****

**АДМИНИСТРАЦИЯ**

**НЕФТЕЮГАНСКОГО РАЙОНА**

**постановление**

|  |  |
| --- | --- |
| 01.08.2019 | № 1636-па |
|  |

г.Нефтеюганск

Об организации работ по защите персональных данных, обрабатываемых   
в информационных системах персональных данных

В соответствии c Федеральными [законами](consultantplus://offline/ref=07514055834D34FD0F41D3ED3EA022B7AA4A47AC3ECDF4AC15DF23DB9B13559C73B565AF5B392EEFAF34G) от 27.07.2006 № 152-ФЗ   
«О персональных данных», от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановлением Правительства Российской Федерации 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 Главы Нефтеюганского район   
от 01.07.2019 № 87-пг-нпа «Об обработке персональных данных», в рамках реализации работ по защите персональных данных, обрабатываемых   
в информационных системах персональных данных, п о с т а н о в л я ю:

1. Утвердить:
   1. Инструкцию по обеспечению безопасности системы обработки персональных данных (приложение № 1).
   2. Инструкцию пользователя информационной системы персональных данных (приложение № 2).
   3. Инструкцию администратора информационной безопасности информационных систем персональных данных (приложение № 3).

# Инструкцию по антивирусной защите при работе в информационных системах персональных данных (приложение № 4).

* 1. Инструкцию ответственного за защиту информации (приложение № 5).
  2. Инструкцию по учету лиц, допущенных к работе с персональными данными в информационных системах персональных данных администрации Нефтеюганского района (приложение № 6).
  3. Инструкцию по учету машинных носителей информации и регистрации   
     их выдачи (приложение № 7).
  4. Типовую форму журнала учета лиц, допущенных к работе   
     с персональными данными в информационных системах персональных данных (приложение № 8).
  5. Типовую форму журнала по учету машинных носителей и регистрации   
     их выдачи (приложение № 9).
  6. Типовую форму журнала по учету применяемых средств защиты информации, эксплуатационной и технической документации к ним   
     (приложение № 10).
  7. Типовую форму журнала учета нештатных ситуаций информационных систем персональных данных, выполнения профилактических работ, учета установки и модификации программных средств на автоматизированных рабочих местах информационных систем персональных данных (приложение № 11).
  8. Типовую форму журнала учета мероприятий по защите персональных данных (приложение № 12).

1. Руководителям структурных подразделений администрации Нефтеюганского района ознакомить под роспись подчиненных работников   
   с настоящим постановлением и обеспечить его исполнение при обработке персональных данных.
2. Настоящее постановление подлежит размещению на официальном сайте органов местного самоуправления Нефтеюганского района.
3. Контроль за выполнением распоряжения возложить на управляющего   
   делами Ширкунову Я.В.

Глава района Г.В.Лапковская

Приложение № 1

к постановлению администрации

Нефтеюганского района

от 01.08.2019 № 1636-па

# ИНСТРУКЦИЯ по обеспечению безопасности системы обработки персональных данных

(далее – Инструкция)

1. Общие положения
   1. Инструкция разработана в соответствии с Федеральным законами   
      от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации», от 27.07.2006 № 152-ФЗ «О персональных данных», постановлениями Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
   2. Сокращения и понятия, применяемые в настоящей Инструкции:

* операторы персональных данных (оператор) – администрация Нефтеюганского района и её структурные подразделения с правом юридического лица самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;
* персональные данные (ПДн) - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);
* ИСПДн – информационные системы персональных данных;
* АРМ – автоматизированное рабочее место.
  1. Настоящая Инструкция определяет порядок организации обеспечения безопасности персональных данных операторов.
  2. Настоящая Инструкция и все дополнения и изменения к ней утверждаются Главой Нефтеюганского района.
  3. Работники операторов должны быть ознакомлены с отдельными разделами Инструкции и приложениями к ней, другими организационно-распорядительными или эксплуатационными документами в необходимом и достаточном объеме   
     для выполнения своих должностных обязанностей.

1. Подразделения, должностные лица, ответственные

за обеспечение безопасности ПДн

* 1. Глава Нефтеюганского района:
     1. Осуществляет следующие основные функции по обеспечению безопасности ПДн:
        1. Организация обработки ПДн, а также определение целей обработки ПДн и действий, совершаемых с ними.
        2. Определение порядка обработки ПДн.
        3. Назначение должностных лиц, ответственных за обеспечение безопасности.
        4. Утверждение перечня конфиденциальной информации (в том числе персональных данных), обрабатываемой в системе обработки (далее так же – СО) ПДн «Сауми», «Кодекс: Управление персоналом», «1С:Предприятие», «1С:Зарплата   
           и Кадры», «СЭД ОБРАЩЕНИЕ ГРАЖДАН» операторов.
        5. Утверждение актов определения уровня защищенности   
           и классификации ИСПДн операторов.
        6. Утверждение Матрицы доступа к ресурсам СО ПДн «Сауми», «Кодекс: Управление персоналом», «1С:Предприятие», «1С:Зарплата и Кадры», «СЭД ОБРАЩЕНИЕ ГРАЖДАН» операторов;
        7. Утверждение перечня лиц, допущенных к обработке конфиденциальной информации (в том числе персональных данных).
        8. Утверждение списков лиц, допущенных в помещения, в которых располагаются технические средства СО ПДн.
        9. Утверждение документов, определяющих политику операторов   
           в отношении обработки ПДн, локальных актов по вопросам обработки ПДн, а также локальных актов, устанавливающих процедуры, направленные на предотвращение   
           и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.
        10. Утверждение документов, регламентирующих организацию обеспечения безопасности ПДн.
        11. Принятие мер по результатам расследования инцидентов безопасности информации.
        12. Принятие решения о приостановлении предоставления ПДн   
            при обнаружении нарушений порядка их предоставления.
        13. Отдача распоряжения о возобновлении предоставления ПДн после устранения нарушения порядка предоставления ПДн.
  2. Уполномоченным органом по защите информации и персональных данных является Управление информационных технологий и административного реформирования администрации Нефтеюганского района, которое:
     1. Осуществляет следующие основные функции по обеспечению безопасности ПДн:
        1. Передает список лиц, допущенных к работе с ПДн в ИСПДн, ответственному за организацию обработки персональных данных операторов.
        2. Принятие необходимых правовых, организационных и технических мер или обеспечивает их принятие для защиты персональных данных   
           от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.
        3. Обеспечение сохранность технических средств, носителей ПДн   
           и средств защиты информации.
        4. Исключение возможности неконтролируемого проникновения или пребывания посторонних лиц в помещениях, в которых расположены технические средства ИСПДн и (или) осуществляется обработка ПДн.
        5. Ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных,   
           а также хранятся носители информации.
     2. Осуществляет контроль за:
        1. Соответствием процесса обработки персональных данных Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных»   
           и принятыми в соответствии с ним нормативными правовыми актами, требованиями   
           к защите персональных данных, политикой операторов в отношении обработки персональных данных и локальными актами.
        2. Доведением до сведений всех работников операторов положений законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки ПДн и требований к защите ПДн, а также их права   
           и обязанности в этой области.
        3. Соблюдением прав субъектов ПДн.
        4. Соблюдением операторов и её работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
        5. Принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.
        6. Разбирательством и составлением заключений по фактам несоблюдения условий хранения носителей ПДн, использования средств защиты информации (далее также – СЗИ), которые могут привести к нарушению конфиденциальности ПДн или другим нарушениям, разработкой и принятием мер   
           по предотвращению возможных опасных последствий подобных нарушений.
        7. Содержанием и объемом обрабатываемых персональных данных.   
           ПДн должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.
        8. Передачей ПДн третьим лицам.
        9. Блокированием неправомерно обрабатываемых персональных данных, относящихся к субъекту персональных данных.
        10. Процессом прекращения обработки ПДн при отзыве субъектом ПДн согласия на обработку ПДн.
        11. Проведением мероприятий по исключению акустического   
            и визуального каналов утечки конфиденциальной информации.
        12. Соблюдением запрета записи ПДн на незарегистрированные носители информации.
  3. В соответствии с ч.1 ст.22.1 Федерального закона от 27.07.2006   
     № 152-ФЗ «О персональных данных» лицо, ответственное за организацию обработки ПДн назначается распоряжением администрации Нефтеюганского района. Предназначение, полномочия, обязанности лица, ответственного   
     за организацию обработки ПДн, определены Инструкцией лица, ответственного   
     за организацию обработки персональных данных, утвержденной приложением № 9   
     к постановлению Главы Нефтеюганского района от 01.07.2019 № 87-пг-нпа   
     «Об обработке персональных данных».
  4. Предназначение, полномочия, обязанности администратора безопасности информации определены Инструкцией администратора информационной безопасности информационных систем персональных данных операторов (приложение № 3 к настоящему постановлению).
  5. Обязанности пользователей ИСПДн определены Инструкцией пользователя ИСПДн операторов (приложение № 2 к настоящему постановлению).

1. Защита ПДн в процессе эксплуатации информационной системы
   1. Для обеспечения безопасности ПДн применяются следующие основные меры:
      1. Реализация матрицы допуска пользователей (обслуживающего персонала) к информационным ресурсам, информационной системе и связанным   
         с ее использованием работам, документам.
      2. Ограничение доступа пользователей в помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных,   
         а также, хранятся носители информации.
      3. Разграничение доступа пользователей и обслуживающего персонала   
         к информационным ресурсам, программным средствам обработки (передачи)   
         и защиты информации.
      4. Регистрация действий пользователей и обслуживающего персонала, контроль несанкционированного доступа и действий пользователей, обслуживающего персонала и посторонних лиц.
      5. Учет и хранение съемных носителей информации и их обращение, исключающее хищение, подмену и уничтожение.
      6. Резервирование технических средств, дублирование массивов   
         и носителей информации.
      7. Использование средств защиты информации, прошедших   
         в установленном порядке процедуру оценки соответствия.
      8. Использование защищенных каналов связи.
      9. Размещение технических средств, позволяющих осуществлять обработку персональных данных, в пределах охраняемой территории.
      10. Организация физической защиты помещений и собственно технических средств, позволяющих осуществлять обработку персональных данных.
      11. Предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) и программных закладок.
   2. Информационные системы персональных данных должны иметь комплект эксплуатационной документации, включающий в себя следующие документы:
      1. Описания технического, программного, информационного обеспечения   
         и технологии обработки (передачи) информации.
      2. Инструкции и руководства по эксплуатации технических и программных средств защиты для пользователей, администраторов системы, а также   
         для работников службы защиты информации.
      3. Технические паспорта.
      4. Журналы учета машинных носителей информации (далее также – МНИ), выдачи МНИ, регистрации инцидентов безопасности.
   3. Обязанности должностных лиц, в части касающийся обеспечения безопасности ПДн, изложены в:
      1. Инструкции лица, ответственного за организацию обработки персональных данных операторов.
      2. Инструкции администратора информационной безопасности информационных систем персональных данных операторов.
      3. Инструкции пользователя ИСПДн операторов.
   4. Выполнение отдельных технологических операций регламентируется инструкцией по антивирусной защите при работе в информационных системах персональных данных операторов.
   5. В случае изменения технологического процесса обработки информации, либо по результатам расследования инцидентов безопасности в инструкции могут быть внесены изменения.
   6. При обработке персональных данных в ИСПДн всеми работниками операторов должна соблюдаться Парольная политика:
      1. Личные пароли доступа к элементам ИСПДн выдаются администратором безопасности информации или создаются самостоятельно.
      2. Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 3 месяца.
      3. Об утере, компрометации, несанкционированном изменении паролей   
         и несанкционированном изменении сроков действия паролей необходимо незамедлительно сообщать администратору безопасности информации.
      4. При формировании пароля должны выполняться следующие правила:
         1. Пароль не должен содержать имя учетной записи пользователя или какую-либо его часть.
         2. Пароль должен состоять не менее чем из 6 символов.
         3. В пароле должны присутствовать символы минимум трех категорий   
            из числа следующих четырех:

прописные буквы английского алфавита от A до Z;

строчные буквы английского алфавита от a до z;

десятичные цифры (от 0 до 9);

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

* + - 1. Запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123456», «111111», «qwerty» и им подобные, а также имена   
         и даты рождения себя и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь   
         на информации о пользователе.
      2. Запрещается использовать в качестве пароля один и тот   
         же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;
      3. Запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);
      4. Запрещается выбирать пароли, которые уже использовались ранее.
    1. Во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).
    2. При вводе неверного имени или пароля предоставляется повторная попытка их введения. Количество попыток - 3 раза. В случае неверного ввода имени пользователя и (или) пароля за указанное число попыток персональная электронно-вычислительная машина (далее так же – ПЭВМ) блокируется и выдается сообщение   
       о необходимости вызова администратора безопасности информации.
    3. запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах.
    4. запрещается сообщать кому-либо личный пароль.
  1. Порядок работы с выводимыми на экран персональными данными
     1. Экран монитора в помещении должен располагаться во время работы так, чтобы исключалась возможность несанкционированного ознакомления   
        с отображаемой на нем информацией посторонними лицами, в зависимости   
        от этажности или наличия близлежащих зданий равной этажности и (или) выхода оконных проемов на неконтролируемую территорию, шторы должны быть завешаны (жалюзи закрыты).
     2. Должно обеспечиваться блокирование сеанса доступа пользователя после 5 минут бездействия или по запросу пользователя.
  2. Порядок работы с носителями персональных данных
     1. Информация из ИСПДн может отчуждаться либо на бумажные, либо на машинные носители информации (USB-накопители, оптические диски, магнитные дискеты). Право на отчуждение информации определяется «Матрицей доступа ...».
     2. При выводе персональных данных на бумажные носители необходимо исключить просмотр выводимой информации лицами, не допущенными к обработке ПДн.
     3. Выводимые на печать ПДн должны обособляться от иной,   
        не относящейся к ПДн, информации.
     4. Места хранения носителей персональных данных (комната, инв. номер шкафа (сейфа)), должностные лица, ответственные за их сохранность, вид носителя персональных данных определяются в документе «Перечень мест хранения материальных носителей персональных данных», разрабатываемом лицом, ответственным за организацию обработки (далее так же – ЛООО).
  3. Порядок учета машинных носителей информации
     1. В качестве машинных носителей информации (МНИ) в ИСПДн могут использоваться накопители на жесткий магнитный диск (далее так же – ЖМД),   
        USB-накопители, накопители на оптических дисках, дискеты.
     2. Все машинные носители информации, включая накопители на жестких магнитных дисках, входящие в состав системных блоков ЭВМ, должны быть зарегистрированы в «Журнале учета машинных носителей информации». Ответственный за регистрацию, хранение и выдачу МНИ — администратор безопасности информации.
     3. При регистрации на МНИ любым доступным способом наносятся: гриф «ПДн», регистрационный номер, дата регистрации и подпись лица, ответственного   
        за регистрацию.
     4. Зарегистрированные МНИ выдаются пользователям под роспись   
        в «Журнале учета выдачи машинных носителей информации».
     5. Запрещается запись информации, содержащей ПДн,   
        на незарегистрированные носители информации.
     6. Уничтожение МНИ осуществляется по акту, подписанному комиссией, способом, исключающим возможность восстановления информации.
  4. Порядок резервирования технических средств, дублирования массивов   
     и носителей информации
     1. Резервное копирование должно осуществлять на периодической основе:
        1. Для обрабатываемых персональных данных – не реже раза в неделю.
        2. Для технологической информации – не реже раза в месяц.
        3. Эталонные копии программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты),   
           с которых осуществляется их установка на элементы ИСПДн – не реже раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий).
     2. Данные о проведение процедуры резервного копирования, должны отражаться в специально созданном журнале учета.
     3. Носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования.
     4. Носители рекомендуется хранить в несгораемом шкафу   
        или помещении, оборудованном системой пожаротушения.
     5. Периодически должна проверяться возможность восстановления данных с резервных копий.

1. Регистрация событий безопасности
   1. В информационных системах персональных данных должны регистрироваться следующие события безопасности и информация, определяющая эти события:
      1. Попытки входа (выхода) субъектов доступа в информационную систему и загрузки (останова) операционной системы:

▪ дата и время входа (выхода) в систему (из системы) или загрузки (останова) операционной системы;

▪ результат попытки входа (успешная или неуспешная);

▪ результат попытки загрузки (останова) операционной системы (успешная или неуспешная);

▪ идентификатор, предъявленный при попытке доступа.

* + 1. Подключение машинных носителей информации и вывод информации   
       на носители информации:

▪ дата и время подключения машинных носителей информации и вывода информации на носители информации;

▪ логическое имя (номер) подключаемого машинного носителя информации;

▪ идентификатор субъекта доступа, осуществляющего вывод информации   
на носитель информации.

* + 1. Запуск (завершение) программ и процессов (заданий, задач), связанных   
       с обработкой защищаемой информации:

▪ дата и время запуска;

▪ имя (идентификатор) программы (процесса, задания);

▪ идентификатор субъекта доступа (устройства);

▪ запросившего программу (процесс, задание);

▪ результат запуска (успешный, неуспешный).

* + 1. Попытки доступа программных средств к определяемым операторами защищаемым объектам доступа (техническим средствам, узлам сети, линиям (каналам) связи, внешним устройствам, программам, томам, каталогам, файлам, записям, полям записей) и иным объектам доступа:

▪ дата и время попытки доступа к защищаемому объекту с указанием   
ее результата (успешная, неуспешная);

▪ идентификатор субъекта доступа (устройства);

▪ спецификацию защищаемого объекта доступа (логическое имя (номер).

* + 1. Попытки удаленного доступа:

▪ включать дату и время попытки удаленного доступа с указанием   
ее результата (успешная, неуспешная),

▪ идентификатор субъекта доступа (устройства);

▪ используемый протокол доступа;

▪ используемый интерфейс доступа;

▪ иную информацию о попытках удаленного доступа к информационной системе.

* 1. Срок хранения событий безопасности – не менее 3 лет.
  2. Защита информации о событиях безопасности обеспечивается СЗИ   
     от несанкционированного доступа (далее так же – НСД).
  3. Доступ к информации о событиях безопасности должен обеспечиваться только уполномоченным лицам

1. Контроль за обеспечением уровня защищенности ПДн
   1. В целях обеспечения заданных характеристик безопасности ИСПДн должен осуществляться контроль состояния и эффективности защиты информации.
   2. Контроль заключается в проверке по действующим методикам выполнения требований нормативных документов по защите информации, а также в оценке обоснованности и эффективности принятых мер.
   3. Контроль может быть повседневным, периодическим и внеплановым.
   4. Повседневный контроль, с целью своевременного обнаружения фактов НСД, проводится:
      1. Непосредственно пользователями автоматизированных рабочих мест перед началом и в ходе работы с защищаемой информацией.
      2. Администратором безопасности с выделенного рабочего места   
         с использованием встроенных средств мониторинга СЗИ и средствами обнаружения вторжений.
   5. Периодический, с целью тестирования функций системы защиты персональных данных с помощью тест-программ, имитирующих попытки несанкционированного доступа. Выполняется администратором безопасности информации или Лицензиатом по отдельному договору.
   6. Периодичность контроля определяется ЛООО и отражается в плане работ по защите информации.
   7. Внеплановый контроль выполняется в случаях изменения разрешительной системы, подозрения на НСД, распространения вирусных эпидемий и др. случаях.
   8. О проведениях периодического и внепланового контролей делается отметка в техническом паспорте ИСПДн.
2. Реагирование на инциденты информационной безопасности и сбои
   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. Происшествие, вызывающее инцидент, может произойти:
      1. В результате непреднамеренных действий пользователей.
      2. В результате преднамеренных действий пользователей и третьих лиц.
      3. В результате нарушения правил эксплуатации технических средств ИСПДн.
      4. В результате возникновения внештатных ситуаций и обстоятельств непреодолимой силы.
   3. Пользователи ИСПДн должны быть проинформированы о необходимости обращать внимание и сообщать о любых замечаниях или предполагаемых недостатках, или угрозах в области безопасности. При наличии такой информации пользователи должны сообщать ее администратору безопасности информации. Пользователи ни при каких обстоятельствах не должны самостоятельно искать подтверждения подозреваемому недостатку в системе безопасности, так как это может быть интерпретировано как неправомочное использование системы.
      1. Инцидентами нарушения информационной безопасности являются компрометация ключевой и (или) парольной информации (утеря или оставление без присмотра носителей ключевой и (или) парольной информации, разглашение пароля, ввод пароля в присутствии посторонних лиц), получение предупредительных сообщений от средств защиты ин- формации, странное поведение системы, подозрения в НСД, отсутствие (повреждение, недоступность информационных ресурсов), нарушение физической целостности технических средств или их печатей (пломб) и т.п.
      2. При возникновении (подозрении) инцидентов нарушения информационной безопасности пользователи информационной системы должны:
         1. Зафиксировать симптомы инцидента (появляющиеся сообщения).
         2. При необходимости блокировать скомпрометированные пароли.
         3. Физически отключить АРМ от локальной вычислительной сети (далее также – ЛВС), прекратить обработку ПДн.
         4. Не допускать использования МНИ на других АРМ.
         5. Незамедлительно информировать любыми доступными средствами своего непосредственного руководителя и администратора безопасности информации.
      3. Администратор безопасности информации при получении информации о возникновении (подозрении) инцидента безопасности информации должен:
         1. Принимать меры к сбору информации для расследования инцидента. При этом, копирование информации с носителей и оперативной памяти следует выполнять таким образом, чтобы обеспечить их доступность. Журнал всех действий, выполненных в течение процесса копирования необходимо сохранять, а сам процесс копирования необходимо документировать. Одну копию и журнал необходимо хранить безопасным способом.
         2. В случае предполагаемых судебных разбирательств на ранней стадии привлекать юриста или полицию для консультации относительно требуемых свидетельств.
         3. Принимать меры к смене утерянных (скомпрометированных) атрибутов доступа и ключей.
         4. Принимать меры к восстановлению системы. При нарушении целостности системы должна быть выполнена переустановка программного обеспечения (далее также – ПО) и СЗИ с оригинальных дистрибутивов.
         5. Регистрировать информацию об инцидентах нарушения информационной безопасности в специальном журнале.
         6. Докладывать лицу, ответственному за организацию обработки ПДн,   
            о инцидентах безопасности информации.
         7. Периодически, совместно с ЛООО, проводить анализ зарегистрированных инцидентов с целью совершенствования существующих или внедрения дополнительных мероприятий по обеспечению безопасности ПДн.
         8. Использовать информацию об инцидентах с целью повышения информированности пользователей.
      4. По фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести   
         к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, лицо, ответственное за организацию обработки ПДн, назначает разбирательство.   
         По результатам разбирательства разрабатываются меры по предотвращению возможных опасных последствий подобных нарушений, и вся информация докладывается Главе Нефтеюганского района.
      5. При обнаружении нарушений порядка предоставления ПДн пользователям информационной системы Глава Нефтеюганского района отдает распоряжение о приостановке предоставления персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин.

Приложение № 2

к постановлению администрации

Нефтеюганского района

от 01.08.2019 № 1636-па

# ИНСТРУКЦИЯ пользователя информационной системы персональных данных

1. Общие положения
   1. Пользователь ИСПДн (далее – Пользователь) осуществляет обработку персональных данных в информационной системе персональных данных.
   2. Пользователем является каждый работник операторов, участвующий   
      в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.
   3. Настоящая инструкция содержит общие сведения о работе пользователя   
      на защищенной от несанкционированного доступа автоматизированной системе (АС) при обработке персональных данных и является дополнением к его должностным обязанностям.
   4. Пользователь несет персональную ответственность за свои действия.
   5. Пользователь в своей работе руководствуется настоящей инструкцией,   
      и другими регламентирующими документами администрации Нефтеюганского района.
   6. Обработка персональных данных должна осуществляться с соблюдением принципов и правил, предусмотренных Федеральным закона «О персональных данных».
   7. В случае получения согласия на обработку персональных данных   
      от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от имени субъекта персональных данных проверяются работниками операторов.
   8. Пользователям запрещается осуществлять обработку персональных данных, не указанных в «Перечне конфиденциальной информации (в том числе персональных данных), обрабатываемой в СО ПДн «Сауми», «Кодекс: Управление персоналом», «1С:Предприятие», «1С:Зарплата и Кадры» операторов», «СЭД ОБРАЩЕНИЕ ГРАЖДАН».
   9. При наличии технической возможности, пользователь должен удалять или обезличивать обрабатываемые персональные данные по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное   
      не предусмотрено федеральным законом.
   10. При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность   
       по отношению к целям обработки персональных данных. Пользователи должны принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.
   11. В случае выявления неправомерной обработки персональных данных пользователь обязан осуществить блокирование неправомерно обрабатываемых персональных данных или обеспечить их блокирование.
   12. Методическое руководство работой пользователя в вопросах защиты ПДн осуществляется администратором безопасности информации.
2. Обязанности Пользователя
   1. Перед работой на защищаемом АРМ Пользователь должен пройти соответствующую подготовку (инструктаж), и ознакомиться под роспись   
      с «Перечнем конфиденциальной информации (в том числе персональных данных), обрабатываемой в СО ПДн «Сауми», «Кодекс: Управление персоналом», «1С:Предприятие», «1С:Зарплата и Кадры», «СЭД ОБРАЩЕНИЕ ГРАЖДАН» операторов», и внутренними документами, устанавливающими порядок обработки ПДн, а также своими правами и обязанностями в этой области.
   2. Пользователь обязан знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководств по защите информации и распоряжений, регламентирующих порядок действий по защите информации.
   3. При сборе персональных данных пользователь обязан предоставить субъекту персональных данных по его просьбе информацию, касающуюся обработки его персональных данных, в том числе содержащей:
      1. Подтверждение факта обработки персональных данных операторами.
      2. Правовые основания и цели обработки персональных данных.
      3. Цели и применяемые операторами способы обработки персональных данных.
      4. Место нахождения операторов, сведения о лицах (за исключением работников операторов), которые имеют доступ к персональным данным   
         или которым могут быть раскрыты на основании договора с операторами или   
         на основании федерального закона.
      5. Обрабатываемые персональные данные, относящиеся   
         к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом.
      6. Сроки обработки персональных данных, в том числе сроки их хранения.
      7. Порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом «О персональных данных».
      8. Информацию об осуществленной или о предполагаемой трансграничной передаче данных.
      9. Наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению операторов, если обработка поручена или будет поручена такому лицу.
      10. Иные сведения, предусмотренные федеральными законами.
   4. В случае отказа субъекта ПДн от предоставления персональных данных, являющихся обязательными в соответствии с федеральным законом, пользователь обязан разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.
   5. При получении персональных данных не от субъекта персональных данных, пользователь, до начала обработки таких персональных данных обязан предоставить субъекту персональных данных следующую информацию:
      1. Наименование, либо фамилию, имя, отчество и адрес операторов или его представителя.
      2. Цель обработки персональных данных и ее правовое основание.
      3. Предполагаемые пользователи персональных данных.
      4. Установленные Федеральным законом «О персональных данных» права субъекта персональных данных.
      5. Источник получения персональных данных.
   6. Пользователь освобождается от обязанности предоставить субъекту персональных данных сведения, предусмотренные п.2.5 настоящей Инструкции,   
      случаях, если:
      1. Субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим операторами.
      2. Персональные данные получены операторами на основании федерального закона или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.
      3. Персональные данные сделаны общедоступными субъектом персональных данных или получены из общедоступного источника.
      4. Операторы осуществляют обработку персональных данных для статистических или иных исследовательских целей, для осуществления профессиональной деятельности журналиста либо научной, литературной или иной творческой деятельности, если при этом не нарушаются права и законные интересы субъекта персональных данных.
      5. Предоставление субъекту персональных данных сведений, предусмотренных п.2.5 настоящей Инструкции, нарушает права и законные интересы третьих лиц.
   7. Пользователь обязан соблюдать условия использования средств защиты информации, предусмотренных эксплуатационной и технической документации.
   8. Для получения справочной информации о СЗИ от НСД «Secret Net 7»   
      и выполнения ряда функций пользователю необходимо ознакомиться с документом «Средство защиты информации Secret Net 7. Руководство пользователя».
   9. Пользователь обязан соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн, а также руководящих   
      и организационно-распорядительных документов.
   10. Пользователь должен осуществлять свою деятельность в соответствии   
       с правилами разграничения доступа, определенными в документах «Матрица доступа к ресурсам СО ПДн «Сауми», «Кодекс: Управление персоналом», «1С:Предприятие», «1С:Зарплата и Кадры», «СЭД ОБРАЩЕНИЕ ГРАЖДАН» операторов.
   11. Соблюдать требования парольной политики (раздел 4 настоящей Инструкции).
   12. Соблюдать правила при работе в сетях общего доступа и (или) международного обмена – Интернет и других (раздел 7 настоящей Инструкции).
   13. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой   
       на них информацией посторонними лицами, в зависимости от этажности или наличия близлежащих зданий равной этажности и (или) выхода оконных проемов   
       на неконтролируемую территорию, шторы должны быть завешаны (жалюзи закрыты).
   14. Перед началом работы, пользователь должен убедиться в актуальности антивирусных баз.
   15. Обо всех выявленных нарушениях, связанных с информационной безопасностью, а также для получения консультаций по вопросам информационной безопасности, необходимо обратиться к администратору безопасности информации
   16. Для получения консультаций по вопросам работы и настройке элементов ИСПДн необходимо обращаться к Системному администратору.
   17. Для хранения информации, содержащей конфиденциальную информацию, должны использоваться только машинные носители информации (МНИ), поставленные на учет операторами. Ответственный за регистрацию МНИ – администратор безопасности информации.
   18. При отсутствии визуального контроля за рабочей станцией доступ   
       к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Win><L>.
   19. В случае возникновения внештатных и аварийных ситуаций, с целью ликвидации их последствий, в пределах возложенных на него функций пользователь должен принимать соответствующие меры по реагированию.
3. Пользователю запрещается
   1. Распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральными законами.
   2. Копировать защищаемую информацию на внешние носители   
      без разрешения своего руководителя, если это непосредственно не предусмотрено должностными обязанностями.
   3. Самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств.
   4. Несанкционированно открывать общий доступ к папкам на своей рабочей станции.
   5. Подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства.
   6. Отключать (блокировать) средства защиты информации.
   7. Обрабатывать на АРМ информацию и выполнять другие работы,   
      не предусмотренные должностными обязанностями.
   8. Сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн.
   9. Привлекать посторонних лиц для производства ремонта или настройки АРМ.
   10. В процессе работы на ПЭВМ озвучивать голосом обрабатываемую информацию.
4. Организация парольной защиты
   * 1. Личные пароли доступа к элементам ИСПДн выдаются пользователям администратором безопасности информации или создаются самостоятельно.
     2. Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 3 месяца.
     3. Лица, использующих паролирование, обязаны:
5. четко знать и строго выполнять требования настоящей инструкции   
   и других руководящих документов по паролированию;
6. своевременно сообщать администратору безопасности информации   
   об утере, компрометации, несанкционированном изменении паролей   
   и несанкционированном изменении сроков действия паролей.
   * 1. Пароль не должен содержать имя учетной записи пользователя или какую-либо его часть.
     2. Пароль должен состоять не менее чем из 6 символов.
     3. В пароле должны присутствовать символы трех категорий из числа следующих четырех:

прописные буквы английского алфавита от A до Z;

строчные буквы английского алфавита от a до z;

десятичные цифры (от 0 до 9);

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

* + 1. Запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123456», «111111», «qwerty» и им подобные, а также имена   
       и даты рождения себя и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь   
       на информации о пользователе.
    2. Запрещается использовать в качестве пароля один и тот   
       же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;
    3. Запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);
    4. Запрещается выбирать пароли, которые уже использовались ранее.
    5. Ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан.
    6. Во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).
    7. При вводе неверного имени или пароля предоставляется повторная попытка их введения. Количество попыток - 3 раза. В случае неверного ввода имени пользователя и (или) пароля за указанное число попыток ПЭВМ блокируется   
       и выдается сообщение о необходимости вызова администратора безопасности информации.
    8. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах.
    9. Запрещается сообщать другим пользователям личный пароль   
       и регистрировать их в системе под своим паролем.

1. Порядок работы с персональными идентификаторами (USB-ключами)
   1. Персональный идентификатор выдается администратором безопасности информации.
   2. Персональный идентификатор используется для входа   
      в автоматизированную систему — при появлении экрана приветствия (приглашение на вход в систему) необходимо предъявить свой персональный идентификатор   
      и ввести пароль. При вводе правильного пароля осуществится вход в систему.
   3. Пользователю запрещается:
      1. Передавать персональный идентификатор другим пользователям.
      2. Оставлять персональный идентификатор в компьютере в случае покидания рабочего места.
   4. Пользователь обязан сообщать администратору безопасности информации об утере и повреждении персонального идентификатора.
2. Порядок работы на АС
   1. Перед началом работы убедиться в целостности печати (пломбы)   
      на системном блоке, отсутствии подключения посторонних устройств.
   2. Для входа в автоматизированную систему используется два способа:
      1. При помощи имени пользователя и пароля.
      2. При помощи персонального идентификатора и пароля.
   3. Создание файлов на ЖМД, их корректировка и другие действия   
      с информацией выполняются пользователем в соответствии с инструкцией используемой версии операционной системы и пакета прикладных программ.
   4. Хранение защищаемых файлов должно осуществляться   
      в регламентированных папках в соответствии с документом «Матрица доступа   
      к ресурсам СО ПДн «Сауми», «Кодекс: Управление персоналом», «1С:Предприятие», «1С:Зарплата и Кадры», «СЭД ОБРАЩЕНИЕ ГРАЖДАН» администрации Нефтеюганского района.
   5. Копирование защищаемой информации должно осуществляться пользователем на МНИ, учтенных операторами.
   6. Перед работой с информацией на отчуждаемых МНИ пользователь обязан убедиться в отсутствии на них вирусов с использованием штатных антивирусных программ, установленных на АС, в соответствии с документом «Инструкция   
      по антивирусной защите при работе в информационных системах персональных данных операторов.
   7. В случае обнаружения вирусов на МНИ пользователь обязан прекратить работу на АС и сообщить об этом администратору безопасности информации. Возобновление работы производить после получения разрешения от администратора безопасности информации.
3. Правила работы в сетях общего доступа и (или) международного обмена
   1. Работа в сетях общего доступа и (или) международного обмена (сети Интернет и других) (далее – Сеть) на элементах ИСПДн, должна проводиться   
      при служебной необходимости.
   2. При работе в Сети запрещается:
      1. Осуществлять работу при отключенных средствах защиты (антивирус   
         и других).
      2. Передавать по Сети защищаемую информацию без использования средств шифрования.
      3. Запрещается скачивать из Сети программное обеспечение и другие файлы.
      4. Запрещается посещение сайтов сомнительной репутации (порно-сайты, сайты содержащие нелегально распространяемое ПО и другие).
      5. Запрещается нецелевое использование подключения к Сети.
4. Реагирование на инциденты нарушения информационной безопасности и сбои
   1. Пользователь должен обращать внимание и сообщать о любых замечаниях или предполагаемых недостатках или угрозах в области безопасности. При наличии такой информации пользователь должен сообщать ее администратору безопасности информации. Пользователь ни при каких обстоятельствах не должен самостоятельно искать подтверждения подозреваемому недостатку в системе безопасности, так как это может быть интерпретировано как неправомочное использование системы.
   2. Инцидентами нарушения информационной безопасности являются компрометация парольной информации (разглашение пароля, ввод пароля   
      в присутствии посторонних лиц), получение предупредительных сообщений   
      от средств защиты информации, странное поведение системы, подозрения в НСД, отсутствие (повреждение, недоступность информационных ресурсов), нарушение физической целостности технических средств или их печатей (пломб), утеря персонального идентификатора и т.п.
   3. При возникновении (подозрении) инцидентов нарушения информационной безопасности пользователь информационной системы должен:

зафиксировать симптомы инцидента (появляющиеся сообщения);

физически отключить АРМ от ЛВС, прекратить обработку ПДн;

не допускать использования МНИ на других АРМ;

незамедлительно информировать любыми доступными средствами своего непосредственного руководителя и администратора безопасности информации.

1. Ответственность

Пользователь ИСПДн несет ответственность за нарушение требований обработки конфиденциальной информации.

Приложение № 3

к постановлению администрации

Нефтеюганского района

от 01.08.2019 № 1636-па

# ИНСТРУКЦИЯ администратора информационной безопасности информационных систем персональных данных

1. Общие положения
   1. Настоящая Инструкция определяет основные функции, обязанности, права и ответственность администратора безопасности информации при эксплуатации ИСПДн и является дополнением к действующим нормативным документам   
      по вопросам обеспечения режима обращения конфиденциальной информации   
      и не исключает обязательного выполнения их требований. С настоящей Инструкцией должен быть под роспись ознакомлен администратор безопасности информации.
   2. Администратор безопасности информации назначается распоряжением администрации Нефтеюганского района.
   3. Администратор безопасности информации подчиняется лицу, ответственному за организацию обработки ПДн.
   4. Администратор безопасности информации в своей работе руководствуется настоящей инструкцией, Инструкцией по обеспечению безопасности СО ПДн,   
      и другими локально-нормативными актами администрации Нефтеюганского района.
   5. Администратор безопасности информации отвечает за поддержание необходимого уровня безопасности объектов защиты.
   6. Администратор безопасности информации является ответственным должностным лицом администрации Нефтеюганского района, уполномоченным   
      на проведение работ по технической защите информации и поддержанию достигнутого уровня защиты ИСПДн и ее ресурсов на этапах промышленной эксплуатации и модернизации.
   7. Администратор безопасности информации должен иметь специальное рабочее место, размещенное в здании администрации Нефтеюганского района так, чтобы исключить несанкционированный доступ к нему посторонних лиц и других пользователей.
   8. Администратор безопасности информации осуществляет методическое руководство пользователей ИСПДн и системных администраторов, в вопросах обеспечения безопасности ПДн.
   9. Требования администратора безопасности информации, связанные   
      с выполнением им своих должностных обязанностей, обязательны для исполнения всеми пользователями ИСПДн.
   10. Администратор безопасности информации несет персональную ответственность за качество проводимых им работ по контролю действий пользователей при работе в ИСПДн, состояние и поддержание установленного уровня защиты ИСПДн.
2. Основные функции администратора безопасности информации
   1. Предоставление пользователям ИСПДн операторов технической возможности уничтожать либо обезличивать ПДн в случаях. В случае невозможности выполнения данной функции пользователями ИСПДн, обязанности по удалению или обезличиванию ПДн лежат на администраторе безопасности информации.
   2. По указанию лица, ответственного за организацию обработки ПДн, администратор безопасности информации предоставляет пользователям ИСПДн операторов возможность осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к субъекту персональных данных.
   3. Подготовка и корректировка, при необходимости, инструкции пользователей защищаемых ИСПДн.
   4. Выполнение всех действий по настройке и сопровождению СЗПДн   
      в процессе ее эксплуатации.
   5. Проверка готовности средств защиты информации к использованию   
      с составлением заключений о возможности их эксплуатации.
   6. Настройка и сопровождение подсистемы управления доступом   
      к информации в процессе эксплуатации ИСПДн включает:
      1. Подготовку идентификаторов и паролей доступа, доведение   
         их до пользователей.
      2. Формирование матрицы доступа для ИСПДн.
      3. Настройку полномочий для каждого пользователя ко всем элементам защищаемых информационных ресурсов в соответствии с требованиями документов «Матрица доступа к ресурсам СО ПДн «Сауми», «Кодекс: Управление персоналом», «1С:Предприятие», «1С:Зарплата и Кадры», «СЭД ОБРАЩЕНИЕ ГРАЖДАН» администрации Нефтеюганского района.
      4. Ввод описаний пользователей ИСПДн в информационные базы СЗИ, установленных в ИСПДн.
      5. Разблокирование ПЭВМ, анализ информации о несанкционированных действиях (НСД).
      6. Своевременное удаление описания пользователя из базы данных СЗИ при смене пользователя.
      7. Контроль состава технических средств и программного обеспечения ИСПДн.
      8. Контроль за отсутствием физического доступа к основным техническим средствам и системе (далее так же – ОТСС) (опечатывание).
   7. Настройка и сопровождение подсистемы регистрации и учета действий пользователей при работе в ИСПДн включает:
      1. Определение информации, подлежащей регистрации в системном журнале СЗИ;
      2. регулярное проведение анализа системного журнала для выявления попыток несанкционированного доступа к защищаемым ресурсам;
      3. сохранение зарегистрированной информации, необходимой для возможного расследования фактов НСД или восстановления информационных ресурсов.
   8. Сопровождение подсистемы обеспечения целостности информации ИСПДн включает:
      1. Тестирование установленной в ИСПДн СЗИ от НСД при изменении программной среды или полномочий пользователей.
      2. Восстановление программной среды, программных средств и настроек СЗИ при сбоях.
      3. Создание двух копий дистрибутивов программных средств СЗИ от НСД, контроль их работоспособности и целостности.
      4. Контроль поддержания установленного порядка и правил антивирусной защиты информации в ИСПДн со стороны пользователей.
      5. Участие в периодическом обновлении антивирусных средств, установленных в ИСПДн.
   9. 2.9 Немедленное реагирование на инциденты безопасности.
3. Обязанности

Администратор безопасности информации обязан:

* 1. Знать сведения, необходимые для установки, настройки и управления СЗИ установленных операторами, изложенные в технической документации, поставляемой совместно с дистрибутивами СЗИ.
  2. Передавать в опечатанном виде на хранение лицу, ответственному   
     за организацию обработки, и поддерживать в актуальном состоянии информацию   
     о паролях привилегированных пользователей всех систем (администраторов, серверов, АРМ, СУБД и т.п).
  3. Проверять готовность средств и систем защиты информации к работе   
     поддерживать их работоспособность.
  4. Периодически анализировать состояние защиты ИСПДн и ее отдельных подсистем.
  5. Контролировать неизменность состояния средств защиты их параметров   
     и режимов защиты.
  6. Проводить обучение лиц, использующих средства защиты информации, применяемые в информационных системах администрация Нефтеюганского района, правилам работы с ними.
  7. Контролировать исполнение пользователями ИСПДн введенного режима безопасности, а также соблюдение правил работы с элементами ИСПДн и средствами защиты информации.
  8. Контролировать размещение информационных систем, специального оборудования и охрану помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключение возможности неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.
  9. Контролировать соответствие фактического состава пользователей   
     и объектов доступа ИСПДн с данными документа «Матрица доступа к ресурсам   
     СО ПДн «Сауми», «Кодекс: Управление персоналом», «1С:Предприятие», «1С:Зарплата и Кадры», «СЭД ОБРАЩЕНИЕ ГРАЖДАН» администрации Нефтеюганского района с внесением изменений в него при необходимости.
  10. Не допускать к работе на элементах ИСПДн посторонних лиц.
  11. Периодически тестировать функции системы защиты ПДн с помощью тест-программ, имитирующих попытки несанкционированного доступа   
      к информации
  12. Периодически контролировать соответствие фактического состава технических средств и программного обеспечения ИСПДн с данными технического паспорта, целостность печатей (пломб) системных блоков ОТСС.
  13. Осуществлять контроль качества резервных и архивных копий СЗИ.
  14. Контролировать резервное копирование информации в ИСПДн.
  15. Осуществлять резервное копирование конфигураций и журналов регистрации событий компонентов СЗПДн.
  16. Осуществлять контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией.
  17. Регулярно осуществлять обновление антивирусных баз и производить проверку на отсутствие вирусов.
  18. Принимать меры по восстановлению в случае неработоспособности операционной системы, прикладных программ и системы защиты информации. Если восстановление функционирования программной среды штатными средствами операционной системы невозможно или не было заранее подготовлено,   
      то необходима полная переустановка ПО.
  19. Допускать к обслуживанию и ремонту технических средств работников, имеющих соответствующее разрешение на работу.
  20. Проводить учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, в документе «Технический паспорт...» на ИСПДн.
  21. Регистрировать и проводить учет машинных носителей ПДн.
  22. Уничтожать машинные носители ПДн.
  23. Снимать все узлы и блоки с элементами накопления и хранения ПДн (ЖМД, USB-накопители и т.д.) и оставлять их в хранилищах при сдаче в ремонт технических средств ИСПДн.
  24. Участвовать в приемке новых программных средств.
  25. Передавать пользователям персональные идентификаторы и вести журнал их выдачи.
  26. Принимать меры по немедленному реагированию на инциденты безопасности ПДн.
  27. Докладывать лицу, ответственному за организацию обработки ПДн,   
      о нештатных ситуациях на объектах ИСПДн, инцидентах нарушения информационной безопасности идопущенных пользователями нарушениях установленных требований по защите информации.

1. Права
   1. Участвовать в анализе ситуаций, касающихся функционирования средств защиты информации, и в расследовании фактов несанкционированного доступа.
   2. Требовать прекращения обработки информации в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации.
2. Ответственность

Администратор безопасности информации несет ответственность за:

* 1. Разглашение сведений, составляющих конфиденциальную информацию, ставшую известной ему по роду работы.
  2. Несанкционированное предоставление доступа к защищаемой информации, передачу посторонним лицам информацию об идентификаторах   
     и паролях пользователей.
  3. Несанкционированное отключение СЗИ в ИСПДн.
  4. Использование чужих учетных данных для маскирования своих действий, ввод ложной информации в ИСПДн.
  5. Некачественное проведение работ по обеспечению защиты информации   
     и сопровождению используемой СЗИ.

Приложение № 4

к постановлению администрации

Нефтеюганского района

от 01.08.2019 № 1636-па

# ИНСТРУКЦИЯ по антивирусной защите при работе в информационных системах персональных данных

1. Общие положения
   1. Настоящая Инструкция разработана в соответствии с ГОСТ Р 51188-98 «Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство», введенного постановлением Госстандарта России   
      от 14.07.1998 № 295 «Государственный стандарт Российской Федерации средства программные систем вооружения порядок разработки», и предназначена для организации порядка проведения антивирусного контроля операторами с целью предотвращения несанкционированных вредоносных воздействий   
      на информационные ресурсы операторов и возникновения фактов заражения программного обеспечения компьютерными вирусами.
   2. Требования настоящей Инструкции обязательны для выполнения всеми пользователями, обрабатывающими персональные данные посредством электронно-вычислительной техники операторов.
   3. Инструкция устанавливает обязанности пользователей, ответственность   
      за соблюдением мероприятий по защите от вирусов, определяет порядок антивирусного контроля на автономных средствах вычислительной техники, обновления баз вирусных сигнатур и антивирусного программного обеспечения, действий при обнаружении компьютерных вирусов.
2. Антивирусное программное обеспечение
   1. В ИСПДн операторов в качестве антивирусного средства используется сертифицированное по требованиям безопасности информации антивирусное программное обеспечение «Kaspersky Endpoint Security 10 для Windows».
   2. Использование указанного антивирусного ПО должно осуществляться   
      в соответствии с инструкцией пользователя антивирусной программы.
3. Обязанности пользователей
   1. Изучить настоящую Инструкцию и ознакомиться с необходимостью несения ответственности за выполнение ее требований под роспись.
   2. В ходе работы в ИСПДн следить за работоспособностью установленного антивирусного ПО и своевременностью установки обновлений компонентов антивирусной программы и вирусных баз.
   3. Сообщать администратору безопасности информации о необходимости проведения обновления антивирусной программы.
   4. Прекращать работу в ИСПДн и сообщить администратору безопасности информации о сигнализации антивирусной программы о вирусной активности.
   5. При проведении работ в ИСПДн с использованием внешних МНИ пользователь обязан перед первым обращением к используемому МНИ проверить его на наличие вредоносных программ и закладок.
   6. Использовать антивирусное программное обеспечение при работе   
      с сетями общего пользования (Интернет).
4. Пользователю запрещается
   1. Отключать средства антивирусной защиты и самостоятельно вносить изменения в настройки антивирусного ПО.
   2. Использовать средства антивирусной защиты информации, отличные   
      от поддерживаемых операторами.
5. Порядок антивирусного контроля
   1. Обязательному антивирусному контролю подлежит любая информация, вводимая с отчуждаемых машинных носителей и полученная из сетей общего пользования.
   2. После установки или изменения программного обеспечения антивирусный контроль должен осуществляться для жестких магнитных дисков.
   3. Профилактический антивирусный контроль должен проводиться не реже одного раза в неделю с лечением (уничтожением) обнаруженных зараженных объектов.
   4. Перед проведением контроля необходимо обновить имеющееся антивирусное ПО до последней версии компонентов ПО и вирусных баз.
   5. При возникновении подозрения на наличие компьютерных вирусов (нестабильная работа ПЭВМ, появление графических или звуковых эффектов, искажения данных и т.п.) следует незамедлительно сообщить об этом администратору безопасности информации, и провести антивирусный контроль ПЭВМ.
   6. При обнаружении вирусов принять меры по недопущению   
      их распространения: определить отчуждаемые машинные носители информации (МНИ), использованные в работе за период после последнего антивирусного контроля, и проверить их на наличие вирусов. Провести лечение или уничтожение зараженных файлов на ЖМД и отчуждаемых МНИ.
   7. При обнаружении нового вируса, не поддающегося лечению применяемыми антивирусными средствами, направить зараженный вирусом файл   
      на гибком магнитном диске в организацию, с которой заключен договор   
      на антивирусную поддержку. Данный файл не должен содержать информацию ограниченного распространения.
6. Порядок обновления баз вирусных сигнатур и антивирусного   
   программного обеспечения
   1. Установка и обновление средств антивирусного контроля на технических средствах ИСПДн осуществляется администратором безопасности информации.
   2. Обновления компонентов антивирусного ПО и баз данных вирусных сигнатур администратор безопасности информации получает по сети Интернет   
      с сайта производителя антивирусного ПО.
7. Ответственность за соблюдением мероприятий по защите от вирусов
   1. Администратор безопасности информации несет ответственность за:
      1. Своевременное получение и распространение обновленных баз данных вирусных сигнатур.
      2. Своевременное обновление новых лицензионных ключей   
         на антивирусное ПО при истечении их срока действия.
      3. Обучение пользователей правилам антивирусного контроля.
      4. Соблюдение графика антивирусного контроля пользователями.
      5. Последствия заражения ПЭВМ компьютерными вирусами   
         в соответствии с действующим Российским законодательством.
   2. Администратор безопасности информации имеет право:
      1. Вносить предложения по совершенствованию системы антивирусной защиты информации операторов.
      2. Проводить служебные проверки по фактам заражения программными вирусами автоматизированных систем обработки информации и средств вычислительной техники.
   3. Пользователь несет ответственность за:
      1. Допущенное по своей халатности заражение ПЭВМ компьютерными вирусами.
      2. Последствия заражения ПЭВМ компьютерными вирусами   
         в соответствии с действующим Российским законодательством.

Приложение № 5

к постановлению администрации

Нефтеюганского района

от 01.08.2019 № 1636-па

Инструкция

ответственного за защиту информации

Перечень сокращений

|  |  |  |
| --- | --- | --- |
| ИБ |  | - информационная безопасность; |
| ИСПДн |  | - информационная система персональных данных; |
| ПДн |  | - персональные данные; |
| СВТ |  | - средства вычислительной техники. |

1. Общие положения

* 1. Настоящая Инструкция ответственного за защиту информации определяет основные права и обязанности ответственного за защиту информации, обрабатываемой в информационных системах персональных данных   
     в администрации Нефтеюганского района.
  2. Ответственный за защиту информации:
* назначается распоряжением администрации Нефтеюганского района;
* руководствуется требованиями нормативных документов Российской Федерации, нормативных актов администрации Нефтеюганского района, настоящей Инструкцией, а также другими распорядительными документами в части, его касающейся;
* в пределах своих функциональных обязанностей обеспечивает руководство процессом обеспечения безопасности ПДн, контроль над соблюдением инструкций по работе с ИСПДн, а также в пределах своих полномочий принимает меры при выявлении несоблюдения требований по защите ПДн, по привлечению   
  к ответственности виновных лиц;
* обеспечивает безопасность информации, обрабатываемой, передаваемой   
  и хранимой при помощи средств вычислительной техники в ИСПДн администрации Нефтеюганского района, а также обрабатываемой без использования средств автоматизации;
  1. Ответственный за защиту информации и администратор информационной безопасности, определенные муниципальным правовым актом администрации Нефтеюганского района, организуют проверку ИСПДн на предмет несанкционированного доступа к конфиденциальной информации   
     и наличие документов и машинных носителей информации.

2. Обязанности ответственного за защиту информации

Ответственный обязан:

* + 1. четко знать и выполнять требования действующих нормативных   
       и руководящих документов, а также внутренних инструкций, руководства по защите информации (в том числе персональных данных) и распоряжений, регламентирующих порядок действий по защите информации;
    2. разрабатывать и поддерживать в актуальном состоянии Перечень персональных данных, обрабатываемых в администрации Нефтеюганского района;
    3. организовывать подачу уведомлений в уполномоченный орган по защите прав субъектов персональных данных;
    4. знать перечень подразделений, где осуществляется обработка ПДн, а также лиц, допущенных к обработке ПДн;
    5. знать перечень задач, решаемых с использованием СВТ, по обработке ПДн;
    6. в случае увольнения, все носители защищаемой информации (рукописи, черновики, чертежи, диски, дискеты, распечатки с принтеров, модели, материалы, изделия и пр.), которые находились в его распоряжении в связи с выполнением   
       им служебных обязанностей во время работы передать начальнику подразделения,   
       в штате которого он состоит;
    7. производить классификацию информационных систем персональных данных, разрабатывать и представлять на утверждение Главе Нефтеюганского района акты определения уровня защищенности ИСПДн;
    8. разрабатывать и поддерживать в актуальном состоянии модели угроз безопасности персональных данных;
    9. организовывать работы по разработке внутренних нормативных документов по защите ПДн, принимать участие в их актуализации, представлять документы на утверждение Главе Нефтеюганского района;
    10. распределять ответственность по вопросам обработки ПДн   
        и обеспечению безопасности ПДн между исполнителями;
    11. проводить мероприятия по контролю лояльности администратора ИБ ИСПДн;
    12. определять необходимость обучения сотрудников по вопросам обеспечения безопасности ПДн, формы и программы обучения сотрудников администрации Нефтеюганского района;
    13. осуществлять контроль за целевым использованием автоматизированного рабочего места, а также всех его внешних устройств, за выполнением пользователями СВТ установленного комплекса мероприятий по обеспечению безопасности информации;
    14. контролировать целостность печатей (пломб) на устройствах СВТ;
    15. осуществлять плановые и внеплановые проверки соблюдения требований всех лиц, допущенных к обработке ПДн, а также выполнять другие возложенные на него работы в соответствии с распорядительными, инструктивными и методическими материалами в части, его касающейся;
    16. осуществлять контроль соответствия изменений в составе и архитектуре ИСПДн требованиям нормативных документов Российской Федерации по защите ПДн, а также внутренних организационно-распорядительных документов администрации Нефтеюганского района;
    17. обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических СВТ   
        и отправке их в ремонт;
    18. контролировать ввод в действие, эксплуатацию системы защиты персональных данных;
    19. рассматривать поступающие предложения по усовершенствованию системы защиты персональных данных;
    20. контролировать своевременное обновление программного обеспечения элементов ИСПДн и системы защиты ПДн по мере появления таких обновлений;
    21. осуществлять контроль за порядком учета, создания, хранения   
        и использования резервных и архивных копий массивов данных, машинных (выходных) документов;
    22. в случае возникновения нештатных ситуаций (сбоев) принимать меры согласно требованиям соответствующих инструкций;
    23. контролировать ведение «Журнала учета нештатных ситуаций»;
    24. проводить служебные расследования фактов нарушений или угроз нарушения безопасности защищаемой информации;
    25. организовывать и осуществлять взаимодействие с надзорными   
        и регулирующими органами по вопросам защиты ПДн.

3. Права ответственного за защиту информации

Ответственный имеет право:

* + 1. требовать от пользователей безусловного соблюдения установленной технологии обработки персональных данных, выполнения требований внутренних документов администрации Нефтеюганского района, регламентирующих вопросы обеспечения безопасности ПДн;
    2. контролировать работу пользователей в части соблюдения ими требований по обеспечению безопасности ПДн;
    3. требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования СВТ;
    4. инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности в ИСПДн   
       в администрации Нефтеюганского района;
    5. инициировать привлечение к ответственности сотрудников администрации Нефтеюганского района, не соблюдающих установленные требования   
       по обеспечению безопасности персональных данных.

4. Ответственность ответственного за защиту информации

4.1. Ответственный несет ответственность:

* за ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей Инструкцией, другими инструктивными документами в соответствии с действующим трудовым законодательством Российской Федерации;
* за полноту и качество проводимых им работ по обеспечению безопасности персональных данных;
* за правонарушения, совершенные в процессе своей деятельности   
  в пределах, определенных действующим административным, уголовным   
  и гражданским законодательством Российской Федерации;
* за разглашение сведений конфиденциального характера и другой защищаемой информации администрации Нефтеюганского района в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.

5. Порядок пересмотра инструкции

Инструкция подлежит полному пересмотру при изменении требований законодательства Российской Федерации в части обеспечения безопасности персональных данных, приводящих к существенным изменениям технологии обработки и обеспечения безопасности персональных данных. Полный пересмотр Инструкции проводится ответственным за защиту информации по согласованию   
с Главой Нефтеюганского района с целью проверки соответствия ее положений реальным условиям применения их в администрации Нефтеюганского района. Инструкция подлежит частичному пересмотру в остальных случаях. Частичный пересмотр проводится ответственным за защиту информации в администрации Нефтеюганского района. Вносимые изменения не должны противоречить другим положениям Инструкции.

Приложение № 6

к постановлению администрации

Нефтеюганского района

от 01.08.2019 № 1636-па

Инструкция

по учету лиц, допущенных к работе с персональными данными   
в информационных системах персональных данных администрации Нефтеюганского района

Перечень сокращений

|  |  |  |
| --- | --- | --- |
| ИБ |  | - информационная безопасность; |
| ИСПДн |  | - информационная система персональных данных; |
| ПДн |  | - персональные данные; |

1. Общие сведения

* 1. Настоящая инструкция разработана в соответствии с требованиями   
     к защите персональных данных при их обработке в информационных система персональных данных, утвержденных постановлением Правительства Российской Федерации от 01.11.2012 № 1119, пунктом 6 Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденного постановлением Правительства Российской Федерации от 15.09.2008 № 687, и определяет порядок учета лиц, допущенных к работе с персональными данными обработке в информационных система персональных данных   
     в администрации Нефтеюганского района.
  2. Настоящая инструкция определяет порядок допуска учета лиц, допущенных к работе с персональными данными в информационных системах персональных данных, обрабатываемых в информационных системах и без использования средств автоматизации операторами, а так же их уровень прав доступа к обрабатываемым персональным данным в ИСПДн.
  3. Основанием для допуска работников оператора к персональным данным является назначение на должность, указанную в Перечне должностей работников операторов, замещение которых предусматривает осуществление обработки ПДн либо осуществление доступа к ПДн.
  4. Основанием для прекращения допуска работников операторов   
     к персональным данным является прекращение трудовых отношений, изменение должностных обязанностей и исключение из Перечня должностей работников операторов, замещение которых предусматривает осуществление обработки ПДн либо осуществление доступа к ПДн.
  5. К работе допускаются лица, ознакомившиеся с руководящими документами по защите персональных данных.
  6. Учет лиц, допущенных к работе с персональными данными в ИСПДн, ведется в Журнале учета лиц, допущенных к работе с персональными данными   
     в информационных системах персональных данных.

2. Действия по учету лиц, допущенных к работе с персональными данными   
в ИСПДн:

* 1. Руководители операторов предоставляют администратору ИБ ИСПДн список работников, доступ которых к персональным данным, обрабатываемых   
     в информационной системе, необходим для выполнения служебных (трудовых) обязанностей.
  2. Лица, допущенные к обработке ПДн в ИСПДн, должны расписаться   
     в журнале учета лиц, допущенных к работе с персональными данными   
     в информационных системах персональных данных (Приложение 8 к настоящему постановлению).

Приложение № 7

к постановлению администрации

Нефтеюганского района

от 01.08.2019 № 1636-па

Инструкция

по учету машинных носителей информации и регистрации их выдачи

1. Термины и определения

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

Носитель информации – любой материальный объект или среда, используемый для хранения или передачи информации.

Персональные данные (далее также – ПДн) – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу.

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

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

Операторы – администрация Нефтеюганского района, её структурные подразделения с правом юридического лица.

2. Общие положения

2.1. Настоящая Инструкция регламентирует порядок учета, хранения   
и регистрации выдачи машинных носителей информации операторами.

2.1. Под машинными носителями информации в настоящей Инструкции понимаются следующие носители информации:

* оптические диски (CD, DVD) однократной и многократной записи;
* жесткие диски автоматизированных рабочих мест (далее - АРМ);
* USB-flash носители информации и др.

3. Порядок хранения и учета машинных носителей информации

3.1. Машинные носители информации, содержащие персональные данные, подлежат обязательному учету администратором информационной безопасности ИСПДн. Учет осуществляется с помощью «Журнала учета машинных носителей».

3.2. Носители информации, содержащие персональные данные, должны иметь специальную маркировку. Тип маркировки выбирается администратором информационной безопасности ИСПДн.

3.3. Оптические диски и USB-flash носители информации храниться в сейфе, расположенном в помещении оператора, и изыматься только для выполнения служебных (трудовых) обязанностей.

3.4. При поступлении нового машинного носителя информации, который будет использоваться для хранения или передачи персональных данных, администратор информационной безопасности ИСПДн регистрирует его в Журнале учета машинных носителей информации. (Приложение 9 к настоящему постановлению).

3.5. Машинные носители, которые не являются необходимыми для выполнения служебных (трудовых) обязанностей, хранятся в сейфе не более одного года, после чего их необходимо уничтожить без возможности восстановления с последующей регистрацией в Журнале учета машинных носителей информации.

4. Порядок регистрации выдачи машинных носителей

4.1. Учет выдачи машинных носителей ведется в Журнале учета машинных носителей информации, в котором указывается маркировка носителя, дата, время, фамилия, имя и отчество должностного лица, получившего материальный носитель.

4.2. В случае возврата должностным лицом машинного носителя информации   
в Журнале учета машинных носителей информации администратором информационной безопасности ИСПДн проставляется отметка о возврате с указанием даты, времени возврата, личных подписей передающей и принимающей стороны.

5. Порядок уничтожения информации на машинных носителях информации

5.1. Учреждением должно обеспечиваться уничтожение (удаление) информации на машинных носителях информации при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (удаление) информации.

5.2. Уничтожение (удаление) информации на машинных носителях должно исключать возможность восстановления информации конфиденциального характера (защищаемая информация) при передаче машинных носителей между пользователями, в сторонние организации для ремонта или утилизации.

5.3. Уничтожению (удалению) подлежит информация, хранящаяся   
на цифровых и нецифровых, съемных и несъемных машинных носителях информации.

5.4. Перед подключением к информационной системе оператором должно быть обеспечено уничтожение (удаление) информации с носителей информации после их приобретения и при первичном подключении к информационной системе, при использовании в иных информационных системах, при передаче для постоянного использования от одного пользователя другому пользователю, после возвращения из ремонта, а также в иных случаях, предусмотренных оператором.

5.5. Машинные носители информации, не подлежащие очистке   
(не перезаписываемые машинные носители информации, такие как оптические диски типа CD-R) должны быть уничтожены.

5.6. Оператором для уничтожения (удаления) информации на машинных носителях информации, исключающего возможность восстановления информации конфиденциального характера, должна производиться перезапись уничтожаемых (удаляемых) файлов случайной битовой последовательностью в один цикл, удаление записи о файлах, обнуление журнала файловой системы или полная перезапись всего адресного пространства машинного носителя информации случайной битовой последовательностью в один цикл с последующим форматированием.

6. Ответственность

6.1. Персональную ответственность за несоблюдение требований настоящей Инструкции несет администратор информационной безопасности ИСПДн.

За разглашение персональных данных и нарушение порядка обращения   
с машинными носителями информации, содержащими персональные данные, администратор информационной безопасности ИСПДн может быть привлечен   
к гражданской, уголовной, административной, дисциплинарной и иной предусмотренной законодательством Российской Федерации ответственности.

Приложение № 8

к постановлению администрации

Нефтеюганского района

от 01.08.2019 № 1636-па

Типовая форма

журнал

учета лиц, допущенных к работе с персональными данными в информационных системах персональных данных

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № п/п | Должность  и ФИО сотрудника | Сведения о допуске к персональным данным | | | Работник, проводивший инструктаж | Подпись  инструкти-руемого  лица | Сведения о прекращении допуска к персональным данным | | |
| Наименование ИСПДн | Дата утверждения «Списка сотрудников…» | Дата и под­пись допус­каемого лица | Дата утвер­ждения «Списка сотрудников…» или дата распоряжения об увольне­нии | Номер распоряжения об увольне­нии | Дата и подпись лица  об озна­комлении с до­кументом, пре­кращающим до­пуск к ПДн |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|  |  |  |  |  |  |  |  |  |  |

Приложение № 9

к постановлению администрации

Нефтеюганского района

от 01.08.2019 № 1636-па

Типовая форма

журнал

по учету машинных носителей и регистрации их выдачи

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| №  п/п | Регистрационный номер/дата | Тип/ёмкость машинного носителя персональных данных | Ответственное должностное лицо (Ф.И.О.) | Расписка в получении (Ф.И.О.,подпись, дата) | Расписка в обратном приеме (Ф.И.О., подпись, дата) | Место хранения машинного носителя персональных данных | Сведения об уничтожении машинных носителей персональных данных, стирании информации (подпись, дата) |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|  |  |  |  |  |  |  |  |

Приложение № 10

к постановлению администрации

Нефтеюганского района

от 01.08.2019 № 1636-па

Типовая форма

Журнал

по учету применяемых средств защиты информации, эксплуатационной и технической документации к ним

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № п/п | Индекс и наименование средства защиты информации | Серийный (заводской) номер | Номер специального защитного знака | Наименование организации, установившей средство защиты информации | Место установки | Примечание |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|  |  |  |  |  |  |  |

Приложение № 11

к постановлению администрации

Нефтеюганского района

от 01.08.2019 № 1636-па

Типовая форма

Журнал

учета нештатных ситуаций информационных систем персональных данных,   
выполнения профилактических работ, учета установки и модификации программных средств   
на автоматизированных рабочих местах информационных систем персональных данных

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № п/п | Наименование ИСПДн,  расположение и обозначение АРМ | Краткое описание выполненной работы (нештатной ситуации) | Дата и время выполненной работы (нештатной ситуации) | ФИО исполнителей работ и их подписи | Подпись лица, ответственного за защиту информации | Примечание |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|  |  |  |  |  |  |  |

Приложение № 12

к постановлению администрации

Нефтеюганского района

от 01.08.2019 № 1636-па

Типовая форма

Журнал

учета мероприятий по защите персональных данных

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Мероприятие | Дата | Исполнитель | Результат |
| 1 | 2 | 3 | 4 | 5 |
|  |  |  |  |  |