обработки персональных данных в Контрольно-счетной палате города Таганрога требованиям к защите персональных данных, установленным Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами Контрольно-счетной палаты города Таганрога, утвержденными приказом председателя Контрольно-счетной палаты города Таганрога от 10.03. 2016 № 10);

24) участвовать при необходимости в качестве члена комиссии по:

проведению классификации информационных систем персональных данных;

установлению уровней защищенности информационных систем персональных данных;

уничтожению персональных данных;

контролю защищенности персональных данных;

25) разрабатывать предложения лицу, ответственному за организацию обработки персональных данных в Палате по изменению правовых актов Палаты, регламентирующих процессы обработки и обеспечения безопасности персональных данных в Палате;

26) планировать дальнейшее развитие структуры и функциональности ИСПДн Палаты, а также вносит предложения о совершенствовании работы и повышении эффективности функционирования средств вычислительной техники ИСПДн Палаты и системы защиты информации ИСПДн Палаты.

3. Права администратора ИСПДн Палаты

8. Администратор ИСПДн Палаты имеет право:

1) анализировать работу любых элементов ИСПДн Палаты для выявления и устранения неисправностей, а также для оптимизации ее функционирования;

2) отключать любые элементы ИСПДн Палаты при изменении конфигурации, регламентном техническом обслуживании или устранении неисправностей после согласования и заблаговременного предупреждения пользователей ИСПДн Палаты;

3) отключать элементы системы защиты персональных данных ИСПДн Палаты при изменении конфигурации, регламентном техническом обслуживании или устранении неисправностей в установленном порядке после согласования с администратором информационной безопасности ИСПДн Палаты.

4) изменять конфигурацию элементов ИСПДн Палаты в установленном порядке;

5) требовать от пользователей ИСПДн Палаты соблюдения Инструкции пользователя информационной системы персональных данных Контрольно-счетной палаты города Таганрога;

6) вносить предложения по совершенствованию функционирования ИСПДн Палаты.

4. Ответственность администратора ИСПДн Палаты

9. Администратор ИСПДн Палаты несет ответственность:

1) за ненадлежащее исполнение или неисполнение обязанностей, предусмотренных настоящей Инструкцией, другими инструктивными документами, в соответствии с действующим трудовым законодательством Российской Федерации;

2) за правонарушения, совершенные в процессе своей деятельности, а также за разглашение сведений конфиденциального характера и другой защищаемой информации, в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.

10. Контроль выполнения требований настоящей Инструкции осуществляет лицо, ответственное за организацию обработки персональных данных в Палате.

Приложение 2
к приказу председателя
Контрольно-счетной палаты
города Таганрога от
от _____ № ____

ИНСТРУКЦИЯ
администратора информационной безопасности информационной системы персональных данных Контрольно-счетной палаты города Таганрога

1. Общие положения

1. Инструкция администратора информационной безопасности информационной системы персональных данных Контрольно-счетной палаты города Таганрога (далее – Инструкция) устанавливает права, обязанности и ответственность администратора информационной безопасности информационной системы персональных данных Контрольно-счетной палаты города Таганрога (далее также ИСПДн, Палата).

2. Администратор информационной безопасности ИСПДн Палаты назначается распоряжением председателя Палаты и функционально подчиняется лицу, ответственному за организацию обработки персональных данных в Палате.

3. В своей деятельности администратор информационной безопасности руководствуется требованиями нормативных правовых актов Российской Федерации, нормативных правовых актов Палаты, настоящей Инструкцией, а также другими распорядительными документами в части, его касающейся.

4. Администратор информационной безопасности ИСПДн Палаты в пределах своих обязанностей обеспечивает работоспособность ИСПДн Палаты, безопасность информации, обрабатываемой, передаваемой и хранимой при помощи средств вычислительной техники в ИСПДн Палаты.

5. Работники Палаты, задействованные в обеспечении функционирования ИСПДн Палаты, могут быть ознакомлены с настоящей Инструкцией по мере необходимости.

6. В случае увольнения, администратор информационной безопасности ИСПДн Палаты обязан передать лицу, ответственному за организацию обработки персональных данных в Палате все носители защищаемой информации Палаты, которые находились в его распоряжении во время работы в Палате.

7. Ознакомление администратора информационной безопасности ИСПДн Палаты с требованиями настоящей Инструкции осуществляет лицо, ответственное за организацию обработки персональных данных в Палате под подпись в листе ознакомления с выдачей копии Инструкции непосредственно для повседневного использования в работе

2. Обязанности администратора информационной безопасности ИСПДн Палаты

8. Администратор информационной безопасности ИСПДн Палаты обязан:

1) знать перечень установленных в Палате средств вычислительной техники и перечень задач, решаемых с их использованием;

2) осуществлять контроль изменений (в том числе и несанкционированных) аппаратного обеспечения автоматических рабочих мест и серверного оборудования;

3) обеспечивать установление и настройку средств защиты информации;

4) рассматривать целесообразность применения новых технологий для повышения эффективности функционирования ИСПДн Палаты;

5) обеспечивать своевременное обновление средств защиты персональных данных по мере появления таких обновлений;

6) обеспечивать контроль за выполнением пользователями ИСПДн Палаты Инструкции пользователя информационной системы персональных данных Контрольно-счетной палаты города Таганрога;

7) осуществлять контроль работы пользователей ИСПДн Палаты, выявление попыток несанкционированного доступа к защищаемой информации и техническим средствам ИСПДн Палаты, а при выявлении фактов несанкционированного доступа – фиксировать данные в Журнале учета нештатных ситуаций в Контрольно-счетной палате города Таганрога;

8) обеспечивать осуществление настройки средств защиты, выполнение других действий по изменению элементов ИСПДн Палаты;

9) осуществлять учет всех защищаемых носителей информации с помощью их любой маркировки и с занесением учетных данных в Журнал учета носителей персональных данных в Контрольно-счетной палате города Таганрога и выдавать их пользователям под подпись в указанном Журнале;

10) контролировать исполнение запрета использования неучтенных носителей персональных данных, равно как их выдачи/приема без записи в Журнал учета носителей персональных данных в Контрольно-счетной палате города Таганрога;

11) осуществлять текущий и периодический контроль работы средств и систем защиты информации;

12) осуществлять текущий контроль технологического процесса обработки защищаемой информации;

13) обеспечивать периодическое осуществление тестирования всех функций системы защиты с помощью тестовых программ, имитирующих попытки несанкционированного доступа, а также при изменении программной среды и персонала ИСПДн Палаты;

14) участвовать в проведении служебных расследований фактов нарушения или угрозы нарушения безопасности защищаемой информации;

15) участвовать в проведении работ по восстановлению работоспособности средств и систем защиты информации;

16) вести Журнал учета нештатных ситуаций в Контрольно-счетной палате города Таганрога;

17) проводить проверку регистраций событий безопасности;

18) проводить обучение работников Палаты правилам работы со средствами вычислительной техники и средствами защиты информации с отметкой в Журнале учета проведения инструктажей по вопросам защиты информации в Контрольно-счетной палате города Таганрога в части:

обеспечения антивирусной защиты при работе в информационных системах персональных данных;

порядка парольной защиты при работе в информационных системах персональных данных;

19) участвовать в разработке нормативных и методических материалов, связанных с функционированием средств вычислительной техники и применением средств защиты информации, выполнением мероприятий по обеспечению защиты информации;

20) немедленно докладывать лицу, ответственному за организацию обработки персональных данных в Палате, о возникновении нештатных ситуаций;

21) рассматривать заявки пользователей на доступ к ИСПДн;

22) обеспечивать осуществление контроля технологических процессов обработки защищаемой информации;

23) разрабатывать предложения по изменению нормативных документов, регламентирующих процессы обработки и обеспечения безопасности персональных данных;

24) осуществлять совместно с лицом, ответственным за организацию обработки персональных данных в Палате периодические проверки состояния защиты персональных данных (в соответствии Правилами осуществления внутреннего контроля соответствия обработки персональных данных в Контрольно-счетной палате города Таганрога требованиям к защите персональных данных, установленным Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», принятыми в соответствии с ним нормативными правовыми

актами и локальными актами Контрольно- счетной палаты города Таганрога, утвержденными приказом председателя Контрольно-счетной палаты города Таганрога от 10.03. 2016 № 10);

25) участвовать в качестве члена комиссий по:

проведению классификации информационных систем персональных данных;

установлению уровней защищенности информационных систем персональных данных;

уничтожению персональных данных;

контролю защищенности персональных данных;

26) вести учет всех средств защиты информации и технической документации к ним, используемых в Контрольно-счетной палате города Таганрога в Журнале поэкземплярного учета средств защиты персональных данных, эксплуатационной и технической документации к ним;

27) оказывать помощь администратору ИСПДн Палаты в разработке и согласовывать перечень информации ИСПДн Палаты, подлежащей резервному копированию, а также осуществлять контроль выполнения резервного копирования информации администратором ИСПДн Палаты;

28) осуществлять надежное хранение резервных копий;

29) осуществлять контроль действий пользователей ИСПДн Палаты с паролями;

30) оказывать помощь лицу, ответственному за организацию обработки персональных данных в Палате в других вопросах, касающихся обеспечения безопасности и обработки персональных данных в Палате.

3. Права администратора информационной безопасности ИСПДн Палаты

9. Администратор информационной безопасности ИСПДн Палаты имеет право:

1) отключать любые элементы средств защиты персональных данных при изменении конфигурации, регламентном техническом обслуживании или устранении неисправностей в установленном порядке;

2) изменять конфигурацию элементов ИСПДн Палаты и средств защиты персональных данных в установленном порядке ;

3) требовать от работников Палаты соблюдения правил работы в ИСПДн Палаты, приведенных в Инструкции пользователя информационной системы персональных данных Контрольно-счетной палаты города Таганрога;

4) требовать от пользователей ИСПДн Палаты безусловного соблюдения установленной технологии обработки защищаемой информации и выполнения требований внутренних документов Палаты, регламентирующих вопросы обеспечения безопасности и защиты информации;

5) обращаться к лицу, ответственному за организацию обработки персональных данных в Палате с требованием о прекращении обработки защищаемой информации в случаях нарушения установленной технологии обработки защищаемой информации или нарушения функционирования средств и систем защиты информации;

6) вносить свои предложения по совершенствованию функционирования ИСПДн Палаты;

7) инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности в ИСПДн Палаты.

4. Ответственность администратора информационной безопасности ИСПДн Палаты

10. Администратор информационной безопасности ИСПДн несет ответственность:

1) за ненадлежащее исполнение или неисполнение обязанностей, предусмотренных настоящей инструкцией, другими инструктивными документами, за полноту и качество проводимых им работ по обеспечению защиты информации в соответствии с действующим

законодательством Российской Федерации, трудовым законодательством Российской Федерации;

2) за правонарушения, совершенные в процессе своей деятельности, а также за разглашение сведений конфиденциального характера и другой защищаемой информации, в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации

3) за обеспечение работоспособности средств защиты персональных данных в Палате.

11. Контроль выполнения требований настоящей Инструкции осуществляет лицо, ответственное за организацию обработки персональных данных в Палате.

Приложение 3
к приказу председателя
Контрольно-счетной палаты
города Таганрога от
от _____ № ____

ИНСТРУКЦИЯ
пользователя информационной системы персональных данных
Контрольно-счетной палаты города Таганрога

1. Общие положения

1. Инструкция пользователя информационной системы персональных данных Контрольно-счетной палаты города Таганрога (далее – Инструкция) устанавливает обязанности, запреты и ответственность пользователя информационной системы персональных данных Контрольно-счетной палаты города Таганрога (далее также ИСПДн, Палата).

2. Пользователями ИСПДн Палаты являются работники Палаты, участвующие в рамках своих должностных обязанностей в процессах автоматизированной обработки персональных данных и имеющий доступ к аппаратным средствам, программному обеспечению и данным, содержащимся в ИСПДн Палаты (далее – пользователи ИСПДн Палаты).

3. Ознакомление пользователей ИСПДн Палаты с требованиями настоящей Инструкции осуществляет администратор информационной безопасности ИСПДн под подпись в листе ознакомления с выдачей копий настоящей Инструкции непосредственно для повседневного использования в работе.

2. Обязанности пользователя ИСПДн Палаты

4. Пользователь ИСПДн Палаты обязан:

1) соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн Палаты;

2) выполнять свои должностные обязанности строго в рамках прав доступа к внутренним и внешним информационным ресурсам, техническим средствам, полученным в установленном порядке;

3) знать и выполнять правила работы со средствами защиты информации, установленными в ИСПДн Палаты;

4) хранить в тайне свой пароль (пароли);

5) исполнять требования Инструкции по организации парольной защиты в информационной системе персональных данных Контрольно-счетной палаты города Таганрога, а также других документов, регламентирующих вопросы работы в ИСПДн и обеспечения безопасности информации в части, его касающейся;

6) незамедлительно ставить в известность администратора информационной безопасности ИСПДн Палаты в случае утери личных реквизитов доступа, при компрометации личных паролей, подозрении на совершение попыток несанкционированного доступа к персональным электронно-вычислительным машинам, обнаружении несанкционированных изменений в конфигурации программных или аппаратных средств ИСПДн Палаты;

7) незамедлительно ставить в известность администратора ИСПДн Палаты при обнаружении отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию ИСПДн Палаты, выхода из строя или неустойчивого функционирования устройств персональных электронно-вычислительных машин (дисководов, клавиатуры, принтера и т.п.), а также перебоев в системе электроснабжения, некорректного функционирования установленных технических средств защиты информации;

8) незамедлительно ставить в известность администратора информационной безопасности ИСПДн Палаты в случае обнаружения недокументированных свойств и ошибок в программном обеспечении или в настройках средств защиты;

9) присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию персональной электронно-вычислительной машины, закрепленной за ним, в случае обработке на ней защищаемой информации;

10) применять только учтенные носители информации при обработке на персональных электронно-вычислительных машинах защищаемой информации и необходимости использовать носители информации.

5. Пользователям ИСПДн Палаты ЗАПРЕЩАЕТСЯ:

1) использовать компоненты программного и аппаратного обеспечения ИСПДн Палаты в неслужебных целях;

2) хранить и обрабатывать личную информацию на персональных электронно-вычислительных машинах и серверном оборудовании ИСПДн Палаты;

3) при работе в сети Интернет:

использовать информационные ресурсы сети Интернет, содержание которых нарушает действующее законодательство Российской Федерации;

использовать информационные ресурсы сети Интернет для целей, не связанных с областью служебной деятельности пользователя;

использовать информационные ресурсы сети Интернет в личных целях;

вносить изменения в состав и/или процесс работы внешних информационных ресурсов, если такие изменения не санкционированы собственником (владельцем) соответствующего ресурса;

4) самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн Палаты или устанавливать дополнительно любые программные и аппаратные средства;

5) оставлять без присмотра включенную персональную электронно-вычислительную машину, закрепленную за ним, не активизировав средства защиты от несанкционированного доступа;

6) оставлять без личного присмотра на рабочем месте или где бы то ни было свои персональные реквизиты доступа (логины и (или) пароли);

7) оставлять без личного присмотра в свободном доступе на рабочем месте или где бы то ни было свои машинные носители или бумажные носители, содержащие персональные данные;

8) использовать в работе неучтенные носители информации для обработки защищаемой информации;

9) умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты.

3. Ответственность пользователя ИСПДн Палаты

6. Пользователи ИСПДн Палаты несут ответственность:

1) за ненадлежащее исполнение или неисполнение обязанностей, а также нарушение запретов предусмотренных настоящей инструкцией, другими инструктивными документами в соответствии с действующим законодательством Российской Федерации, трудовым законодательством Российской Федерации;

2) за правонарушения, совершенные в процессе своей деятельности, а также за разглашение сведений конфиденциального характера и другой защищаемой информации Палаты в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.

7. Контроль за исполнением пользователями ИСПДн Палаты настоящей Инструкции осуществляется администратором информационной безопасности ИСПДн Палаты.

Приложение 4
к приказу председателя
Контрольно-счетной палаты
города Таганрога от
от _____ № ____

ИНСТРУКЦИЯ
по организации резервного копирования и восстановления защищаемой информации в информационной системе персональных данных Контрольно-счетной палаты города Таганрога

1. Общие положения

1. Инструкция по организации резервного копирования и восстановления защищаемой информации в информационной системе персональных данных Контрольно-счетной палаты города Таганрога (далее – Инструкция) устанавливает основные требования к организации резервного копирования (восстановления) информации, содержащейся в информационной системе персональных данных Контрольно-счетной палаты города Таганрога (далее также ИСПДн, Палата).

2. Настоящая Инструкция разработана в целях:

определения категории информации, подлежащей обязательному резервному копированию;

определения процедуры резервирования данных для последующего восстановления работоспособности ИСПДн при полной или частичной потере (уничтожении, повреждении) информации, вызванной сбоями или отказами аппаратного или программного обеспечения, умышленными действиями третьих лиц, несанкционированными доступами в систему, воздействием вирусов, ошибками пользователей, чрезвычайными ситуациями (пожар, стихийное бедствие и т.д.) (далее – нештатная ситуация);

определения порядка восстановления информации в случае возникновения такой необходимости;

упорядочения работы и определения ответственности работников Палаты, связанной с резервным копированием и восстановлением информации.

3. Под резервным копированием информации понимается создание копий защищаемой информации в электронном виде для быстрого восстановления работоспособности ИСПДн Палаты в случае возникновения нештатной ситуации, повлекшей за собой потерю (повреждение, уничтожение) данных.

4. Резервному копированию подлежит информация следующих основных категорий:

персональная информация пользователей (личные каталоги) и групповая информация (общие каталоги) на файловых серверах;

информация, обрабатываемая пользователями в ИСПДн Палаты, а также информация, необходимая для восстановления работоспособности ИСПДн Палаты;

рабочие копии установочных компонент программного обеспечения общего назначения и специализированного программного обеспечения ИСПДн Палаты, СУБД, серверного оборудования и рабочих станций;

информация, необходимая для восстановления серверного оборудованияи систем управления базами данных ИСПДн Палаты, локальной вычислительной сети, системы электронного документооборота;

регистрационная информация системы информационной безопасности ИСПДн Палаты;

другая информация ИСПДн Палаты, по мнению пользователей и администратора информационной безопасности, являющаяся критичной для работоспособности ИСПДн Палаты.

5. Резервное копирование осуществляется администратором информационной безопасности ИСПДн Палаты и контролируется лицом, ответственным за организацию обработки персональных данных в Палате.

6. Работники Палаты, задействованные в осуществлении резервного копирования информации содержащейся в ИСПДн Палаты ознакамливаются с настоящей Инструкциейв части их касающейся под подпись в листе ознакомления с выдачей копий настоящей Инструкции непосредственно для повседневного использования в работе.

2. Периодичность и схема резервного копирования

7. При осуществлении резервного копирования используются два типа копирования: полное резервное копирование и резервное копирование измененных после последнего копирования блоков информации (инкрементальное резервное копирование).

8. Резервное копирование информации, содержащейся в ИСПДн Палаты, осуществляется по следующей двухуровневой схеме ротации:

полное резервное копирование информации выполняется ежемесячно (15-16 числа). Архив хранится в течение трех месяцев и является архивом Уровня 1;

инкрементальное резервное копирование информации выполняется ежедневно (по окончанию рабочего дня). Архив хранится в течение недели и является архивом Уровня 2.

3. Порядок резервного копирования

9. Администратор информационной безопасности ИСПДн Палаты настраивает задания для программного обеспечения, осуществляющего резервное копирование на автоматическое выполнение в соответствии с перечнем информации, подлежащей резервному копированию, а также периодичностью и схемой резервного копирования.

10. Перед выполнением задания резервного копирования информации администратор информационной безопасности ИСПДн Палаты осуществляет проверку доступности резервного носителя, а также наличие на нем свободного места для записи данных.

11. После завершения выполнения резервного копирования информации администратор информационной безопасности ИСПДн Палаты должен извлечь резервный носитель, подписать его по формату «число, месяц, год, уровень №» и поместить в сейф (запираемый шкаф, запираемый ящик).

12. Проведение полного ежемесячного резервного копирования регистрируется в Журнале учета проведения полного резервного копирования в Контрольно-счетной палате города Таганрога.

13. Инкрементальное резервное копирование осуществляется в порядке, предусмотренном для полного резервного копирования. Регистрация инкрементального резервного копирования не осуществляется.

4. Хранение резервных копий

14. Хранение носителей резервных копий осуществляется в помещении, отдельном от помещения, в котором хранится копируемая информация.

15. Носители резервных копий хранятся в хранилище резервных копий (сейф, запираемый шкаф или запираемый ящик) на безопасном расстоянии от источников электромагнитных полей: блоков питания, телефонов, мониторов и т.д.

16. Доступ к хранилищу резервных копий имеют только администратор информационной безопасности и лицо, ответственное за организацию обработки персональных данных в Палате.

17. Доступ к носителям резервных копий имеют только уполномоченные работники Палаты, непосредственно осуществляющие резервное копирование, которые несут персональную ответственность за сохранность резервных копий и невозможность ознакомления с ними лиц, не имеющих на то права.

18. Контроль за доступом и выдачей носителей резервных копий возлагается на администратора безопасности ИСПДн.

5. Восстановление работоспособности ИСПДн

19. В случае потери (повреждения, уничтожения) информации администратором информационной безопасности ИСПДн из хранилища резервных копий извлекается носитель с резервной копией той информации, которая нуждается в восстановлении, от последнего произведенного резервного копирования.

В зависимости от характера и уровня потери (повреждения, уничтожения) информации администратор информационной безопасности ИСПДн восстанавливает либо весь массив резервных данных, либо отдельные потерянные (уничтоженные, поврежденные) файлы и (или) папки.

20 Действия по восстановлению фиксируются в Журнале учета работ по восстановлению защищаемой информации в информационной системе персональных данных Контрольно-счетной палаты города Таганрога.

21. Восстановление системного программного обеспечения и программного обеспечения общего назначения производится с их носителей в соответствии с инструкциями производителя.

Восстановление специализированного программного обеспечения производится с дистрибутивных носителей или их резервных копий в соответствии с инструкциями по установке или восстановлению данного программного обеспечения.

Восстановление системного программного обеспечения, программного обеспечения общего назначения и специализированного программного обеспечения осуществляется без регистрации в Журнале учета работ по восстановлению защищаемой информации в информационной системе персональных данных Контрольно-счетной палаты города Таганрога.

Приложение 5
к приказу председателя
Контрольно-счетной палаты
города Таганрога от
от _____ № ____

ИНСТРУКЦИЯ
по организации антивирусной защиты информационной системы персональных данных Контрольно-счетной палаты города Таганрога

1. Общие положения

1. Инструкция по организации антивирусной защиты информационной системы персональных данных Контрольно-счетной палаты города Таганрога (далее – Инструкция) определяет требования к организации защиты информационной системы персональных данных Контрольно-счетной палаты города Таганрога (далее также ИСПДн, Палата) от разрушающего воздействия компьютерных вирусов и другого вредоносного программного обеспечения.

2. Требования настоящей Инструкции распространяются на всех работников Палаты, являющихся пользователями ИСПДн Палаты.

3. В целях закрепления знаний по вопросам практического исполнения требований настоящей Инструкции, разъяснения возникающих вопросов администратором информационной безопасности ИСПДн при необходимости могут проводится семинары и персональные инструктажи пользователей ИСПДн Палаты.

4. Ознакомление пользователей ИСПДн Палаты с настоящей Инструкции в части их касающейся осуществляет администратор информационной безопасности ИСПДн Палаты под подпись в листе ознакомления с выдачей копий настоящей Инструкции непосредственно для повседневного использования в работе.

2. Применение средств антивирусной защиты

5. Антивирусный контроль дисков и файлов ИСПДн Палаты после загрузки компьютера должен проводиться в автоматическом режиме (периодическое сканирование или мониторинг).

6. Периодически, не реже одного раза в неделю, должен проводиться полный антивирусный контроль всех дисков и файлов ИСПДн Палаты (сканирование).

7. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая информация по телекоммуникационным каналам связи, на съемных носителях (магнитных дисках, CD-ROM и т.п.).

8. Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема.

Контроль исходящей информации необходимо проводить непосредственно перед отправкой (записью на съемный носитель).

9. Установка (обновление и изменение) системного и прикладного программного обеспечения осуществляется в соответствии с Инструкцией по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационной системы персональных данных Контрольно-счетной палаты города Таганрога.

10. Обновление антивирусных баз должно проводиться регулярно, но не реже, чем 1 раз в неделю.

3. Функции администратора информационной безопасности ИСПДн Палаты

11. Администратор информационной безопасности ИСПДн Палаты обязан:

1) проводить при необходимости инструктажи пользователей ИСПДн Палаты по вопросам применения средств антивирусной защиты;

2) настраивать параметры средств антивирусного контроля в соответствии с руководствами по применению конкретных антивирусных средств;

3) предварительно проверять устанавливаемое (обновляемое) программное обеспечение на отсутствие вирусов;

4) производить обновление антивирусных программных средств при необходимости;

5) производить получение и рассылку (при необходимости) обновлений антивирусных баз;

6) разрабатывать (при необходимости) инструкции по работе пользователей с программными средствами и системой антивирусной защиты;

7) проводить работы по обнаружению и обезвреживанию вирусов;

8) участвовать в работе комиссии по расследованию причин заражения персональных электронно-вычислительных машин и серверного оборудования;

9) хранить эталонные копии антивирусных программных средств;

10) осуществлять периодический контроль за соблюдением пользователями персональных электронно-вычислительных машин требований настоящей Инструкции;

11) проводить периодический контроль работы программных средств системы антивирусной защиты на персональных электронно-вычислительных машинах (серверном оборудовании).

4. Функции пользователей ИСПДн Палаты

12. Пользователи ИСПДн Палаты получают по локальной вычислительной сети обновление антивирусных баз, а в случае отсутствия механизмов централизованного распространения антивирусных баз – получают от администратора информационной безопасности ИСПДн Палаты носители с обновлениями антивирусных баз и проводят обновления антивирусных баз на персональных электронно-вычислительных машинах.

13. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь ИСПДн Палаты должен :

привлечь администратора информационной безопасности ИСПДн для определения факта наличия или отсутствия компьютерного вируса;

самостоятельно или вместе с администратором информационной безопасности ИСПДн Палаты провести внеочередную антивирусную проверку персональной электронно-вычислительной машины пользователя ИСПДн Палаты.

14. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь ИСПДн Палаты обязан:

приостановить работу;

немедленно поставить в известность о факте обнаружения зараженных вирусом файлов своего непосредственного руководителя и администратора информационной безопасности ИСПДн Палаты, владельца зараженных файлов, а также иных работников Палаты использующих эти файлы в работе;

провести анализ необходимости дальнейшего их использования;

провести лечение или уничтожение зараженных файлов (при необходимости для совершения указанных действий привлечь администратора информационной безопасности ИСПДн Палаты);

по факту обнаружения зараженных вирусом файлов составить служебную записку на имя администратора информационной безопасности ИСПДн Палаты, в которой указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации и выполненные антивирусные мероприятия.

Приложение 6
к приказу председателя
Контрольно-счетной палаты
города Таганрога от
от _____ № ____

ИНСТРУКЦИЯ
по организации парольной защиты в информационной системе персональных данных Контрольно-счетной палаты города Таганрога

1. Общие положения

1. Инструкция по организации парольной защиты в информационной системе персональных данных Контрольно-счетной палаты города Таганрога (далее - Инструкция) определяет порядок организации парольной защиты в информационной системе персональных данных Контрольно-счетной палаты города Таганрога (далее также ИСПДн, Палата) и включает в себя взаимоувязанный комплекс организационно-технических мер, регламентирующих генерацию и/или выбор, использование, хранение, уничтожение парольной информации в ИСПДн Палаты.

2. Требования настоящей Инструкции являются неотъемлемой частью комплекса мер безопасности и защиты информации в Палате.

3. Требования настоящей Инструкции распространяются на всех пользователей ИСПДн Палаты, использующих все виды программного обеспечения, эксплуатируемого Палатой.

4. Ознакомление с требованиями настоящей Инструкции пользователей ИСПДн Палаты осуществляет администратор информационной безопасности ИСПДн под подпись в листе ознакомления с выдачей копий настоящей Инструкции непосредственно для повседневного использования в работе.

5. В целях закрепления знаний по вопросам практического исполнения требований настоящей Инструкции, разъяснения возникающих вопросов, проводятся (при необходимости) персональные инструктажи пользователей ИСПДн Палаты.

2. Функции работников Палаты

6. Пользователи ИСПДн Палаты обязаны:

осуществлять смену используемой в работе парольной информации, с частотой, установленной настоящей Инструкцией ;

выбирать парольную информацию с качеством, установленным настоящей Инструкцией.

7. Администратор информационной безопасности ИСПДн Палаты обязан :

осуществлять организационно-методическое обеспечение процессов генерации, смены и удаления паролей в ИСПДн Палаты;

разрабатывать необходимые инструкции по вопросам парольной защиты ИСПДн Палаты;

доводить до пользователей ИСПДн Палаты требования по парольной защите;

организовывать периодический и выборочный контроль исполнения работниками Палаты требований настоящей Инструкции;

согласовывать выдачу управляющих учетных записей к ИСПДн Палаты;

осуществлять текущий контроль действий работников Палаты по работе с паролями (автоматизированный контроль качества паролей – при наличии программно-технических средств);

осуществлять техническое обеспечение процессов генерации/выбора, смены и удаления паролей (при наличии программно-технических средств).

3. Качество и обращение парольной информации

8. Пароли доступа к электронно-вычислительным машинам, к информации находящейся в ИСПДн Палаты формируются (выбираются) пользователями этих ресурсов с учетом следующих требований к качеству парольной информации:

№ пп	Параметр качества пароля	Администратор	Пользователь
1	Минимальная длина пароля в символах	10	8[1]
2	Максимальная длина пароля в символах	32	16
3	Содержание в пароле букв верхнего и нижнего регистра	да	да
4	Содержание в пароле специальных символов (@, #, $, &, * и т.п.) и цифр	обязательно	рекомендуется
5	Содержание в пароле личных имен, фамилий, кличек домашних животных, № телефонов, дат рождения, географических названий, именований АРМ и т.п.	нет	нет
6	Содержание в пароле общепринятых сокращений (ПЭВМ, ЛВС, USER, SYSOP и т.д.)	нет	нет
7	Минимальное отличие нового пароля от предыдущего (в позициях)	3	3
8	Максимальный срок действия пароля	30 дней	60 дней
9	Минимальный срок действия пароля	нет	нет
10	Дополнительный идентификатор (типа ТМ, eToken[2] или другие электронные ключи)	рекомендуется	рекомендуется
11	Пароль на заставку монитора	да	да

10. Хранение работником Палаты личных паролей допускается только в личном сейфе (запираемом шкафу, запираемом ящике), либо в сейфе (запираемом шкафу, запираемом ящике) администратора информационной безопасности, либо в сейфе (запираемом шкафу, запираемом ящике) непосредственного руководителя (при наличии).

При этом бумажный носитель должен быть упакован в отдельный опечатанный конверт.

11. Работники Палаты не вправе сообщать и(или) передавать каким-либо лицам личные пароли и/или дополнительные идентификаторы (электронные ключи).

Работники Платы раскрывают значение своего пароля и/или передают физический идентификатор только своим непосредственным руководителям и только в случае служебной необходимости и/или при проведении контрольно-проверочных мероприятий. По прекращению служебной необходимости/завершению контрольно-проверочных мероприятий, работники производят немедленную смену значений раскрытых паролей.

12. Внеплановая смена/удаление пароля (и при возможности учетной записи) работника Палаты в случае прекращения его полномочий должна производиться немедленно после окончания последнего сеанса работы данного пользователя с системой.

Внеплановая полная смена паролей должна производиться в случае прекращения полномочий администратора информационной безопасности ИСПДн, другими работниками Палаты, которым по роду работы были предоставлены либо полномочия по управлению ИСПДн Палаты, либо полномочия по управлению подсистемой защиты информации ИСПДн Палаты[3].

---

[1] При использовании электронных ключей (USB, Touch Memory) не менее 6 символов.

[2] При использовании электронного ключа такого типа требования вышеприведенной таблицы актуальны только по пунктам №1 и №9.

[3] Смена паролей производится для учетных записей систем, в которых не используется

13. В случае компрометации пароля доступа в ИСПДн Палаты администратором информационной безопасности ИСПДн Палаты должны быть немедленно предприняты меры в зависимости от полномочий владельца скомпрометированного пароля и обстоятельств компрометации.

14. Администратор информационной безопасности ИСПДн Палаты, по согласованию с лицом, ответственным за организацию обработки персональных данных в Палате и при его непосредственном участии, проводит ежеквартальный выборочный контроль выполнения работниками Палаты требований настоящей Инструкции.

15. О фактах несоответствия качества паролей и/или условий обеспечения их сохранности администратор информационной безопасности ИСПДн Палаты докладывает лицу, ответственному за организацию обработки персональных данных в Палате.

4. Обращение дополнительных идентификаторов

16. В целях усиления процедур идентификации и аутентификации в ИСПДн Палаты, пользователи ИСПДн Палаты должны использовать дополнительные индивидуальные электронные идентификаторы (смарт-карты, eToken и т.д.) совместно с личным паролем доступа.

17. Дополнительные идентификаторы выдаются и учитываются в соответствии с утвержденным председателем Палаты перечнем лиц, осуществляющих в Палате обработку персональных данных, с учетом следующих требований:

работники Палаты получают дополнительные идентификаторы под подпись;

администратор информационной безопасности ИСПДн Палаты регистрирует дополнительные идентификаторы в ИСПДн Палаты и инструктирует работников Палаты с учетом требований настоящей Инструкции и правил эксплуатации дополнительных идентификаторов.

18. Работники Палаты, получившие в пользование дополнительные идентификаторы, лично обеспечивают надежное круглосуточное безопасное хранение и использование идентификаторов. Оставление идентификатора без присмотра запрещается.

19. В случае утраты дополнительного идентификатора работники немедленно ставят об этом в известность администратора информационной безопасности ИСПДн Палаты, который организует немедленную блокировку утерянных ключей, и своего непосредственного руководителя.

5. Ответственные за организацию и контроль выполнения порядка

20. Ответственность за соблюдение требований настоящей Инструкции возлагается на всех работников Палаты, участвующих в обработке персональных данных

21. Ответственность за организацию проверочных мероприятий по вопросам парольной защиты возлагается на администратора информационной безопасности ИСПДн Палаты.

аутентификация посредством дополнительных идентификаторов (Touch Memory, eToken и т.п.)

Приложение 7
к приказу председателя
Контрольно-счетной палаты
города Таганрога от
от _____ № ____

ИНСТРУКЦИЯ
по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационной системы персональных данных Контрольно-счетной палаты города Таганрога

1. Общие положения

1. Инструкция по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационной системы персональных данных Контрольно-счетной палаты города Таганрога (далее – Инструкция) определяет комплекс организационно-технических мер по проведению работ по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационной системы персональных данных Контрольно-счетной палаты города Таганрога (далее также ИСПДн, Палата).

2. Требования настоящей Инструкции распространяются на всех работников Палаты, использующих в работе ИСПДн Палаты.

3. Работники Палаты, задействованные в обеспечении функционирования ИСПДн Палаты, знакомятся с настоящей Инструкцией в части, их касающейся, по мере необходимости.

4. Ознакомление с требованиями Инструкции пользователей ИСПДн Палаты осуществляет администратор информационной безопасности ИСПДн под подпись в листе ознакомления с выдачей копий настоящей Инструкции непосредственно для повседневного использования в работе.

5. Непосредственное исполнение настоящей Инструкции определяется администратором информационной безопасности ИСПДн Палаты по согласованию с лицом, ответственным за организацию обработки персональных данных в Палате.

2. Порядок проведения работ

6. Все изменения конфигурации технических и программных средств персональных электронно-вычислительных машин и серверного оборудования, входящих в состав аттестованных по требованиям безопасности ИСПДн Палаты, должны производиться только на основании заявки по форме Приложения 1 к настоящей должностной инструкции, согласованной с председателем Палаты.

7. В заявке указываются наименование персональной электронной вычислительной машины (ПЭВМ) и работник Палаты, за которым она закреплена.

8. После согласования заявки председателем Палаты, она передается администратору информационной безопасности ИСПДн Палаты для исполнения работ по внесению изменений в конфигурацию персональной электронно-вычислительной машины или серверного оборудования.

9. Внесение изменений в конфигурацию аппаратно-программных средств персональной электронно-вычислительной машины осуществляется администратором информационной безопасности ИСПДн Палаты.

Изменение конфигурации аппаратно-программных средств электронно-вычислительной машины и серверного оборудования кем-либо без согласования с администратором информационной безопасности ИСПДн Палаты и(или) лицом, ответственным за организацию обработки персональных данных ЗАПРЕЩЕНО.

9. Установка и настройка программного средства осуществляется администратором

информационной безопасности ИСПДн Палаты согласно эксплуатационной документации.

10. Запрещается установка и использование на персональной электронно-вычислительной машине (серверном оборудовании) программного обеспечения, не входящего в перечень программного обеспечения, разрешенного к использованию в Палате.

11. Установка (обновление) программного обеспечения (системного, тестового и т.п.) производится с эталонных копий программных средств, хранящихся у администратора ИСПДн Палаты. Все добавляемые программные и аппаратные компоненты должны быть предварительно проверены на работоспособность, а также отсутствие компьютерных вирусов и другого вредоносного программного обеспечения в соответствии с Инструкцией по организации антивирусной защиты информационной системы персональных данных Контрольно-счетной палаты города Таганрога.

12. После установки (обновления) программного обеспечения администратор информационной безопасности ИСПДн Палаты должен произвести настройку средств управления доступом к компонентам программного обеспечения в соответствии с требованиями к системе защиты информации и совместно с работником, за которым закреплена персональная электронно-вычислительная машина, проверить правильность настройки средств защиты.

13. В случае обнаружения недекларированных (не описанных в документации) возможностей программного средства, работники незамедлительно информируют об этом администратора информационной безопасности ИСПДн Палаты. Использование программного средства до получения специальных указаний ЗАПРЕЩАЕТСЯ.

14. После завершения работ по внесению изменений в состав аппаратных средств персональной электронно-вычислительной машины, аттестованной по требованиям безопасности ИСПДн Палаты, системный блок должен быть опечатан (опломбирован, защищен специальной наклейкой) администратором информационной безопасности ИСПДн Палаты.

15. При изъятии системного блока из состава персональной электронно-вычислительной машины, аттестованной по требованиям безопасности ИСПДн Палаты, его передача на склад, в ремонт или другому работнику Палаты для решения иных задач осуществляется только после того, как администратор информационной безопасности ИСПДн Палаты снимет с данной персональной электронно-вычислительной машины средства защиты и предпримет необходимые меры для затирания (уничтожения) защищаемой информации, которая хранилась на дисках системного блока. Факт уничтожения данных, находившихся на дисках системного блока, оформляется актом за подписью администратора информационной безопасности ИСПДн по форм, согласно приложению 2 к настоящей Инструкции.

16. Оригиналы заявок, на основании которых производились изменения в составе технических или программных средств персональной электронно-вычислительной машины с отметками о внесенных изменениях, должны храниться у администратора информационной безопасности ИСПДн Палаты.

17. Об осуществленных изменениях необходимо уведомить организацию, производившую аттестацию, в целях принятия ею решения о необходимости проведения контроля эффективности аттестованного объекта информатизации.

18. Все изменения конфигурации технических и программных средств, входящих в состав аттестованных по требованиям безопасности ИСПДн Палаты, отражаются в Техническом паспорте объекта информатизации.

Приложение 1
к Инструкции по установке,модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационной системы персональных данных Контрольно-счетной палаты города Таганрога

(Лицевая сторона заявки)

ЗАЯВКА
на внесение изменений в состав __программного /аппаратного__ обеспечения
(ненужное зачеркнуть)

_____
(наименование персональной электронно-вычислительной машины)

Прошу дать указания работникам Контрольно-счетной палаты города Таганрога ответственным за установку (изменение настроек) программного (аппаратного) обеспечения организовать *установку /изменение настроек):*
(ненужное зачеркнуть)

_____
(перечень программного обеспечения (аппаратных средств) и необходимых настроек)
для решения задач:

_____
_____
_____
_____
следующим пользователям:

_____
(фамилия, имя, отчество)

_____	_____	_____
(наименование должности)	(подпись)	(Фамилия, инициалы)

«___» _____ 20__ г.

Оборотная сторона заявки

Изменения на персональной электронно-вычислительной машине ИСПДн *произведены (не произведены)* по следующей причине:

(ненужное зачеркнуть)

_____

_____

_____

_____

_____

Выполнены следующие работы:

_____

_____

_____

_____

_____

_____

_____

Выполнены следующие изменения в настройках средств защиты:

_____

_____

_____

_____

_____

_____

_____

Администратор информационной безопасности ИСПДн Палаты

«___» _____ 20__ г. _____ _____

(подпись) (фамилия, инициалы)

Приложение 2
к Инструкции по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационной системы персональных данных Контрольно-счетной палаты города Таганрога

АКТ
уничтожения (затирания) остаточной информации,
хранившейся на диске системного блока

Все файлы, содержащие подлежащую защите информацию, находившиеся на НЖМД

_____

(модель, серийный номер)

передаваемого

_____

(с какой целью)

_____

(кому: должность, Ф.И.О.)

_____

(наименование персональной электронно-вычислительной машины)

уничтожены (затерты) посредством программы _____.

Администратор информационной безопасности ИСПДн Палаты

«___» _____ 20__ г. _____ _____
(подпись) (фамилия, инициалы)

Приложение 8

к приказу председателя
Контрольно-счетной палаты
города Таганрога от
от _____ № ____

ИНСТРУКЦИЯ
по учету средств защиты, документации и электронных носителей персональных данных в Контрольно-счетной палате города Таганрога

1. Общие положения

1. Инструкция по учету средств защиты, документации и электронных носителей персональных данных в Контрольно-счетной палате города Таганрога (далее – Инструкция) устанавливает:

1) порядок учета технических средств, участвующих в обработке персональных данных в информационной системе персональных данных Контрольно-счетной палаты города Таганрога (далее также – ИСПДн, Палата);

2) порядок учета, ввода в эксплуатацию и изъятия из употребления средств, используемых для обеспечения безопасности персональных данных при их обработке в ИСПДн Палаты;

3) порядок приема, учета, обработки и хранения документов Палаты, содержащих персональные данные;

4) порядок учета и хранения электронных носителей информации Палаты, содержащих персональные данные (далее – носители с персональными данными).

2. Требования настоящей Инструкции распространяются на всех работников Палаты , являющихся пользователями ИСПДн Палаты.

3. Ознакомление с требованиями настоящей Инструкции администратора информационной безопасности ИСПДн и администратора ИСПДн осуществляет ответственный за организацию обработки персональных данных в Палате под подпись с выдачей копий Инструкции для повседневного использования в работе.

Ознакомление с требованиями настоящей Инструкции иных работников Палаты, являющихся пользователями ИСПДн Палаты, осуществляет администратор информационной безопасности ИСПДн Палаты под подпись с выдачей копий соответствующих разделов настоящей Инструкции для повседневного использования в работе.

2. Порядок учета и хранения средств защиты персональных данных

4. Используемые или хранимые средства защиты персональных данных, эксплуатационная и техническая документация к ним подлежат поэкземплярному учету в Журнале поэкземплярного учета средств защиты персональных данных, эксплуатационной и технической документации к ним (далее – Журнал учета).

При этом программные средства защиты персональных данных должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование.

Если аппаратные или аппаратно-программные средства защиты персональных данных подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие средства защиты персональных данных учитываются также совместно с соответствующими аппаратными средствами.

5. Все полученные экземпляры средств защиты персональных данных, эксплуатационной и технической документации к ним выдаются пользователям средств защиты персональных данных под подпись в Журнале учета.

Пользователи средств защиты несут персональную ответственность за их сохранность.

6. Эксплуатационная и техническая документация, а также электронные носители с инсталляционными файлами средств защиты персональных данных должны храниться в сейфах (запираемых шкафах, запираемых ящиках), исключающих свободный доступ к ним, а также их непреднамеренное уничтожение.

7. Средства защиты персональных данных изымаются из эксплуатации по решению ответственного за организацию обработки персональных данных в Палате. При этом вносятся необходимые изменения в Журнал учета.

8. Если эксплуатация средств защиты персональных данных, намеченных к изъятию, происходит в составе аттестованной ИСПДн Палаты, о прекращении эксплуатации средств защиты персональных данных необходимо уведомить организацию, производившую аттестацию данной ИСПДн.

При этом средства защиты персональных данных считаются изъятыми из эксплуатации, если исполнена предусмотренная эксплуатационной и технической документацией процедура удаления программного обеспечения средств защиты персональных данных и они полностью отсоединены от аппаратных средств.

3. Порядок учета документов, содержащих персональные данные

9. Организация обработки всех поступивших в Палату и отправляемых Палатой документов, содержащих персональные данные, предусмотренные Перечнем персональных данных, обрабатываемых Контрольно-счетной палатой города Таганрога в связи с реализацией служебных и трудовых отношений, а также в связи с осуществлением муниципальных функций Контрольно-счетной палаты города Таганрога, утвержденным приказом председателя Палаты от 10.03.2016 № 10 (далее - Перечень персональных данных), осуществляется лицом, на которое возложены функции делопроизводителя Палаты (далее – делопроизводитель).

10. Регистрации подлежат все документы, требующие учета, исполнения и использования в справочных целях, как создаваемые и используемые внутри Палаты, так и направляемые в другие органы, организации или физическим лицам и поступающие из других органов, организаций или от физических лиц.

11. Регистрация осуществляется делопроизводителем в системе электронного документооборота «Дело» (далее – СЭД «Дело»), путем создания регистрационной карточки в порядке, установленном Инструкцией по делопроизводству в Палате.

12. Содержание поступивших в Палату и отправляемых Палатой документов при их регистрации в СЭД «Дело» анализируется делопроизводителем на предмет содержания персональных данных, предусмотренных Перечнем персональных данных.

Если поступивший в Палату или отправляемый Палатой документ содержит хотя бы одну из позиций Перечня персональных данных, делопроизводитель при его регистрации в СЭД «Дело» определяет категорию доступа к документу как «Персональные данные».

13. Документы, содержащие персональные данные, необходимые для ведения кадровой работы, налогового (в части налога на доходы физических лиц) и персонифицированного учета, осуществления мероприятий в сфере воинского учета, противодействия коррупции, обеспечения требований охраны труда, работники Палаты, в чьи должностные обязанности входит работа с такими документами должны получать непосредственно от субъектов персональных данных на бумажных носителях в виде бумажных документов.

При автоматизации процесса ведения кадрового делопроизводства документы, подлежащие включению в личное дело сотрудника, выводятся на бумажные носители и включаются в личное дело.

На основе представленных субъектами персональных данных документов на бумажных носителях формируются личные дела работников Палаты, составляются личные карточки по формам Т-2 и Т-2ГС(МС), утвержденной постановлением Государственного комитета Российской Федерации по статистике от 05.01.2004 № 1 «Об утверждении унифицированных форм первичной учетной документации по учету труда и его оплаты», карточка гражданина,

подлежащего воинскому учету по форме 10, утвержденной приказом Министра обороны Российской Федерации от 22.11.2021 № 700 «Об утверждении Инструкции об организации работы по обеспечению функционирования системы воинского учета», иные предусмотренные действующим законодательством документы, в том числе реестры, регистры, а также карточки и журналы учета.

4. Порядок учета электронных носителей

15. Учёт электронных носителей персональных данных осуществляется администратором информационной безопасности ИСПДн Палаты.

При смене администратора информационной безопасности ИСПДн Палаты, составляется акт приема-сдачи электронных носителей персональных данных и всех журналов учета, который утверждается лицом, ответственным за обеспечение безопасности и обработки ПДн.

16. Учет электронных носителей персональных данных, а также регистрация выдачи и возврата таких носителей производится в Журнале учета носителей персональных данных в Контрольно-счетной палате города Таганрога.

Выдача электронных носителей персональных данных работнику Палаты производится под его личную подпись.

17. Передача электронных носителей с персональными данными другим работникам, обрабатывающим персональные данные в Палате, производится с обязательной записью в Журнале учета носителей персональных данных в Контрольно-счетной палате города Таганрога.

5. Порядок хранения носителей

18. Документы, дела и другие носители информации с персональными данными (далее – носители персональных данных) должны храниться в служебных помещениях в сейфе (запираемом шкафу, запираемом ящике). При этом должны быть созданы надлежащие условия, обеспечивающие их физическую сохранность.

19. Запрещается выносить носители персональных данных из служебных помещений за пределы Палаты для работы с ними на дому, в гостиницах и т.д.

В необходимых случаях лицо, ответственное за организацию обработки персональных данных может разрешить исполнителям вынос за пределы Палаты носителей персональных данных для их согласования, подписи и т.п.

20. После окончания работы работники Палаты, допущенные к работе с персональными данными, должны запирать носители персональных данных в сейф (запираемый шкаф, запираемый ящик).

21. Проверка наличия носителей персональных данных проводится один раз в год постоянно действующей комиссией Палаты по контролю защищенности персональных данных

Проверка наличия носителей персональных данных при необходимости также может быть проведена администратором информационной безопасности ИСПДн, лицом, ответственным за организацию обработки персональных данных или председателем Палаты.

Раз в год постоянно действующая экспертная комиссия Палаты при проведении экспертизы ценности документов, определяет перечень носителей персональных данных с истекшим сроком хранения, которые подлежат уничтожению.

22. Уничтожение носителей персональных данных осуществляется в порядке, установленном главой 12 Правил обработки персональных данных в Контрольно-счетной палате города Таганрога, утвержденными приказом председателя Палаты от 10.03.2016 № 10.

6. Ответственные за выполнение инструкции

23. На пользователей ИСПДн Палаты, возлагается персональная ответственность за выполнение всех обязанностей, предусмотренных настоящей Инструкцией.

24. Пользователи ИСПДн Палаты несут ответственность за нарушение, настоящей Инструкции, совершенные в процессе своей деятельности, в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.

Приложение 9
к приказу председателя
Контрольно-счетной палаты
города Таганрога от
от _____ № ____

ИНСТРУКЦИЯ
по действиям пользователей информационной системы персональных данных Контрольно-счетной палаты города Таганрога в нештатных ситуациях

1. Общие положения

1. Инструкция по действиям пользователей информационной системы персональных данных Контрольно-счетной палаты города Таганрога в нештатных ситуациях (далее – Инструкция) определяет порядок действий пользователей информационной системы персональных данных Контрольно-счетной палаты города Таганрога (далее также ИСПДн, Палата) при возникновении нештатных ситуаций.

2. В случае возникновения нештатной ситуации, при наступлении которой порядок действий не регламентирован настоящей Инструкцией администратором информационной безопасности ИСПДн Палаты совместно с лицом, ответственным за организацию обработки персональных данных в Палате вырабатывается конкретный план действий с учетом текущей ситуации.

3. Требования настоящей Инструкции распространяются на всех работников Палаты, являющихся пользователями ИСПДн Палаты.

4. Для эффективной реализации мероприятий по реагированию в случае нештатных ситуаций администратором информационной безопасности ИСПДн Палаты проводятся регулярные инструктажи по действиям в различных нештатных ситуациях.

5. Ознакомление пользователей ИСПДн Палаты с настоящей Инструкцией в части их касающейся осуществляет администратор информационной безопасности ИСПДн Палаты под подпись в листе ознакомления с выдачей копий настоящей Инструкции непосредственно для повседневного использования в работе.

2. Нештатные ситуации и их классификация

6. Нештатными ситуациям для целей настоящей инструкции признаются:

1) разглашение информации ограниченного доступа, не составляющей государственную тайну (далее – защищаемая информация) работниками Палаты, как имеющими к ней право доступа, так и не имеющими такового (далее – внутренний злоумышленник), в том числе:

передача защищаемой информации по открытым линиям связи;

обработка защищаемой информации на незащищенных технических средствах обработки информации;

опубликование защищаемой информации в открытой печати и других средствах массовой информации;

передача носителя информации лицу, не имеющему права доступа к ней;

утрата носителя с защищаемой информацией;

2) неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации, а именно:

несанкционированное изменение защищаемой информации;

несанкционированное копирование защищаемой информации;

3) несанкционированный доступ к защищаемой информации сторонних лиц (внешний злоумышленник), а именно:

подключение технических средств к средствам и системам Палаты;

использование закладочных устройств;

маскировка под зарегистрированного пользователя;
использование дефектов программного обеспечения Палаты;
использование программных закладок;
применение программных вирусов;
хищение носителя защищаемой информации;
нарушение функционирования технических средств обработки информации;
блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку;

4) дефекты, сбои, отказы, аварии технических средств и систем Палаты;

5) дефекты, сбои и отказы программного обеспечения Палаты;

6) сбои, отказы и аварии систем обеспечения Палаты;

7) природные явления, стихийные бедствия, в том числе:
термические, климатические факторы (пожары, наводнения и т.д.);
механические факторы (землетрясения, оползни и т.д.);
электромагнитные факторы (грозовые разряды и т.д.).

7. Нештатные ситуации классифицируются в соответствии с оценками, представленными в таблице .

Таблица

Нештатная ситуация		Оценка ситуации	Порядок действий (пункты Инструкции)
Разглашение защищаемой информации сотрудниками, имеющими к ней право доступа			9
Неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации	Несанкционированное копирование защищаемой информации	Обнаружился случившийся факт	9
		Производится в текущий момент	10
	Несанкционированное изменение защищаемой информации	Обнаружился случившийся факт	9
		Производится в текущий момент	10
Несанкционированный доступ к защищаемой информации	Подключение технических средств к средствам и системам Палаты	Обнаружился случившийся факт	9
		Производится в текущий момент	11
	Установка закладочных устройств	Обнаружение установленных	9
		Устанавливаются в настоящий момент	12
	Маскировка под зарегистрированного пользователя	Внешним злоумышленником в текущий момент	13
		Внутренним злоумышленником, либо производилась в прошлом	9
	Использование дефектов программного обеспечения Палаты	Внешним злоумышленником в текущий момент	14
		Внутренним злоумышленником, либо производилось в прошлом	9
	Использование программных закладок	Внешним злоумышленником в текущий момент	15
		Внутренним злоумышленником, либо производилось в прошлом	9
	Обнаружение программных вирусов		16

	Хищение носителя защищаемой информации		9
	Нарушение функционирования технических средств обработки информации злоумышленником	Производится в текущий момент	17
		Обнаружился случившийся факт	18
	Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку	Производится в текущий момент внешним злоумышленником	19
		Производится в текущий момент внутренним злоумышленником	20
		Обнаружился случившийся факт	21
Ошибки пользователей системы при эксплуатации программных средств, технических средств, средств и систем защиты информации		Ошибка повлекла утрату или повреждение защищаемой информации	22
		Ошибка привела к нарушению работоспособности технических средств и программного обеспечения	23
Дефекты, сбои, отказы, аварии технических средств, программных средств и систем Палаты			24
Сбои, отказы и аварии систем обеспечения Палаты			25
Природные явления, стихийные бедствия	Несущие угрозу жизни человека		26
	Не несущие угрозу жизни человека		27

3. Порядок действий в нештатных ситуациях

8. Порядок оповещения должностных лиц Палаты и сроки выполнения мероприятий при нештатных ситуациях определены в приложении к настоящей Инструкции.

9. В случае возникновения нештатной ситуации, которая повлекла утечку или повреждение защищаемой информации, либо создана внутренним злоумышленником:

1) администратор информационной безопасности ИСПДн Палаты осуществляет сбор и обеспечение сохранности улик незаметно для злоумышленника при нештатных ситуациях, связанных с:

разглашением защищаемой информации;

обнаружением несанкционированно скопированной или измененной защищаемой информации;

обнаружением подключения технических средств к средствам и системам Палаты;

обнаружением закладочных устройств;

маскировкой под зарегистрированного пользователя внутренним злоумышленником или обнаружением факта маскировки в прошлом (как внутренним, так и внешним злоумышленником);

использованием дефектов программного обеспечения Палаты внутренним злоумышленником или обнаружением факта их использования в прошлом (как внутренним, так и внешним злоумышленником);

использованием программных закладок внутренним злоумышленником или обнаружением факта их использования в прошлом (как внутренним, так и внешним злоумышленником);

хищением носителя защищаемой информации;

2) для расследования соответствующей нештатной ситуации создается комиссия, которая дополнительно к общему порядку действий, предусмотренному разделом 4 настоящей Инструкции:

определяет, при наличии возможности, организации, в которые произошла утечка защищаемой информации;

определяет возможные меры, призванные уменьшить ущерб от утечки информации.

10. В случае обнаружения злоумышленника неправомерно копирующего, либо изменяющего защищаемую информацию;

1) администратор информационной безопасности ИСПДн Палаты:

прерывает несанкционированный процесс;

блокирует доступ к ИСПДн Палаты для злоумышленника;

удаляет совместно с лицом, ответственным за организацию обработки персональных данных в Палате, нарушителя от средств ИСПДн Палаты;

2) администратор информационной безопасности ИСПДн Палаты совместно с лицом, ответственным совместно с лицом, ответственным за организацию обработки персональных данных в Палате, предпринимает действия по сбору и обеспечению сохранности улик;

3) для расследования соответствующей нештатной ситуации создается комиссия.

11. В случае обнаружения злоумышленника, производящего подключение к техническим средствам и системам Палаты в текущий момент времени:

1) администратор информационной безопасности ИСПДн Палаты:

прерывает процесс работы злоумышленника;

блокирует доступ к ИСПДн Палаты для нарушителя, в случае если нарушителем является пользователь ИСПДн Палаты;

2) для расследования соответствующей нештатной ситуации создается комиссия.

12. В случае обнаружения злоумышленника, устанавливающего закладочные устройства:

1) администратор информационной безопасности ИСПДн Палаты принимает меры к установлению личности злоумышленника, а также готовит обращение в правоохранительные органы;

2) для расследования соответствующей нештатной ситуации создается комиссия.

13. В случае обнаружения внешнего злоумышленника маскирующегося под зарегистрированного пользователя:

1) администратор информационной безопасности ИСПДн Палаты блокирует доступ к ИСПДн Палаты для злоумышленника;

2) для расследования соответствующей нештатной ситуации создается комиссия.

14. В случае обнаружения использования дефектов программного обеспечения Палаты внешним нарушителем в текущий момент времени:

1) администратор информационной безопасности ИСПДн Палаты блокирует доступ из внешних сетей к оборудованию, на котором используется уязвимое программное обеспечение;

2) для расследования соответствующей нештатной ситуации создается комиссия.

15. В случае обнаружения использования программной закладки внешним нарушителем в текущий момент времени администратор информационной безопасности ИСПДн Палаты:

блокирует доступ из внешних сетей к оборудованию, на котором установлена программная закладка;

определяет возможный ущерб, нанесенный программной закладкой;

проводит мероприятия по обнаружению внедренных программных закладок и их нейтрализации;

планирует и организует мероприятия по предотвращению повторения, нейтрализации последствий нештатной ситуации;

составляет акт об инциденте.

16. В случае обнаружения программных вирусов выполняются действия предусмотренные Инструкцией по организации антивирусной защиты информационной системы персональных данных Контрольно-счетной палаты города Таганрога.

17. В случае обнаружения злоумышленника нарушающего функционирование технических средств обработки информации в текущий момент времени:

1) администратор информационной безопасности ИСПДн Палаты:

принимает меры по немедленному удалению злоумышленника от средств вычислительной техники;

блокирует доступ к ИСПДн Палаты для злоумышленника, в случае если злоумышленник является пользователем ИСПДн Палаты;

определяет ущерб, нанесенный техническим средствам и информации, в случае наличия повреждений;

производит восстановление работоспособности системы;

2) для расследования соответствующей нештатной ситуации создается комиссия.

18. В случае обнаружения нарушений в функционировании технических средств Палаты:

1) администратор информационной безопасности ИСПДн Палаты

определяет возможный круг лиц, причастных к нарушению функционирования технических средств;

определяет объем повреждений техническим средствам и информации;

производит восстановление работоспособности системы;

2) для расследования соответствующей нештатной ситуации создается комиссия.

19. В случае обнаружения внешней атаки, направленной на блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку в текущий момент времени администратор информационной безопасности ИСПДн Палаты:

1) выявляет источник ложных заявок;

2) вырабатывает решение по блокированию потока ложных заявок и реализует выбранное решение;

3) уведомляет провайдера, от которого идут ложные заявки, планирует и организует мероприятия по предотвращению повторения, нейтрализации последствий инцидента;

4) составляет акт об инциденте.

20. В случае обнаружения внутренней атаки, направленной на блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку в текущий момент времени:

1) администратор информационной безопасности ИСПДн Палаты выявляет источник ложных заявок и блокирует доступ к ИСПДн Палаты для злоумышленника;

2) создается комиссия для расследования инцидента.

21. При обнаружении факта блокировки доступа к защищаемой информации, произошедшей в прошлом:

1) администратор информационной безопасности ИСПДн Палаты:

выявляет источник ложных заявок;

уведомляет провайдера, от которого идут ложные заявки, планирует и организует мероприятия по предотвращению повторения, нейтрализации последствий инцидента, и оставляет акт об инциденте, в случае если злоумышленник является внешним;

2) создается комиссия для расследования инцидента.

22. В случае обнаружения ошибок пользователей системы при эксплуатации технических средств, программных средств, средств и систем защиты информации, повлекшие утрату или повреждение защищаемой информации:

1) выполняется последовательность действий, предусмотренная настоящей Инструкции для соответствующих нештатных ситуаций, в случае возможности злоумышленных действий;

2) проводится проверка знаний работника Палаты, виновного в инциденте, а в случае необходимости – также его обучение;

3) администратор информационной безопасности ИСПДн Палаты:

проводит анализ и идентификацию причин инцидента;

определяет ущерб, нанесенный нештатной ситуацией;

проводит мероприятия по восстановлению работоспособности системы и информации;

составляет акт об инциденте;

вносит предложение председателю Палаты о применении дисциплинарного взыскания в отношении нарушителя (при необходимости).

23. В случае обнаружения ошибок пользователей системы при эксплуатации технических средств, программных средств, средств и систем защиты информации, повлекшие нарушение работоспособности технического средства и программного обеспечения:

1) выполняется последовательность действий, предусмотренная настоящей Инструкции для соответствующих нештатных ситуаций, в случае возможности злоумышленных действий;

2) проводится проверка знаний работника виновного в инциденте, а в случае необходимости – также его обучение.

3) администратор информационной безопасности ИСПДн Палаты:

проводит анализ и идентификацию причин инцидента (при необходимости);

определяет ущерб, нанесенный нештатной ситуацией, восстанавливает работоспособность системы:

составляет акт об инциденте

вносит предложение председателю Палаты о применении дисциплинарного взыскания в отношении нарушителя (при необходимости).

24. В случае возникновения дефектов, сбоев, отказов, аварий технических средств и систем Палаты:

1) выполняется порядок действий в соответствии с Приложением к настоящей Инструкции, в случае наличия злоумышленных действий;

2) администратор информационной безопасности ИСПДн Палаты:

выявляет возможные причины появления дефектов, сбоев, отказов, аварий;

восстанавливает работоспособность систем;

в случае потери данных по возможности проводит восстановление их из резервных копий;

составляет акт об инциденте.

25. В случае сбоев, отказов и аварий систем обеспечения Палаты (электроснабжения, вентиляции, других обеспечивающих инженерных систем) администратор информационной безопасности ИСПДн Палаты:

1) производит отключение технических средств до момента истечения резервов системы бесперебойного питания при продолжительном отключении электроснабжения Палаты;

2) в случае потери защищаемых данных по возможности проводит восстановление их из резервных копий;

3) составляет акт об инциденте.

26. В случае возникновения нештатной ситуации, вызванной стихийным бедствием, природным явлением, которые несут угрозу жизни человека:

1) работники Палаты:

предпринимают максимально возможные меры по обеспечению сохранности личных реквизитов защиты (например: металлические и/или электронные ключи, карты-идентификаторы, ключевые дискеты, печати и пр.) во время эвакуации;

обеспечивают выключение персональных электронно-вычислительных машин;

2) администратор информационной безопасности ИСПДн Палаты:

выключает серверное и сетевое оборудование;

принимает меры к эвакуации резервных копий с информацией.

27. В случае возникновения нештатной ситуации, вызванной стихийным бедствием, природным явлением, которые не несут угрозу жизни человека:

1) работники Палаты выключают свои электронно-вычислительные машины;

2) администратор информационной безопасности ИСПДн:

выключает серверное и сетевое оборудование;

принимает меры к эвакуации резервных копий с информацией, системных блоков компьютеров, содержащих особо ценную информацию, документов и другого имущества;

3) пользователи ИСПДн Палаты принимают меры по обеспечению сохранности личных реквизитов защиты (например: металлические и/или электронные ключи, карты-идентификаторы, ключевые дискеты, печати и пр.).

4. Проведение расследований

28. Для расследования нештатных ситуаций в случаях, предусмотренных настоящей Инструкцией создается комиссия, в состав которой, как правило, входят:

председатель Палаты;

лицо, ответственное за организацию обработки персональных данных;

администратор информационной безопасности ИСПДн Палаты;

другие лица по решению председателя Палаты.

29. При проведении расследования комиссия осуществляет:

анализ и идентификацию причин инцидента, определение лиц, виновных в нештатной ситуации;

определение ущерба, нанесенного нештатной ситуацией;

планирование мер для предотвращения повторения, нейтрализации последствий (при наличии возможности);

анализ и сохранение следов инцидента, доказательств, улик и свидетельств. При сохранении улик, при наличии возможности, администратором информационной безопасности ИСПДн Палаты производится резервное копирование системной и защищаемой информации, вовлеченной в инцидент;

определение возможной меры взыскания с виновного;

взаимодействие с правоохранительными органами (при необходимости).

30. При проведении расследований, комиссия также подготавливает ответы на следующие вопросы:

можно ли было предупредить нештатную ситуацию?

вызвана ли она слабостью средств защиты?

является ли нештатная ситуация такого рода первой?

достаточно ли имеющегося резерва?

есть ли необходимость пересмотра системы защиты?

есть ли необходимость пересмотра настоящей Инструкции?

31. По результатам деятельности комиссии составляется акт с описанием ситуации. К акту прилагаются материалы расследования (копии экрана, распечатки журнала событий и др.).

32. По результатам расследования администраторами организуются мероприятия по реализации предложенных комиссией мер для предотвращения либо уменьшения вероятности проявления подобных инцидентов в дальнейшем.

5. Ответственные за контроль выполнения инструкции

33. Ответственными за контроль выполнения требований настоящей Инструкции являются:

администратор информационной безопасности ИСПДн Палаты в части задач, возложенных на него настоящей Инструкцией;

ответственный за организацию обработки персональных данных в части общего контроля информационной безопасности.

Приложение
к Инструкции по действиям пользователей
информационной системы персональных данных
Контрольно-счетной палаты города Таганрога
в нештатных ситуациях

План обеспечения непрерывной работы и восстановления информации

Тип нештатной ситуации	Критерии нештатной ситуации	Кому и в какие сроки докладывается		Срок реализации первоочередных действий	Максимальное время для выполнения всех мероприятий
		В рабочее время	В нерабочее время		
Неправомерные действия со стороны лиц допущенных к защищаемой информации					
Разглашение защищаемой информации сотрудниками, имеющими к ней право доступа		Администратору информационной безопасности ИСПДн Палаты сразу после обнаружения инцидента	Администратору информационной безопасности ИСПДн Палаты как можно скорее, в дневное время, но не позднее 8 часов после инцидента		
Обнаружение несанкционированно скопированной или измененной конфиденциальной информации		Администратору информационной безопасности ИСПДн Палаты сразу после обнаружения инцидента	Администратору информационной безопасности ИСПДн Палаты как можно скорее, в дневное время, но не позднее 8 часов после инцидента		
Несанкционированное копирование или изменение конфиденциальной информации в текущий момент времени со стороны лиц имеющих право доступа к ней		Администратору информационной безопасности ИСПДн Палаты сразу после обнаружения инцидента	Администратору информационной безопасности ИСПДн Палаты сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	
Несанкционированный доступ к информации					
Обнаружение подключения технических средств к средствам и системам Палаты		Администратору информационной безопасности ИСПДн Палаты сразу после обнаружения инцидента	Администратору информационной безопасности ИСПДн Палаты как можно скорее, в дневное время, но не позднее 8 часов после инцидента		

Подключение технических средств к средствам и системам ОИ в текущий момент времени		Администратору информационной безопасности ИСПДн Палаты сразу после обнаружения инцидента	Администратору информационной безопасности ИСПДн Палаты сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	
Обнаружение закладочных устройств		Администратору информационной безопасности ИСПДн Палаты сразу после обнаружения инцидента	Администратору информационной безопасности ИСПДн Палаты как можно скорее, в дневное время, но не позднее 8 часов после инцидента		
Установка закладочных устройств злоумышленником в текущий момент времени		Администратору информационной безопасности ИСПДн Палаты сразу после обнаружения инцидента	Администратору информационной безопасности ИСПДн Палаты сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	
Маскировка под зарегистрированного пользователя внешним злоумышленником в текущий момент времени		Администратору информационной безопасности ИСПДн Палаты сразу после обнаружения инцидента	Администратору информационной безопасности ИСПДн Палаты сразу после обнаружения инцидента	5 минут в рабочее время (1 час в нерабочее)	
Маскировка под зарегистрированного пользователя внутренним злоумышленником или обнаружением факта маскировки		Администратору информационной безопасности ИСПДн Палаты сразу после обнаружения инцидента	Администратору информационной безопасности ИСПДн Палаты как можно скорее, в дневное время, но не позднее 8 часов после инцидента		
Использование дефектов программного обеспечения ОИ внешним нарушителем в текущий момент времени		Администратору информационной безопасности ИСПДн Палаты сразу после обнаружения инцидента	Администратору информационной безопасности ИСПДн Палаты сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	
Использование программных закладок внешним нарушителем в текущий момент времени		Администратору информационной безопасности ИСПДн Палаты сразу после обнаружения инцидента	Администратору информационной безопасности ИСПДн Палатысразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	

Использование программных закладок внутренним злоумышленником или обнаружение факта использования		Администратору информационной безопасности ИСПДн Палаты сразу после обнаружения инцидента	Администратору информационной безопасности ИСПДн Палаты как можно скорее, в дневное время, но не позднее 8 часов после инцидента		
Обнаружение программных вирусов		Администратору информационной безопасности ИСПДн Палаты сразу после обнаружения инцидента	Администратору информационной безопасности ИСПДн Палаты как можно скорее, в дневное время, но не позднее 8 часов после инцидента		12 часов
Хищение носителя защищаемой информации		Администратору информационной безопасности ИСПДн Палаты сразу после обнаружения инцидента	Администратору информационной безопасности ИСПДн Палаты как можно скорее, в дневное время, но не позднее 8 часов после инцидента		
Нарушение функционирования ТС обработки информации в текущий момент времени злоумышленником	Нарушена работа одного пользователя	Администратору информационной безопасности ИСПДн Палаты сразу после обнаружения инцидента	Администратору информационной безопасности ИСПДн Палаты сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	2 дня
	Нарушена работа группы пользователей	Администратору информационной безопасности ИСПДн Палаты сразу после обнаружения инцидента	Администратору информационной безопасности ИСПДн Палаты сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	1 день
Обнаружение нарушения функционирования ТС обработки информации произведенного злоумышленником	Нарушена работа одного пользователя	Администратору информационной безопасности ИСПДн Палаты сразу после обнаружения инцидента	Администратору информационной безопасности ИСПДн Палаты сразу после обнаружения инцидента		2 дня
	Нарушена работа группы пользователей	Администратору информационной безопасности ИСПДн Палаты сразу после обнаружения инцидента	Администратору информационной безопасности ИСПДн Палаты сразу после обнаружения инцидента		1 день
Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку					

Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку внешним злоумышленником в текущий момент времени		Администратору информационной безопасности ИСПДн Палаты сразу после обнаружения инцидента	Администратору информационной безопасности ИСПДн Палаты как можно скорее, в дневное время, но не позднее 8 часов после инцидента	20 минут в рабочее время (1 час в нерабочее)	7 дней
Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку внутренним злоумышленником в текущий момент времени		Администратору информационной безопасности ИСПДн Палаты сразу после обнаружения инцидента	Администратору информационной безопасности ИСПДн Палаты как можно скорее, в дневное время, но не позднее 8 часов после инцидента	20 минут в рабочее время (1 час в нерабочее)	1 день
Обнаружение произошедшего факта блокировки доступа к защищаемой информации		Администратору информационной безопасности ИСПДн Палаты сразу после обнаружения инцидента	Администратору информационной безопасности ИСПДн Палаты как можно скорее, в дневное время, но не позднее 8 часов после инцидента		1 день
Ошибки пользователей системы					
Ошибки пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие утерю или повреждение защищаемой информации		Администратору информационной безопасности ИСПДн Палаты сразу после обнаружения инцидента	Администратору информационной безопасности ИСПДн Палаты как можно скорее, в дневное время, но не позднее 8 часов после инцидента	2 часа в рабочее время (12 часов в нерабочее)	1 день
Ошибки пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие нарушение работоспособности ТС и ПО	Нарушена работа одного пользователя	Администратору информационной безопасности ИСПДн Палаты сразу после инцидента	Администратору информационной безопасности ИСПДн Палаты в первый рабочий день после инцидента	20 минут	2 дня
	Нарушена работа группы пользователей	Администратору информационной безопасности ИСПДн	Администратору информационной безопасности	20 минут	1 день

		Палаты сразу после обнаружения инцидента	ИСПДн Палаты сразу после обнаружения инцидента		
Объективные факторы					
Дефекты, сбои, отказы, аварии ТС, программных средств и систем ОИ	Сбой технических средств и систем обработки информации	Администратору Администратору информационной безопасности ИСПДн Палаты сразу после инцидента	Администратору Администратору информационной безопасности ИСПДн Палаты сразу после инцидента	1 час	2 дня
	Отказ технических средств и систем обработки информации, затронувший работу группы пользователей	Администратору информационной безопасности ИСПДн Палаты сразу после обнаружения инцидента	Администратору информационной безопасности ИСПДн Палаты как можно скорее, в дневное время, но не позднее 8 часов после инцидента	1 час в рабочее время (8 часов в нерабочее)	1 день
	Отказ технических средств и систем обработки информации, затронувший работу одного пользователя	Администратору информационной безопасности ИСПДн Палаты сразу после инцидента	Администратору информационной безопасности ИСПДн Палаты в первый рабочий день после инцидента	1 час	2 дня
	Авария технических средств и систем обработки информации	Администратору информационной безопасности ИСПДн Палаты сразу после обнаружения инцидента	Администратору информационной безопасности ИСПДн Палаты как можно скорее, в дневное время, но не позднее 8 часов после инцидента	1 час	1 день
Сбои, отказы и аварии систем обеспечения обработки информации	Сбой систем обеспечения обработки информации	Начальнику отдела ПМКиМО сразу после инцидента	Начальнику отдела ПМКиМО в первый рабочий день после инцидента		
	Отказ сисъъъъъъъъем обеспечения обработки информации,	Администратору информационной безопасности ИСПДн Палаты сразу после обнаружения инцидента	Администратору информационной безопасности ИСПДн Палаты сразу после обнаружения инцидента		1 день

	затронувший работу группы пользователей				
	Отказ систем обеспечения обработки информации, затронувший работу одного пользователя	Начальнику отдела ПМКиМО сразу после инцидента	Начальнику отдела ПМКиМО в первый рабочий день после инцидента		2 дня
	Авария систем обеспечения обработки информации	Администратору информационной безопасности ИСПДн Палаты сразу после обнаружения инцидента	Администратору информационной безопасности ИСПДн Палаты как можно скорее, в дневное время, но не позднее 8 часов после инцидента		1 день
Природные явления, стихийные бедствия, несущие угрозу жизни человека		Председателю Контрольно-счетной палаты города Таганрога, заместителям, которые оповещают всех своих сотрудников сразу после получения информации	Председателю Контрольно-счетной палаты города Таганрога, заместителям, которые оповещают всех своих сотрудников сразу после получения информации		30 минут
Природные явления, стихийные бедствия, не несущие угрозу жизни человека		Председателю Контрольно-счетной палаты города Таганрога, заместителю председателя, администратору информационной безопасности ИСПДн Палаты	Председателю Контрольно-счетной палаты города Таганрога, заместителю председателя, администратору информационной безопасности ИСПДн Палаты		30 минут

Приложение 10
к приказу председателя
Контрольно-счетной палаты
города Таганрога от
от _____ № ____

(форма)

ЖУРНАЛ
учета письменных запросов граждан на доступ к своим персональным данным
в Контрольно-счетной палате города Таганрога

№ п/п	Вх. № и дата получения запроса	Фамилия, инициалы гражданина	Сведения о документе, удостоверяющем личность			Отметка о предоставлени и доступа к персональным данным (отказе в доступе)	Исх. № и дата письма с ответом на запрос	Фамилия, инициалы, должность работника, подготовившего ответ на запрос	Примечание
			Серия, номер	Дата выдачи	Кем выдан				
1	2	4	5	6	7	8	9	10	11

Приложение 11
к приказу председателя
Контрольно-счетной палаты
города Таганрога от
от _____ № ____

(форма)

ЖУРНАЛ
учета носителей персональных данных в
Контрольно-счетной палате города Таганрога

№ п\п	Дата регистрации машинного носителя информации, машинного документа	Регистрационный и(или) учетный номер машинного носителя информации, машинного документа, откуда поступил	Тип машинного носителя информации, машинного документа	Количество экземпляров	Номер экземпляра	Количество в экземпляре (штук, листов и др.)	Фамилия, инициалы и подпись лица, получившего машинный носитель информации, машинный документ	Фамилия, инициалы и подпись лица принявшего обратно машинный носитель информации, машинный документ	Место хранения машинного носителя информации, машинного документа	Отметка об уничтожении (складировании в урну) бракованных машинных носителей информации, машинных документов (подпись, дата)	Отметка об уничтожении машинных носителей информации, машинных документов, стирании информации (номер акта и дата)
1	2	3	4	5	6	7	8	9	10	11	12

Приложение 12
к приказу председателя
Контрольно-счетной палаты
города Таганрога от
от _____ № ____

(форма)

ЖУРНАЛ
поэкземплярного учета средств защиты информации, эксплуатационной и технической документации к ним

№ п/п	Наименование средства защиты, эксплуатационной и технической документации	Регистрационный номер средства защиты, эксплуатационной и технической документации	Отметка о выдаче		Отметка о подключении (установке) средства защиты			Отметка об изъятии средства защиты из аппаратных средств	
			Ф.И.О. пользователя средства защиты	Дата и расписка в получении	Ф.И.О. лица (лиц), производившего подключение (установку)	Дата подключения (установки) и подписи лица (лиц), произведших подключение (установку)	Номер ПЭВМ, в которое установлено средство защиты	Ф.И.О. лица (лиц) осуществивших изъятие	Дата изъятия и подпись лица (лиц), осуществивших изъятие
1	2	3	4	5	6	7	8	9	10

Приложение 13
к приказу председателя
Контрольно-счетной палаты
города Таганрога от
от _____ № ____

(форма)

ЖУРНАЛ
учета проведения инструктажей по вопросам защиты информации
в Контрольно-счетной палате города Таганрога

№ п/п	Фамилия, инициалы инструктируемого	Должность инструктируемого с указанием структурного подразделения (при наличии)	Дата проведения инструктажа	Наименование инструкции, в объеме которой проведен инструктаж	Вид инструктажа (в связи с чем проводится)	Фамилия, инициалы инструкти-рующего	Подпись инструкти-рующего	Подпись инструкти-руемого
1	2	3	4		5	6	7	8

Приложение 14
к приказу председателя
Контрольно-счетной палаты
города Таганрога от
от _____ № ____

(форма)

ЖУРНАЛ
учета проведения полного резервного копирования в
Контрольно-счетной палате города Таганрога

№ п/п	Наименование информационной системы персональных данных	Наименование восстанавливаемой защищаемой информации	Средство резервного копирования	Дата и время резервного копирования	Лицо, осуществившее резервное копирование	
					фамилия, инициалы	подпись
1	2	3	4	5	6	7

Приложение 15
к приказу председателя
Контрольно-счетной палаты
города Таганрога от
от _____ № ____

(форма)

ЖУРНАЛ
учета работ по восстановлению защищаемой информации
в информационной системе персональных данных Контрольно-счетной палаты города Таганрога

№ п/п	Наименование информационной системы персональных данных	Наименование восстанавливаемой защищаемой информации	Краткое описание действий по восстановлению	Дата и время восстановления	Лицо, осуществившее восстановление	
					фамилия, инициалы	подпись
1	2	3	4	5	6	7

Приложение 16
к приказу председателя
Контрольно-счетной палаты
города Таганрога от
от _____ № ____

(форма)

ЖУРНАЛ
учета ключевых носителей информации, выданных уполномоченным лицам (работникам)
Контрольно-счетной палаты города Таганрога

№ п/п	Наименование носителя, регистрационный (заводской) номер	Фамилия, имя, отчество, должность, подразделение (при наличии) работника, получившего носитель	Дата получения, работника, получившего носитель	Подпись лица, выдавшего носитель	Дата возврата, подпись работника вернувшего носитель	Отметка об изъятии носителя, дата, подпись лица, изъявшего носитель	Примечание (сетевое имя рабочей станции и т.д.)
1	2	3	4	5	6	7	8

Приложение 17
к приказу председателя
Контрольно-счетной палаты
города Таганрога от
от _____ № ____

(форма)

ЖУРНАЛ
учета нештатных ситуаций в
Контрольно-счетной палате города Таганрога

№ п/п	Дата регистрации нештатной ситуации	Наименование информационной системы персональных данных	Номер ПЭВМ	Краткое описание нештатной ситуации, выполненные работы	Фамилия, инициалы и подпись работника, выявившего нештатную ситуацию	Подпись администратора информационной безопасности
1	2	3	4	5	6	7

Приложение 18
к приказу председателя
Контрольно-счетной палаты
города Таганрога от
от _____ № ____

(форма)

ЖУРНАЛ
учета технических средств, участвующих в обработке персональных данных
в Контрольно-счетной палате города Таганрога

№ п\п	Наименование технического средства, тип машинного носителя информации	Заводской (серийный) номер	Фамилия, имя, отчество, должность, подразделение (при наличии) работника, получившего техническое средство, машинный носитель информации	Дата получения	Подпись работника получившего техническое средство, машинный носитель информации	Дата возврата	Подпись лица, принявшего техническое средство, машинный носитель информации	Место установки технического средства (помещение), место хранения машинного носителя информации	Отметка об уничтожении машинных носителей информации (номер акта и дата)
1	2	3	4	5	6	7	8	9	10

Приложение 19
к приказу председателя
Контрольно-счетной палаты
города Таганрога от
от _____ № ____

(форма)

ЖУРНАЛ
учета работ по уничтожению персональных данных
Контрольно-счетной палаты города Таганрога

№ п/п	Наименование информационной системы персональных данных	Фамилия, имя, отчество субъекта, персональные данные которого подлежат уничтожению	Персональные данные, подлежащие уничтожению[4]	Причина уничтожения	Носитель персональных данных, его место расположения	Дата и номер акта об уничтожении
1	2	3	4	5	6	7

[4] Указываются персональные данные в соответствии с Перечнем персональных данных, обрабатываемых в Контрольно-счетной палате города Таганрога в связи с реализацией служебных и трудовых отношений, а также в связи с осуществлением муниципальных функций, утвержденным приказом председателя Контрольно-счетной палаты города Таганрога от 10.03.2016 № 10

Приложение 20
к приказу председателя
Контрольно-счетной палаты
города Таганрога от
от _____ № ____

(форма)

УТВЕРЖДАЮ
Председатель Контрольно-
счетной палаты города Таганрога

_____ О.В. Субботина
«___» _____ 20___ г.
М.П.

АКТ
об уничтожении персональных данных

г. Таганрог «___»_____20__ г.

Постоянно действующая комиссия Контрольно-счетной палаты города Таганрога по уничтожению персональных данных, созданная распоряжением председателя Контрольно-счетной палаты города Таганрога от _____ № _____ (далее - комиссия) в составе:

председателя комиссии _____

заместителя председателя комиссии _____

членов комиссии _____

_____

_____

_____

в соответствии со статьей 21 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», руководствуясь Требованиями к подтверждению уничтожения персональных данных, утвержденными Приказом Роскомнадзора от 28.10.2022 № 179, составила настоящий

акт об уничтожении персональных данных субъектов персональных данных, обрабатываемых Контрольно-счетной палатой города Таганрога, находящейся по адресу: 347900, Россия, Ростовская область, г. Таганрог, ул. Петровская 73:

№ п/п	Фамилия, имя, отчество (при наличии) субъекта персональных данных, чьи данные были уничтожены	Перечень категорий уничтоженных персональных данных	Наименование уничтоженного материального носителя, содержавшего персональные данные, количество листов материального носителя[1]	Наименование информационной системы персональных данных, из которой были уничтожены персональные данные[2]	Способ уничтожения персональных данных	Причина уничтожения персональных данных	Дата уничтожения
1	2	3	4	5	6	7	8

Уничтожение персональных данных осуществлено _____[3]

Комиссия пришла к заключению, что примененный способ уничтожения персональных данных исключает возможность дальнейшего использования персональных данных или их восстановления.

Приложения:[4]

Председатель комиссии _____ _____
(подпись) (фамилия и инициалы)

заместитель председателя комиссии _____ _____
(подпись) (фамилия и инициалы)

члены комиссии _____ _____
(подпись) (фамилия и инициалы)

_____ _____
(подпись) (фамилия и инициалы)

_____ _____

(подпись) (фамилия и инициалы)

_____ _____

(подпись) (фамилия и инициалы)

---

[1] Указывается в случае обработки персональных данных без использования средств автоматизации.

[2] Указывается в случае обработки персональных данных с использованием средств автоматизации.

[3] При самостоятельном уничтожении персональных данных указывается на их уничтожение постоянно действующей комиссией Контрольно-счетной палаты города Таганрога по уничтожению персональных данных. При уничтожении сторонней организацией указывается наименование такой организации, ее адрес, реквизиты муниципального контракта, исполнителем по которому является организация, а также указывается на уничтожение персональных данных в присутствии постояннодействующей комиссии Контрольно-счетной палаты города Таганрога по уничтожению персональных данных.

[4] В случае если обработка персональных данных осуществляется с использованием средств автоматизации к акту прикладывается выгрузка из журнала регистрации событий в информационной системе персональных данных

Приложение 21
к приказу председателя
Контрольно-счетной палаты
города Таганрога от
от _____ № ____

(форма)

УТВЕРЖДАЮ

Председатель Контрольно-счетной
палаты города Таганрога

_____ О.В. Субботина
«___» _____ 20___ г.

М.П.

АКТ
проверки соответствия обработки персональных данных требованиям к защите персональных данных

г. Таганрог «___»_____20__ г.

Постоянно действующая комиссия Контрольно-счетной палаты города Таганрога по контролю защищенности персональных данных, созданная распоряжением председателя Контрольно-счетной палаты города Таганрога от _____ № _____ (далее - комиссия) в составе:
председателя комиссии _____
заместителя председателя комиссии _____
членов комиссии _____
на основании Плана мероприятий по обеспечению защиты персональных данных в Контрольно-счетной палате города Таганрога на 20___год, утвержденного приказом председателя Контрольно-счетной палаты города Таганрога от _____ №_____, составили настоящий акт по результатам проверки соответствия обработки персональных данных требованиям к защите персональных данных _____
(указывается наименование аудиторского

_____
(направления, структурного подразделения или рабочего места работника Контрольно-счетной палаты города Таганрога в котором (на котором) проведена проверка)

В ходе проверки Комиссией осуществлены:

_____
(указывается наименование проверочного(ых) мероприятия(тий), предусмотренного(ых) Планом мероприятий по обеспечению защиты персональных данных в Контрольно-счетной палате города Таганрога)

В ходе проверки установлено: _____
(указываются требования, на соответствие которым

_____
проводится проверка, выявленные нарушения, иная информация, установленная в ходе проверки)

Выводы по результатам проверки _____

(при наличии нарушений законодательства

_____

Российской Федерации в сфере обработки персональных данных указывается перечень

_____

мероприятий по устранению выявленных нарушений и сроки их устранения (при необходимости)

Председатель комиссии	_____	_____
	(подпись)	(фамилия и инициалы)
заместитель председателя комиссии	_____	_____
	(подпись)	(фамилия и инициалы)
члены комиссии	_____	_____
	(подпись)	(фамилия и инициалы)