АДМИНИСТРАЦИЯ
МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ
БИЛИБИНСКИЙ МУНИЦИПАЛЬНЫЙ РАЙОН
ЧУКОТСКОГО АВТОНОМНОГО ОКРУГА

Р А С П О Р Я Ж Е Н И Е

от 31 мая 2022 года № 157-рг г. Билибино

Об утверждении Инструкции пользователя по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в Администрации муниципального образования Билибинский муниципальный район

Во исполнение Федерального Закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановления Правительства Российской Федерации от 1 ноября 2012 года. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»,

1. Утвердить Инструкцию пользователя по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в Администрации муниципального образования Билибинский муниципальный район согласно приложению к настоящему распоряжению.
2. Настоящее распоряжение вступает в силу с момента его подписания.
3. Контроль за исполнением настоящего распоряжения возложить на заместителя Главы Администрации - начальника Управления правового и организационного обеспечения Гизбрехта В. В.

Исполняющий обязанности
Главы Администрации С.М. Рубцов

Приложение
к Распоряжению Администрации
муниципального образования
Билибинский муниципальный район
от 31 мая 2022года № 157-рг

ИНСТРУКЦИЯ
пользователя по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в Администрации муниципального образования Билибинский муниципальный район

I Общие положения

1. Пользователем персональных данных (далее – Пользователь) является уполномоченный сотрудник Администрации муниципального образования Билибинский муниципальный район (далее – Оператор), участвующий в рамках своих функциональных обязанностей в процессах обработки персональных данных (далее – ПДн).
2. Пользователь должен знать нормы действующего законодательства Российской Федерации в сфере (области) обработки и обеспечения безопасности персональных данных (далее – ПДн).
3. Пользователь несет персональную ответственность за свои действия.

II Обязанности Пользователя

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. Выполнять указания ответственного за обеспечение безопасности ПДн (далее - Ответственный) и Администратора безопасности информационной системы персональных данных.
3. Соблюдать режим допуска в помещения, где проводится обработка ПДн.
4. Выполнять на автоматизированном рабочем месте только те процедуры, которые определены для него должностными обязанностями и на основании разрешительной системы доступа к ресурсам, программным, и техническим средствам соответствующей информационной системы персональных данных.
5. Знать и строго выполнять правила работы со средствами защиты информации, установленными на элементах информационной системы персональных данных (далее – ИСПДн).
6. Хранить в тайне от других свой пароль.
7. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, жалюзи на оконных проемах должны быть закрыты.
8. Использовать при работе только учтённые машинные носители информации.

9. Обеспечивать безопасное хранение материальных носителей информации, исключающее несанкционированный доступ к ним;

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

11. Немедленно сообщать руководителю структурного подразделения или Ответственному о нештатных ситуациях, фактах и попытках несанкционированного доступа к обрабатываемой информации, о блокировании, исчезновении (искажении) защищаемой информации;

12. Пользователям запрещается:

- разглашать сведения, содержащие ПДн, третьим лицам;
- обрабатывать на автоматизированных рабочих местах информацию и выполнять другие работы, не предусмотренные разрешительной системой доступа к ресурсам, программным, и техническим средствам соответствующей информационной системы персональных данных;
- фиксировать на одном материальном носителе ПДн, цели обработки которых заведомо не совместимы;
- записывать и хранить информацию на незарегистрированных машинных носителях информации;
- подключать к рабочей станции незарегистрированные машинные носители информации;
- самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств, вскрывать и ремонтировать технические средства;
- открывать общий доступ к папкам на своей рабочей станции;
- отключать (блокировать) средства защиты информации;
- сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн;
- привлекать посторонних лиц для производства ремонта или настройки автоматизированных рабочих мест без согласования с Ответственным;
- оставлять посторонних лиц без присмотра в помещениях, где ведется обработка ПДн;
- производить какие-либо изменения в электрических схемах, монтаже и размещении технических средств;
- передавать ПДн по открытым каналам связи.
- оставлять во время работы материальные носители информации без присмотра, несанкционированно передавать материальные носители информации другим лицам и выносить их за пределы помещения, в котором производится обработка информации;
- отключать средства антивирусной защиты;
- работать в ИСПДн при обнаружении каких-либо неисправностей.

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

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].

15. Обеспечивать раздельное хранение ПДн (материальных носителей),

обработка которых осуществляется в различных целях.

16. При покидании помещения, где ведется обработка персональных данных, необходимо запирать данные помещения на ключ и сдавать под охрану в соответствии с «Инструкцией по допуску лиц в помещения Администрации муниципального образования Билибинский муниципальный район, в которых ведётся обработка конфиденциальной информации (в том числе персональных данных)».

III Организация парольной защиты

1. Личные пароли доступа к элементам ИСПДн Пользователи получают у Администратора безопасности информационной системы персональных данных.
2. Полная плановая смена паролей в ИСПДн проводится не реже четырёх раз в год.
3. Во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами.
4. Правила хранение пароля:
- запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах;
- запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.
5. Лица, использующие пароли, обязаны:
- четко знать и строго выполнять требования настоящей Инструкции;
- своевременно сообщать Администратору безопасности информационной системы персональных данных об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.
6. Удаление (в т.ч. внеплановая смена) личного пароля любого Пользователя должна производиться в следующих случаях:
- в случае подозрения дискредитации пароля;
- в случае прекращения полномочий (увольнение, переход на другую работу внутри организации) Пользователя после окончания последнего сеанса работы данного Пользователя с системой;
- по указанию Администратора безопасности информационной системы персональных данных.

IV Организация антивирусной защиты

1. Установка и настройка средств антивирусного контроля осуществляется Администратором безопасности информационной системы персональных данных.
2. Обязательному антивирусному контролю подлежат все файлы, получаемые для обработки в элементах ИСПДн.
3. Вновь получаемые файлы должны пройти антивирусный контроль до начала их обработки в элементах ИСПДн.
4. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и.т.п.) Пользователь обязан немедленно сообщить о своих подозрениях Администратору безопасности информационной системы персональных данных и

затем выполнить внеочередной антивирусный контроль.

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

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

- сообщить Администратору безопасности информационной системы персональных данных;
- провести «лечение» файла;
- в случае обнаружения нового вируса, не поддающегося «лечению» применяемыми антивирусными средствами, исключить из обработки зараженный вирусом файл;
- выполнить проверку всех носителей информации в ИСПДн, которые могли стать носителями вируса;
- попытаться найти источник заражения и по возможности вылечить его от вирусов, в противном случае исключить возможность взаимодействия источника заражения с элементами ИСПДн.

V Порядок реагирования на аварийную ситуацию

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.

- отключение электроэнергии;
- сбой в работе вычислительной сети (коммутационного оборудования);
- ошибка персонала, имеющего доступ в серверное помещение;
- нарушение конфиденциальности, целостности и доступности персональных данных;
- физический разрыв внешних каналов связи.

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

- предпринять попытку сохранения обрабатываемой информации, содержащей ПДн;
- прекратить работу на автоматизированном рабочем месте;
- немедленно оповестить Ответственного, Администратора безопасности информационной системы персональных данных, о возникновении аварийной ситуации.

VI Работа с инцидентами информационной безопасности

1. Ответственность за выявление инцидентов ИБ и реагирование на них в Администрации муниципального образования Билибинский муниципальный район возлагается на Администратора информационной безопасности.

2. Администратор информационной безопасности имеет полномочия инициировать проведение служебных проверок по фактам нарушения установленных

требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации.

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

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

- даты и времени;
- причин (умышленные и неумышленные действия, не антропогенные инциденты и т.п.) и описания инцидента и задействованных лиц;
- информации о последствиях;
- информации о возможных последствиях (экономические убытки (в связи с заменой СЗИ, повторной аттестации; временные и трудозатраты на устранение последствий, нарушение работы пользователей, ущерб субъектам ПДн и юридические последствия для Администрации муниципального образования Билибинский муниципальный район и т.п.).

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

6. В случае возникновения рецидива со стороны пользователя или Администратора информационной безопасности, по ходатайству Ответственного за организацию обработки персональных данных Главой Администрации муниципального образования Билибинский муниципальный район накладывается дисциплинарное взыскание.

7. Сокрытие нарушений и инцидентов ИБ, вызванных любыми должностными лицами Администрации муниципального образования, является грубым нарушением трудовой дисциплины. Сокрытие нарушений и инцидентов ИБ, вызванных действиями Администратора информационной безопасности и Ответственным за организацию обработки персональных данных, является грубейшим нарушением дисциплины, и при выяснении данного факта должно строго наказываться.

8. Любой сотрудник должен согласовывать следующие действия с Администратором информационной безопасности:

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

9. Ответственный за организацию обработки персональных данных не может требовать от Администратора информационной безопасности действий, направленных на нарушение настоящего руководства и других организационно-распорядительных документов Администрации муниципального образования Билибинский муниципальный район, требовать сокрытия инцидентов ИБ, вызванных

любыми должностными лицами, требовать сообщения ему паролей на средства защиты информации и нарушения установленного разграничения прав по допуску к информационным ресурсам, установленным матрицей доступа к информационными ресурсам ИС.

VII. Организация учета, использования, передачи и уничтожения съемных носителей персональных данных и другой конфиденциальной информации

1. Учёту подлежат съемные носители, предназначенные для обработки персональных данных и иной конфиденциальной информации, находящиеся в распоряжении Администрации муниципального образования.

2. Носители учитываются в специальном «Журнале учета машинных носителей персональных данных (съемные носители)» (Приложение №1) в котором производится непосредственно регистрация и учёт носителей.

3. Регистрация и учет носителей информации осуществляется администратором информационной безопасности.

4. Учётный номер носителя состоит из сокращенного наименования структурного подразделения (отдела) и порядкового номера по журналу регистрации через дефис.

5. Учетный номер наносятся непосредственно на носитель (корпус). Если невозможно маркировать непосредственно носитель (корпус), то применяется маркировка упаковки, в которой хранится носитель. Каждому носителю в журнале должна соответствовать отдельная строка.

6. Хранение носителей информации осуществляется в условиях (закрываемые шкафы, сейфы и т.п.), исключающих возможность хищения, приведения в негодность или уничтожения содержащейся на них информации.

7. О фактах утраты носителей необходимо незамедлительно докладывать руководителю своего структурного подразделения.

8. Администратор информационной безопасности не реже одного раза в год осуществляет проверку условий хранения носителей персональных данных и иной конфиденциальной информации.

9. Выдача носителей сотрудникам осуществляется администратором информационной безопасности под подпись с отметкой в «Журнале учета машинных носителей персональных данных (съемные носители)». При сдаче носителя в журнале ставится соответствующаяотметка.

10. Носители, которые выдаются сотруднику, должны пройти проверку на отсутствие записанной на ней информации. В случае наличия какой-либо информации на выдаваемом носителе, администратор информационной безопасности обязан удалить (затереть) информацию.

11. В случае повреждения носителей, содержащих персональные данные и (или) иную конфиденциальную информацию, сотрудник, в пользовании которого они находятся, обязан сообщить о случившемся руководителю своего структурного подразделения (отдела) и администратору информационной безопасности.

12. Уничтожение носителей информации, пришедших в негодность или утративших практическую ценность, производится путем их физического разрушения без возможности дальнейшего восстановления.

13. Перед уничтожением носителя вся информация с него должна быть стерта (уничтожена) путем использования специальных средств (сертифицированные программные или программно-аппаратные средства защиты информации, обеспечивающие невозможность восстановления информации), либо путём полного трехкратного его форматирования, если это позволяют физические принципы работы носителя.

14. Уничтожение носителей, затирания (уничтожение) информации с носителей производиться комиссией из 3 человек, назначенной распоряжением Главы Администрации муниципального образования Билибинский муниципальный район.

15. По факту уничтожения носителей, а также затирания (уничтожения) информации на носителях, комиссией составляется Акт (Приложение №2). В Акте указываются учётные номера носителей, характер уничтожаемой (затираемой) информации, причина уничтожения носителя (затирания информации на нем). Реквизиты Акта заносятся председателем данной комиссии в графу «Сведения об уничтожении» «Журнала учета машинных носителей персональных данных (съемные носители)»

Приложение 1
к Инструкции пользователя по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в Администрации муниципального образования Билибинский муниципальный район

Журнал №__
учета машинных носителей персональных данных (съемные носители)

с «__»_____20__ г.
по «__»_____20__ г.

ФИО и должность ответственного за ведение журнала:_____

Журнал составлен на ____ листах

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

Приложение 2
к Инструкции пользователя по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в Администрации муниципального образования Билибинский муниципальный район

А К Т
о затирании/уничтожении персональных данных и иной конфиденциальной информации/электронных носителей

г. Билибино _____20__ г.

Комиссия в составе:
Председатель:_____ (ФИО)
Члены комиссии: _____ (ФИО)
_____ (ФИО)

составила настоящий Акт о том, что информация, зафиксированная на перечисленных в нем носителях информации, подлежит уничтожению

№ п/п	Учетный номер (при наличии)	Причина уничтожения носителя информации; стирания/ обезличивания информации	Тип носителя информации	Производимая операция (стирание, уничтожение, обезличивание)	Дата	Примечание
1.						
2.						
3.						
4.						
5.						
6.						
7.						

Правильность произведенных записей в акте проверена. Регистрационные данные на носителях информации перед стиранием с них информации с записями в акте сверены, произведено стирание содержащейся на носителях информации. Регистрационные данные на носителях информации (твердой копии) перед их (носителей) уничтожением сверены с записями в акте и полностью уничтожены путем. Отметки о стирании информации (уничтожении носителей информации) в

учетных формах произведены.

Председатель комиссии: _____(ФИО)
подпись

Члены комиссии: _____(ФИО)
подпись

_____(ФИО)