Администрация Находкинского городского округа
Приморского края

Р А С П О Р Я Ж Е Н И Е

12 января 2017 года г. Находка № 16-р

Об организации работ по обеспечению безопасности персональных данных в информационных системах персональных данных администрации Находкинского городского округа

В целях обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных администрации Находкинского городского округа (далее – ИСПДн), в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», 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», постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

1. Назначить руководителей отраслевых (функциональных, территориальных) органов администрации Находкинского городского округа (далее – органы), работники которых осуществляют обработку персональных данных, ответственными за обработку персональных данных в отраслевых (функциональных, территориальных) органах администрации Находкинского городского округа

2. Установить, что лица, указанные в пункте 1 данного распоряжения:

2.1. Определяют круг работников органа, доступ которых к персональным данным, обрабатываемым в информационных системах, необходим для выполнения ими служебных (трудовых) обязанностей.

2.2. Принимают организационные меры по обеспечению безопасности персональных данных при их обработке, предусмотренные соответствующими нормативными документами, при эксплуатации информационных систем персональных данных.

2.3. Обеспечивают выполнение требований, установленных постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» при обработке персональных данных, осуществляемых без использования средств автоматизации.

2.4. Ознакамливают работников, которые осуществляют обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных (в том числе с требованиями к защите персональных данных), локальными актами по вопросам обработки персональных данных.

2.5. Обеспечивают своевременное уничтожение персональных данных в случаях, предусмотренных частями 3-6 статьи 21 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

2.6. Обеспечивают обезличивание персональных данных согласно требованиям и методам, утвержденным приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 05.09.2013 № 996 «Об утверждении требований и методов по обезличиванию персональных данных».

2.7. Несут ответственность за выполнение условий статьи 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» в органе.

2.8. Несут ответственность за соблюдение конфиденциальности при обработке персональных данных в органе.

3. Утвердить прилагаемые

3.1. Инструкцию пользователя по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных администрации Находкинского городского округа.

3.2. Инструкцию о внесении изменений в списки пользователей и наделению их полномочиями доступа к ресурсам информационных систем персональных данных администрации Находкинского городского округа.

3.3. Инструкцию о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных администрации Находкинского городского округа.

3.4. Инструкцию по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационных систем персональных данных администрации Находкинского городского округа.

3.5. Порядок доступа работников администрации Находкинского городского округа в помещения, в которых ведется обработка персональных данных, и организации безопасности этих помещений.

3.6. Порядок обработки персональных данных без использования средств автоматизации.

3.7. Порядок уничтожения персональных данных в информационных систем персональных данных администрации Находкинского городского округа при достижении целей обработки или при наступлении иных законных оснований.

4. Работникам администрации Находкинского городского округа, допущенным к обработке персональных данных, обеспечить конфиденциальность персональных данных.

5. Руководителям органов администрации Находкинского городского округа:

5.1. В течение 10 дней с даты регистрации данного распоряжения сформировать и направить в адрес руководителя аппарата администрации Находкинского городского округа Ю.Н. Кайдановича списки работников органов, доступ которых к персональным данным необходим для выполнения ими служебных (трудовых) обязанностей, составленные согласно форме (приложение № 1), и перечень мест хранения материальных носителей персональных данных составленный согласно форме (приложение № 2). Электронные копии направить в отдел компьютерных технологий администрации Находкинского городского округа.

5.2. Своевременно, в течение 10-ти дней, вносить изменения в утвержденные списки и перечни, указанные в пункте 5.1. данного распоряжения.

5.3. Ознакомить работников органов, допущенных к обработке персональных данных, с настоящим распоряжением под роспись.

6. Контроль за исполнением данного распоряжения «Об организации работ по обеспечению безопасности персональных данных в информационных системах персональных данных администрации Находкинского городского округа» возложить на руководителя аппарата администрации Находкинского городского округа Ю.Н. Кайдановича.

Глава Находкинского городского округа А.Е. Горелов

Администрация Находкинского городского округа Приморского края РФ
ОТДЕЛ ДЕЛОПРОИЗВОДСТВА

ФОРМА

Приложение № 1

к распоряжению администрации
Находкинского городского округа
от «12» января 2017 года
№ 16-р

СПИСОК
работников администрации Находкинского городского округа, доступ которых к персональным данным в ИСПДн _____ необходим для
(наименование ИСПДн
выполнения ими служебных (трудовых) обязанностей

№ п/п	Занимаемая должность, ФИО	Автоматизированная обработка (да/нет)	Неавтоматизированная обработка (да/нет)

Начальник отдела компьютерных
технологий администрации
Находкинского городского округа Е.Л. Харчук

ФОРМА

Приложение № 2

к распоряжению администрации
Находкинского городского округа
от «12» января 2017 года
№ 16-р

Перечень мест хранения
материальных носителей персональных данных
в ИСПДн _____
(наименование ИСПДн)
администрации Находкинского городского округа и ответственных лиц

№ п/п	Адрес, помещение	Место хранения материальных носителей персональных данных	Ответственные лица

Начальник отдела компьютерных
технологий администрации
Находкинского городского округа

Е.Л. Харчук

УТВЕРЖДЕНА

распоряжением администрации
Находкинского городского округа
от « 12 » января 2017 года
№ 16-р

ИНСТРУКЦИЯ
пользователя по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных администрации Находкинского городского округа

1. Общие положения

1.1. Пользователем персональных данных (далее — Пользователь) является работник администрации Находкинского городского округа (далее — Оператор), участвующий в рамках своих функциональных обязанностей в процессах обработки персональных данных (далее — ПДн).

1.2. Пользователь несет персональную ответственность за свои действия.

1.3. Методическое руководство работой пользователя осуществляется администратором безопасности информационной системы персональных данных.

2. Обязанности Пользователя

2.1. Знать и выполнять требования действующих нормативных методических документов, а также внутренних организационно-распорядительных документов, регламентирующих порядок обработки и защиты ПДн при их обработке.

2.2. Выполнять указания администратора безопасности информационной системы персональных данных (далее — Администратор).

2.3. Соблюдать режим допуска в помещения, где проводится обработка ПДн.

2.4. Выполнять на автоматизированном рабочем месте только те процедуры, которые определены для него должностными обязанностями и на основании Разрешительных систем доступа к ресурсам, программным и техническим средствам информационных систем персональных данных администрации Находкинского городского округа.

2.5. Знать и строго выполнять правила работы со средствами защиты информации, установленными на элементах информационной системы персональных данных администрации Находкинского городского округа (далее — ИСПДн).

2.6. Хранить втайне от других свой пароль, менять его с установленной периодичностью, соблюдать требования парольной защиты.

2.7. Соблюдать правила при работе в сетях общего доступа и (или) международного информационного обмена — Интернет.

2.8. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

2.9. Перед началом работы с машинными носителями информации осуществить проверку носителя на предмет отсутствия компьютерных вирусов.

2.10. Передавать для хранения установленным порядком свое устройство личной идентификации и другие реквизиты разграничения доступа (при необходимости их использования) только Администратору.

2.11. Обо всех выявленных нарушениях, связанных с информационной безопасностью, а также для получения консультаций необходимо обратиться к Администратору.

2.12. Пользователям запрещается:

2.12.1. Разглашать сведения, содержащие ПДн, третьим лицам.

2.12.2. Обрабатывать на автоматизированных рабочих местах информацию и выполнять другие работы, не предусмотренные Разрешительными системами доступа к защищаемой информации в информационных системах персональных данных администрации Находкинского городского округа» к ресурсам, программным и техническим средствам ИСПДн.

2.12.3. Фиксировать на одном материальном носителе ПДн, цели обработки которых заведомо не совместимы.

2.12.4. Записывать и хранить информацию на незарегистрированных съемных машинных носителях информации.

2.12.5. Подключать к рабочей станции незарегистрированные машинные носители информации.

2.12.6. Подключать к рабочей станции личные машинные носители информации и мобильные устройства.

2.12.7. Самостоятельно устанавливать, тиражировать или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств, вскрывать и ремонтировать технические средства.

2.12.8. Открывать общий доступ к папкам на своей рабочей станции.

2.12.9. Отключать (блокировать) средства защиты информации.

2.12.10. Сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн.

2.12.11. Привлекать посторонних лиц для производства ремонта или настройки автоматизированных рабочих мест без согласования с Администратором.

2.12.12. Оставлять посторонних лиц без присмотра в помещениях, где ведется обработка ПДн.

2.12.13. Производить какие-либо изменения в электрических схемах, монтаже и размещении технических средств.

2.12.14. Передавать ПДн по открытым каналам связи.

2.13. Принимать меры по реагированию в случае возникновения внештатных и аварийных ситуаций с целью уменьшения либо ликвидации их последствий.

2.14. При отсутствии визуального контроля за рабочей станцией доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш [Ctrl] + [Alt] + [Del] и выбрать опцию [Блокировка] или [Windows] + [L].

2.15. При неавтоматизированной обработке хранить ПДн в запираемом шкафу в местах, утвержденных распоряжением администрации Находкинского городского округа.

2.16. Обеспечивать раздельное хранение ПДн (материальных носителей), обработка которых осуществляется в различных целях.

2.17. При покидании помещения, где ведется обработка персональных данных, необходимо запирать данные помещения на ключ.

3. Организация парольной защиты

3.1. Личные пароли доступа к элементам ИСПДн устанавливаются Пользователями единолично в соответствии с правилами формирования паролей.

3.2. Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 3 месяца.

3.3. Правила формирования пароля:

3.3.1. Пароль не может содержать имя учетной записи Пользователя или какую-либо его часть.

3.3.2. Пароль должен состоять не менее чем из 8 символов.

3.3.3. В пароле должны присутствовать символы трех категорий из числа следующих четырех:

1) прописные буквы английского алфавита от A до Z;

2) строчные буквы английского алфавита от a до z;

3) десятичные цифры (от 0 до 9);

4) символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #, %);

3.3.4. Запрещается использовать простые пароли типа «123», «111», «qwerty» и им подобные, а также имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о Пользователе.

3.3.5. Запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов.

3.3.6. Запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.).

3.3.7. Запрещается выбирать пароли, которые уже использовались ранее.

3.4. Во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами.

3.5. Правила хранение пароля:

3.5.1. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах.

3.5.2. Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

3.6. Лица, использующие пароли, обязаны:

3.6.1. Четко знать и строго выполнять требования настоящей Инструкции.

3.6.2. Своевременно сообщать Администратору об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

3.7. Удаление (в т.ч. внеплановая смена) личного пароля любого Пользователя должна производиться в следующих случаях:

3.7.1. В случае подозрения дискредитации пароля.

3.7.2. В случае прекращения полномочий (увольнение, переход на другую работу внутри организации) Пользователя после окончания последнего сеанса работы данного Пользователя с системой.

3.7.3. По указанию Администратора.

4. Правила работы в сетях общего доступа и (или) международного информационного обмена

4.1. Работа в сетях общего доступа и (или) международного информационного обмена (далее — Сеть) на элементах ИСПДн, должна проводиться при служебной необходимости.

4.2. При работе в Сети запрещается:

4.2.1. Осуществлять работу при отключенных средствах защиты, в т.ч. средствах антивирусной защиты.

4.2.2. Передавать по незащищенным каналам связи сведения, содержащие ПДн.

4.2.3. Скачивать из Сети программное обеспечение и другие файлы, не относящиеся к выполнению должностных обязанностей.

4.2.4. Посещать Интернет-ресурсы, содержащие информацию экстремистского, расистского, порнографического и криминального характера, а также загружать данные, содержащие подобную информацию.

4.2.5. Использовать адрес служебной почты при регистрации на Интернет-ресурсах, в ходе деятельности, не связанной с выполнением должностных обязанностей.

4.2.6. Осуществлять попытки проникновения в корпоративные сети других компаний.

4.2.7. Загружать медиа-файлы развлекательного характера.

4.2.8. Подключаться к файлообменным сетям.

4.2.9. Нецелевое использование подключения к сети.

4.3. Руководство администрации Находкинского городского округа оставляет за собой право:

4.3.1. Осуществлять мониторинг использования работниками Сети.

4.3.2. Определять перечень запрещенных web-ресурсов и осуществлять блокировку доступа к ним.

4.3.3. Осуществлять мониторинг появления адресов служебной почты на страницах Интернет-ресурсов.

4.3.4. Осуществлять мониторинг появления информации конфиденциального характера о деятельности Оператора в Сети, в том числе и на страницах социальных сетей.

4.3.5. Предоставлять информацию об использовании Сети работниками правоохранительным органам в случаях, предусмотренных законодательством РФ.

4.3.6. Принимать меры дисциплинарного характера к работникам, нарушающим положения данного раздела.

5. Организация антивирусной защиты

5.1. Установка и настройка средств антивирусного контроля осуществляется Администратором.

5.2. Обязательному антивирусному контролю подлежат все файлы, получаемые для обработки в элементах ИСПДн.

5.3. Вновь получаемые файлы должны проходить антивирусный контроль до начала их обработки в элементах ИСПДн.

5.4. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, исчезновение файлов, частое появление сообщений о системных ошибках и т.п.) Пользователь обязан немедленно сообщить о своих подозрениях Администратору и затем выполнить внеочередной антивирусный контроль.

5.5. Передаваемые в сторонние организации файлы должны проходить антивирусный контроль непосредственно перед отправлением или перед записью на носитель.

5.6. Если при проведении антивирусной проверки информационных ресурсов ИСПДн были обнаружены вирусы или их воздействие на носители информации, пользователь обязан:

5.6.1. Сообщить Администратору.

5.6.2. Провести «лечение» файла.

5.6.3. В случае обнаружения нового вируса, не поддающегося «лечению» применяемыми антивирусными средствами, исключить из обработки зараженный вирусом файл.

5.6.4. Выполнить проверку всех носителей информации в ИСПДн, которые могли стать носителями вируса.

5.6.5. Попытаться найти источник заражения и по возможности вылечить его от вирусов, в противном случае исключить возможность взаимодействия источника заражения с элементами ИСПДн.

6. Порядок реагирования на аварийную ситуацию

6.1. В настоящем документе под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн. Аварийная ситуация становится возможной в результате реализации одной из угроз, приведенных ниже:

6.1.1. Отключение электроэнергии.

6.1.2. Сбой в работе вычислительной сети (коммутационного оборудования).

6.1.3. Ошибка персонала, имеющего доступ к серверной.

6.1.4. Нарушение конфиденциальности, целостности и доступности персональных данных.

6.1.5. Физический разрыв внешних каналов связи.

6.2. В случае реализации любой из угроз (выявлении предпосылок к ее реализации) Пользователь обязан:

6.2.1. Предпринять попытку сохранения обрабатываемой информации, содержащей ПДн.

6.2.2. Прекратить работу на автоматизированном рабочем месте.

6.2.3. Немедленно оповестить Администратора, о возникновении аварийной ситуации.

УТВЕРЖДЕНА

распоряжением администрации
Находкинского городского округа
от « 12 » января 2017 года
№ 16-р

ИНСТРУКЦИЯ
о внесении изменений в списки пользователей и наделению их полномочиями доступа к ресурсам ИСПДн администрации Находкинского городского округа

1. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику ИСПДн администрации Находкинского городского округа (далее – Администрация), допущенному к работе в ИСПДн, должно быть сопоставлено персональное уникальное имя (учетная запись Пользователя), под которым он будет регистрироваться и работать в ИСПДн. Использование несколькими сотрудниками при работе в ИСПДн одного и того же имени Пользователя («группового имени») запрещено.

2. Процедура регистрации (создания учетной записи) пользователя для сотрудника Администрации и предоставления ему (или изменения его) прав доступа к ресурсам ИСПДн инициируется заявкой начальника органа, в котором работает этот сотрудник, составленной по форме (приложение).

3. В заявке указывается:

3.1. Содержание запрашиваемых изменений (регистрация нового пользователя ИСПДн, удаление учетной записи Пользователя, расширение или сужение полномочий и прав доступа к ресурсам ИСПДн ранее зарегистрированного Пользователя).

3.2. Должность (с полным наименованием подразделения), фамилия, имя и отчество сотрудника.

3.3. Полномочия, которых необходимо лишить Пользователя или которые необходимо добавить Пользователю (путем указания решаемых пользователем задач в ИСПДн). Наименования задач должны указываться в соответствии с Перечнем задач, решаемых в ИСПДн.

3.4. Заявку визирует администратор безопасности ИСПДн, утверждая тем самым возможность допуска (изменения прав доступа) данного сотрудника к необходимым для решения им указанных задач ресурсам ИСПДн.

4. Допуск пользователей к обработке информации в ИСПДн производится на основании распоряжения администрации Находкинского городского округа по представлению заинтересованного руководителя органа. К распоряжению прилагаются новые редакции следующих документов:

4.1. Список сотрудников, допущенных к обработке персональных данных в ИСПДн;

4.2. Права доступа пользователей к дискам, портам, программам, каталогам и файлам (матрица доступа) в ИСПДн.

5. После регистрации распоряжения администрации Находкинского городского округа администратор безопасности ИСПДн:

5.1. Производит необходимые настройки системы защиты от НСД и формирует персональный идентификатор Пользователя.

5.2. Сообщает Пользователю:

5.2.1. К каким ресурсам (принтеру, дискам, каталогам и т. д.) он допущен, какие операции ему разрешено выполнять с этими ресурсами.

5.2.2. Перечень программ, разрешенных для запуска.

5.2.3. Уровень конфиденциальности информации, разрешенной для обработки в ИСПДн.

5.2.4. Доступные для работы файлы и папки, их размещение.

5.2.5. Требования, которые необходимо соблюдать при работе с конфиденциальными документами.

5.3. Принимает зачет, сообщает пользователю зарегистрированное имя и временный пароль для входа в систему, после чего допускает Пользователя к работе в ИСПДн.

6. Администратор безопасности знакомит Пользователя с матрицей доступа и выдает ему персональный идентификатор.

7. По окончании внесения изменений в списки пользователей в заявке делается отметка о выполнении задания.

8. Исполненная заявка хранится у администратора безопасности и может быть использована для восстановления полномочий пользователей после сбоев в работе ИСПДн, а также для контроля правомерности наличия у конкретного Пользователя прав доступа к тем или иным ресурсам системы при разборе конфликтных ситуаций.

ФОРМА

Приложение

к Инструкции о внесении изменений в списки пользователей и наделению их полномочиями доступа к ресурсам ИСПДн администрации Находкинского городского округа

ЗАЯВКА
на внесение изменений в списки пользователей и наделение пользователей полномочиями доступа к ресурсам ИСПДн

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

_____
(должность с указанием подразделения)

_____
(фамилия имя и отчество сотрудника)

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

_____
(список задач согласно формуляров задач)

_____

_____

_____

_____

_____

Начальник

_____
(наименование заказывающего подразделения)

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

Согласовано

Администратор безопасности

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

ЗАДАНИЕ
на внесение изменений в списки пользователей ИСПДн

Администратору безопасности информации

_____
(фамилия и инициалы исполнителя)

Произвести изменения в списках пользователей

{Должность руководителя} «Название ИСПДн»

_____ {Фамилия И. О.}

«___» _____ 20__ г.

Обратная сторона заявки

Присвоено **имя** _____ (персональный идентификатор) и предоставлены полномочия, необходимые для решения следующих задач:

Наименование задачи (по перечню задач)

Администратор безопасности {Фамилия И. О.}

Имя, персональный идентификатор и начальное значение пароля получил, о порядке смены пароля при первом входе в систему проинструктирован

Пользователь

_____
(подпись, фамилия)

«___» _____ 20__ года

УТВЕРЖДЕНА

распоряжением администрации
Находкинского городского округа
от « 12 » января 2017 года
№ 16-р

ИНСТРУКЦИЯ
о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных администрации Находкинского городского округа

1. Общие положения

1.1. Настоящая инструкция разработана на основании Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Федерального закона от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации", приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» с целью организации порядка резервирования и восстановления работоспособности технических средств (далее — ТС) и программного обеспечения (далее – ПО), баз данных (далее – БД) и средств защиты информации (далее — СЗИ) в информационных системах персональных данных администрации Находкинского городского округа (далее – ИСПДн).

1.2. Настоящая инструкция определяет порядок резервирования и восстановления работоспособности ТС и ПО, БД и СЗИ, и определяет порядок действий ответственных лиц, связанных с функционированием ИСПДн, меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн.

1.3. Целью настоящего документа является превентивная защита элементов ИСПДн от предотвращения потери защищаемой информации.

Задачами данной инструкции являются:

– определение мер защиты от потери информации;

– определение действий по восстановлению в случае потери информации.

1.4. Действие настоящей инструкции распространяется на всех пользователей администрации Находкинского городского округа, имеющих доступ к ресурсам ИСПДн, а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении аварийных ситуаций, в том числе:

- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа.

1.5. Пересмотр настоящего документа осуществляется по мере необходимости, но не реже одного раза в два года.

1.6. Сотрудником ответственным, за реагирование на инциденты безопасности и контроль мероприятий по предотвращению инцидентов, приводящих к потере защищаемой информации, назначается Администратор безопасности ИСПДн.

2. Порядок реагирования на инцидент

2.1. В настоящем документе под инцидентом понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн, а также потерей защищаемой информации.

2.2. Происшествие, вызывающее инцидент, может произойти:

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

2.3. Все действия в процессе реагирования на инцидент должны документироваться ответственным за реагирование сотрудником в Журнале учета нештатных ситуаций и выполнения профилактических работ, установки, модификации программных средств на рабочих станциях и серверах, составленном

согласно форме (приложение № 1).

2.4. В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование работники администрации Находкинского городского округа, предпринимают меры по восстановлению работоспособности. Предпринимаемые меры, по возможности, согласуются с вышестоящим руководством.

3. Технические меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов

3.1. К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения Инцидентов, такие как:

- системы обеспечения отказоустойчивости;
- системы резервного копирования и хранения данных;
- системы контроля физического доступа;
- системы жизнеобеспечения ИС.

3.2. Системы жизнеобеспечения ИС включают:

- пожарные сигнализации и системы пожаротушения;
- системы вентиляции и кондиционирования;
- системы резервного питания.

3.3. Все помещения администрации Находкинского городского округа, в которых размещаются элементы ИСПДн, материальные носители ПДн и средства защиты, должны быть оборудованы средствами пожарной сигнализации и пожаротушения.

3.4. Для выполнения требований по эксплуатации (температура, относительная влажность воздуха) программно-аппаратных средств ИС в помещениях, где они установлены, должны применяться системы вентиляции и кондиционирования воздуха.

3.5. Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы ИС, сетевое и

коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

– локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных рабочих станций и серверов;

– источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;

– дублированные системы электропитания в устройствах (серверы, концентраторы, мосты и т. д.);

– резервные линии электропитания в пределах комплекса зданий;

– аварийные электрогенераторы.

3.6. Для обеспечения отказоустойчивости критичных компонентов ИС при сбое в работе оборудования и их автоматической замены без простоев должны использоваться методы кластеризации. Могут использоваться следующие методы кластеризации: для наиболее критичных компонентов ИС должны использоваться территориально удаленные системы кластеров.

3.7. Система резервного копирования и хранения данных должна обеспечивать хранение защищаемой информации на съемный носитель (ленту, жесткий диск и т. п.).

4. Организационные меры обеспечения непрерывности работы и восстановления ресурсов при возникновении инцидентов

4.1. Резервное копирование и хранение данных должно осуществляться на периодической основе:

– для обрабатываемых персональных данных – не реже раза в день инкрементальным способом, и не реже одного раза в неделю полный объем данных;

– для технологической информации – не реже одного раза в месяц;

– эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИС – не реже одного раза в

месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).

4.2. Данные о проведение процедуры резервного копирования, должны отражаться в специально созданном журнале резервного копирования информации, составленном согласно форме (приложение № 2).

4.3. Носители, на которые произведено резервное копирование, должны быть пронумерованы номером носителя, датой проведения резервного копирования.

4.4. Носители должны храниться в несгораемом шкафу или помещении оборудованном системой пожаротушения.

4.5. Носители должны храниться не менее года для возможности восстановления данных.

5. Ответственность за поддержание установленного в настоящей инструкции порядка проведения резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных возлагается на администратора безопасности информации ИСПДн.

ФОРМА

Приложение № 1

к Инструкции о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных администрации Находкинского городского округа

ЖУРНАЛ УЧЕТА
нештатных ситуаций и выполнения профилактических работ, установки, модификации программных средств на рабочих станциях и серверах ИСПДн

№ п/п	Дата	Краткое описание выполненной работы (нештатной ситуации)	ФИО ответственного за эксплуатацию	Специалист / организация, выполнявшая работы
1	2	3	4	5

ФОРМА

Приложение № 2

к Инструкции о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных администрации Находкинского городского округа

Журнал резервного копирования информации

№ п/п	Дата	Наименование объекта резервного копирования	Место хранения	Примечание
1	2	3	4	5

УТВЕРЖДЕНА

распоряжением администрации
Находкинского городского округа
от « 12 » января 2017 года
№ 16-р

ИНСТРУКЦИЯ
по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационных систем персональных данных администрации Находкинского городского округа

1. Общие положения

1.1. Инструкция по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств информационных систем персональных данных (далее - ИСПДн) администрации Находкинского городского округа (далее - Администрация), регламентирует действия при проведении работ по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств ИСПДн.

1.2. Требования настоящей Инструкции распространяются на всех должностных лиц и сотрудников органов Администрации, использующих в работе ИСПДн, в которых осуществляется обработка информации ограниченного доступа, не составляющей государственной тайны.

1.3. Сотрудники Администрации, задействованные в обеспечении функционирования ИСПДн, знакомятся с основными положениями и приложениями Инструкции в части, их касающейся, по мере необходимости.

1.4. В случае невозможности исполнения требований настоящей Инструкции в полном объеме, например: в нештатных ситуациях, возникающих вследствие отказов, сбоев, ошибок, стихийных бедствий, побочных влияний, злоумышленных действий, практическая «глубина» исполнения настоящей Инструкции определяется Администратором безопасности ИСПДн (далее – Администратор), по согласованию с начальником отдела компьютерных технологий Администрации.

2. Порядок проведения работ

2.1. Все изменения конфигурации технических и программных средств рабочих станций Администрации должны производиться только на основании

заявок руководителей органов Администрации, составленных согласно форме (приложение №1), согласованных с главой Находкинского городского округа. Производственная необходимость проведения указанных в заявке изменений подтверждается подписью руководителя органа Администрации.

2.2. Все изменения конфигурации технических и программных средств рабочих станций и серверов, входящих в состав аттестованных по требованиям безопасности ИСПДн Администрации, должны производиться только на основании заявок руководителей структурных подразделений Администрации (приложение № 1), согласованных с главой Находкинского городского округа. Производственная необходимость проведения указанных в заявке изменений подтверждается подписью руководителя органа Администрации. При этом необходимо уведомить об осуществленных изменениях организацию, производившую аттестацию, которая принимает решение о необходимости проведения контроля эффективности аттестованного объекта информатизации.

2.3. Все изменения конфигурации технических и программных средств рабочих станций и серверов, входящих в состав аттестованных по требованиям безопасности ИСПДн Администрации, отражаются в Техническом паспорте объекта информатизации. Запрещается изменение состава (в том числе ввод новых) программных средств, осуществляющих обработку ПДн на объектах информатизации, аттестованных по требованиям безопасности информации.

2.4. В заявке указываются наименование ПЭВМ и ответственный за нее сотрудник. После чего заявка передается Администратору ИСПДн для выполнения работ по внесению изменений в конфигурацию ПЭВМ ИСПДн Администрации.

2.5. Право внесения изменений в конфигурацию аппаратно-программных средств рабочих станций ИСПДн Администрации предоставляется Администратору.

2.6. Изменение конфигурации аппаратно-программных средств рабочих станций и серверов кем-либо, кроме Администратора, запрещено.

2.7. Установка и настройка программного средства осуществляется администратором согласно эксплуатационной документации.

2.8. Запрещается установка и использование на ПЭВМ (серверах) программного обеспечения (ПО), не входящего в перечень программного обеспечения, разрешенного к использованию в Администрации.

2.9. Руководители органов Администрации осуществляют контроль за отсутствием на ПЭВМ сотрудников подразделения программного обеспечения и данных, не связанных с выполнением должностных обязанностей.

2.10. Установка (обновление) ПО (системного, тестового и т.п.) на рабочих станциях и серверах производится с эталонных копий программных средств, хранящихся у Администратора. Все добавляемые программные и аппаратные компоненты должны быть предварительно проверены на работоспособность, а также отсутствие вредоносного программного кода.

2.11. После установки (обновления) ПО Администратор должен произвести настройку средств управления доступом к компонентам данной задачи (программного средства) в соответствии с требованиями к системе защиты информации и, совместно с пользователем ПЭВМ, проверить правильность настройки средств защиты.

2.12. В случае обнаружения недекларированных (не описанных в документации) возможностей программного средства, сотрудники немедленно докладывают руководителю своего подразделения и Администратору. Использование программного средства до получения специальных указаний запрещается.

2.13. После завершения работ по внесению изменений в состав аппаратных средств, защищенных ПЭВМ, системный блок должен быть опечатан (опломбирован, защищен специальной наклейкой) Администратором.

2.14. При изъятии ПЭВМ из состава рабочих станций, обрабатывающих информацию ограниченного распространения (защищаемая информация), ее передача на склад, в ремонт или в другое подразделение для решения иных задач осуществляется только после того, как Администратор снимет с данной ПЭВМ средства защиты и предпримет необходимые меры для затирания (уничтожения) защищаемой информации, которая хранилась на дисках компьютера. Факт уничтожения данных, находившихся на диске компьютера, оформляется актом за подписью Администратора, составленным согласно форме(приложении № 2).

2.15. Допуск новых пользователей к решению задач с использованием вновь развернутого ПО (либо изменение их полномочий доступа) осуществляется согласно Инструкции о внесении изменений в списки пользователей и наделению

их полномочиями доступа к ресурсам ИСПДн администрации Находкинского городского округа.

2.16. Оригиналы заявок (документов), на основании которых производились изменения в составе технических или программных средств ПЭВМ с отметками о внесении изменений в состав аппаратно-программных средств должны храниться у Администратора.

ФОРМА

Приложение № 1

к Инструкции по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств ИСПДн администрации Находкинского городского округа

Главе Находкинского городского округа

(резолюция)

ЗАЯВКА

На внесение изменений в состав *программного (аппаратного)* обеспечения
(ненужное зачеркнуть)

_____
(Наименование ПЭВМ)

Прошу дать указания ответственным сотрудникам Администрации
для *установки (изменения настроек)*
(ненужное зачеркнуть)

_____

_____
(перечень ПО (аппаратных средств) и необходимых настроек)

для решения задач:

_____
_____
_____
_____

следующим пользователям:

_____
_____
_____
(Фамилия, Имя, Отчество)

Руководитель _____
(наименование структурного подразделения)

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

Обратная сторона заявки

Изменения на ПЭВМ ИСПДн *произведены (не произведены)* по следующей причине:
(ненужное зачеркнуть)

_____
_____
_____
_____

Выполнены следующие работы:

_____
_____
_____
_____
_____
_____

Выполнены следующие изменения в настройках средств защиты:

_____
_____
_____
_____
_____
_____

Администратор безопасности ИСПДн

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

ФОРМА

Приложение № 2

к Инструкции по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств ИСПДн администрации Находкинского городского округа

АКТ
о затирании остаточной информации, хранившейся на диске компьютера

Все файлы, содержащие подлежащую защите информацию, находившиеся на НЖМД

_____,

передаваемого

(модель, серийный №)

_____

(с какой целью)

_____

(Кому: должность, Ф.И.О.)

ПЭВМ:

_____

(Наименование ПЭВМ)

уничтожены (затерты) посредством программы _____.

Администратор безопасности ИСПДн

«___» _____ 20__ г. _____ _____

(подпись) (Фамилия, инициалы)

УТВЕРЖДЕН

распоряжению администрации
Находкинского городского округа
от « 12 » января 2017 года
№ 16-р

ПОРЯДОК
доступа работников администрации Находкинского городского округа в помещения, в которых ведется обработка персональных данных, и организации безопасности этих помещений

1. Порядок доступа работников администрации Находкинского городского округа в помещения, в которых ведется обработка персональных данных, и организации безопасности этих помещений (далее - Порядок), разработан в соответствии с 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».

2. Ответственность за режим безопасности в защищаемом помещении и правильность использования установленных в нем технических средств несет должностное лицо, которое постоянно в нем работает, или лицо, специально на то уполномоченное.

3. В нерабочее время защищаемое помещение должно закрываться на ключ и сдаваться под охрану ответственным лицом.

4. В рабочее время, в случае ухода ответственного лица, помещение должно закрываться на ключ или оставляться под ответственность уполномоченного лица.

5. Обеспечение безопасности персональных данных от уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных, достигается, в том числе, установлением правил доступа в помещения, где обрабатываются персональные данные.

6. В помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также где хранятся носители

информации, допускаются только работники администрации Находкинского городского округа, уполномоченные на обработку персональных данных.

7. Нахождение лиц, не являющихся уполномоченными лицами на обработку персональных данных, в помещениях администрации Находкинского городского округа возможно только в сопровождении ответственного или уполномоченного лица администрации Находкинского городского округа на время, ограниченное необходимостью решения вопросов, связанных с исполнением должностных обязанностей и (или) осуществлением полномочий в рамках договоров, заключенных с администрацией Находкинского городского округа.

8. При обработке персональных данных и хранении материальных носителей персональных данных должны соблюдаться условия, при которых обеспечивается сохранность носителей персональных данных и средств защиты информации и исключающие несанкционированный доступ к ним, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц.

9. Повседневный контроль за выполнением требований по защите помещения осуществляют лица, ответственные за помещение, назначенные распоряжением администрации Находкинского городского округа.

10. Периодический контроль эффективности мер защиты помещения осуществляется ответственным за организацию обработки персональных данных.

УТВЕРЖДЕН

распоряжением администрации
Находкинского городского округа
от « 12 » января 2017 года
№ 16-р

ПОРЯДОК
обработки персональных данных без использования средств автоматизации

1. Обработка персональных данных (далее – ПДн) без использования средств автоматизации (далее — неавтоматизированная обработка) может осуществляться в виде документов на бумажных носителях и в электронном виде (файлы, базы данных) на электронных носителях информации.

2. При неавтоматизированной обработке различных категорий ПДн должен использоваться отдельный материальный носитель для каждой категории ПДн.

3. При неавтоматизированной обработке ПДн на бумажных носителях:

3.1. Не допускается фиксация на одном бумажном носителе ПДн, цели обработки которых заведомо не совместимы.

3.2. ПДн должны обособляться от иной информации, в частности путем фиксации их на отдельных бумажных носителях, в специальных разделах или на полях форм (бланков).

3.3. Документы, содержащие ПДн, формируются в дела в зависимости от цели обработки ПДн.

3.4. Дела с документами, содержащими ПДн, должны иметь внутренние описи документов с указанием цели обработки и категории ПДн.

4. При использовании типовых форм документов, характер информации которых предполагает или допускает включение в них ПДн (далее — типовые формы), должны соблюдаться следующие условия:

4.1. Типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели неавтоматизированной обработки ПДн, имя (наименование) и адрес Оператора, фамилию, имя, отчество и адрес субъекта ПДн, источник получения ПДн, сроки

обработки ПДн, перечень действий с ПДн, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки ПДн.

4.2. Типовая форма должна предусматривать поле, в котором субъект ПДн может поставить отметку о своем согласии на неавтоматизированную обработку ПДн, — при необходимости получения письменного согласия на обработку ПДн.

4.3. Типовая форма должна быть составлена таким образом, чтобы каждый из субъектов ПДн, содержащихся в документе, имел возможность ознакомиться со своими ПДн, содержащимися в документе, не нарушая прав и законных интересов иных субъектов ПДн.

4.4. Типовая форма должна исключать объединение полей, предназначенных для внесения ПДн, цели обработки которых заведомо не совместимы.

5. Неавтоматизированная обработка ПДн в электронном виде осуществляется на внешних электронных носителях информации.

6. При отсутствии технологической возможности осуществления неавтоматизированной обработки ПДн в электронном виде на внешних носителях информации необходимо принимать организационные (охрана помещений) и технические меры (установка сертифицированных средств защиты информации), исключающие возможность несанкционированного доступа к ПДн лиц, не допущенных к их обработке.

7. Электронные носители информации, содержащие ПДн, учитываются в журнале учета машинных носителей, предназначенных для хранения и обработки персональных данных,составленном согласно форме (приложение).

8. При несовместимости целей неавтоматизированной обработки ПДн, зафиксированных на одном электронном носителе, если электронный носитель не позволяет осуществлять обработку ПДн отдельно от других зафиксированных на том же носителе ПДн, должны быть приняты меры по обеспечению раздельной обработки ПДн, в частности:

8.1. При необходимости использования или распространения определенных ПДн отдельно от находящихся на том же материальном носителе других ПДн осуществляется копирование ПДн, подлежащих распространению или использованию, способом, исключающим одновременное копирование ПДн, не

подлежащих распространению и использованию, и используется (распространяется) копия ПДн.

8.2. При необходимости уничтожения или блокирования части ПДн уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование ПДн, подлежащих уничтожению или блокированию.

9. Документы и внешние электронные носители информации, содержащие ПДн, должны храниться в служебных помещениях в надежно запираемых и опечатываемых шкафах (сейфах), в местах, утвержденных распоряжением администрации Находкинского городского округа. При этом должны быть созданы надлежащие условия, обеспечивающие их сохранность. При покидании помещения, где ведется обработка персональных данных, необходимо запирать данные помещения на ключ.

10. Уничтожение носителей, содержащих ПДн

10.1. Сведения, содержащие ПДн субъектов Оператора, для которых в соответствии с нормативными правовыми документами не установлены сроки хранения, по достижении целей обработки ПДн либо по требованию субъекта ПДн уничтожаются.

10.2. Для удаления информации, содержащей ПДн, создается комиссия, состав которой определяется распоряжением администрации Находкинского городского округа.

10.3. Итоги работы комиссии оформляются Актами уничтожения персональные данных.

10.4. Уничтожение сведений, содержащих ПДн субъектов Оператора, производится любым способом, исключающим ознакомление посторонних лиц с уничтожаемыми материалами и возможность восстановления их содержания.

10.5. Об уничтожении ПДн Оператор обязан уведомить субъекта ПДн или его законного представителя.

ФОРМА

Приложение

к Порядку обработки персональных данных
без использования средств автоматизации

ЖУРНАЛ
учета машинных носителей предназначенных для хранения и обработки персональных данных

№ п/п	Регистрационный (учетный) номер носителя	Тип и емкость носителя	Дата поступления на учет	Отметка о постановке на учет (ФИО, подпись дата)	Отметка о снятии с учета (ФИО, подпись дата)	Место хранения	Сведения об уничтожении носителя
1	2	3	4	6	7	8	9

УТВЕРЖДЕН

распоряжению администрации
Находкинского городского округа
от «12» января 2017 года
№ 16-р

ПОРЯДОК
уничтожения персональных данных в ИСПДн администрации Находкинского городского округа при достижении целей обработки или при наступлении иных законных оснований

1. Настоящий порядок определяет обязательные для всех исполнителей требования по уничтожению документов, содержащих персональные данные.

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

3. Решение об уничтожении персональных данных принимает глава Находкинского городского округа на основании представления ответственного за обработку персональных данных в ИСПДн.

4. Уничтожение документов производится комиссией по уничтожению персональных данных, состав которой утверждается распоряжением администрации Находкинского городского округа. Председатель комиссии несет персональную ответственность за правильность и полноту уничтожения перечисленных в акте документов.

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

6. После уничтожения материальных носителей членами комиссии подписывается акт, составленный согласно форме (приложение), делается запись в журналах их учета и регистрации, а также в номенклатурах и описях дел проставляется отметка «Уничтожено. Акт №__(дата)».

7. Уничтожение информации на машинных носителях необходимо осуществлять путем стирания информации с использованием сертифицированного

программного обеспечения, установленного на ПЭВМ с гарантированным уничтожением (в соответствии с заданными характеристиками для установленного программного обеспечения с гарантированным уничтожением).

ФОРМА

Приложение

к Порядку уничтожения персональных данных в ИСПДн администрации Находкинского городского округа при достижении целей обработки или при наступлении иных законных оснований

УТВЕРЖДАЮ

Глава Находкинского городского округа
_____ / Ф.И.О. /
подпись
«____»_____20____г.

АКТ № _____
об уничтожении персональных данных
субъекта(ов) персональных данных, обрабатываемых
в ИСПДн администрации Находкинского городского округа

Комиссия в составе:

	ФИО	Должность
Председатель		
Члены комиссии		

составила настоящий Акт о том, что информация, зафиксированная на перечисленных в нем носителях информации (электронных, бумажных[1]), подлежат уничтожению.

Учетный номер материального носителя, номер дела и т.д.	Причина уничтожения носителя информации; стирания/обезличивания информации	Тип носителя информации	Производимая операция (стирание, уничтожение, обезличивание)	Дата
1	2	3	4	5

Всего подлежит уничтожению_____ носителей
(цифрами и прописью)

Правильность произведенных записей в акте проверена.

Регистрационные данные на носителях информации перед уничтожением (стиранием с них информации) с записями в акте сверены, произведено уничтожение путем:

_____
(стирания на устройстве гарантированного уничтожения информации, разрезания, сжигания, механического уничтожения, вымарывания и т.п.)

[1] В случае, если объем уничтожаемых документов позволяет перечислять их в Акте.

Отметки о стирании информации (уничтожении носителей информации) в учетных формах произведены.

Председатель комиссии: _____ / /
Члены комиссии: _____ / /
_____ / /

Примечание:
1. Акт составляется раздельно на каждый способ уничтожения носителей.
2. Все листы акта, а так же все произведенные исправления и дополнения в акте заверяются подписями всех членов комиссии.