|  |
| --- |
| Приложение 10  к распоряжению Администрации Заринского района  от \_\_\_\_\_\_\_\_\_\_\_\_ №\_\_\_\_\_\_\_\_ |

ПОРЯДОК

организации работы с машинными носителями защищаемой информации в Администрации Заринского района Алтайского края

1. Перечень используемых определений, обозначений и сокращений

АИБ – администратор информационной безопасности.

ИС – информационная система.

ЗИ – защищаемая информация.

НЖМД – накопитель на жёстких магнитных дисках.

СВТ – средства вычислительной техники.

Администратор информационной безопасности – сотрудник Администрации Заринского района Алтайского края, осуществляющий контроль за обеспечением защиты информации в ИС, а также осуществляющий организацию работ по выявлению и предупреждению возможных каналов утечки информации, потенциальных возможностей осуществления НСД к защищаемой информации.

Защищаемая информация – персональные данные сотрудников Администрации Заринского района Алтайского края, граждан РФ, обрабатываемые Администрацией Заринского района Алтайского края, а также иная информация, подлежащая защиты в соответствии с действующим законодательством в сфере защиты персональных данных, информационных систем персональных данных и государственных информационных систем.

1. Общие положения
   1. Настоящий Порядок устанавливает основные требования к организации учета, использования, передачи и уничтожения электронных носителей информации (далее – носители), предназначенных для обработки ЗИ в Администрации Заринского района Алтайского края (далее – Администрация района).
   2. Под электронными носителям информации в данном документе понимаются: гибкие магнитные диски, CD- и DVD-диски, USB флеш-диски, НЖМД и др.
   3. Ответственность за организацию учета, использования, передачи и уничтожения носителей, предназначенных для обработки и хранения ЗИ, затирание (удаление) информации возлагается на администратора информационной безопасности (АИБ).
   4. Положения данного Порядка обязательны для сотрудников Администрации района, которые в ходе выполнения своих должностных обязанностей используют носители ЗИ, а также имеющими допуск к обработке ЗИ.
2. Учёт и хранение электронных носителей информации
   1. Учёту подлежат все носители информации, находящиеся в распоряжении Администрации района и предназначенные для хранения ЗИ.
   2. Носители учитываются в специальном «Журнале регистрации и учета электронных носителей защищаемой информации», в котором производится непосредственно регистрация и учёт носителей.
   3. Регистрация и учет носителей информации осуществляется АИБом.
   4. Учётный номер носителя состоит из сокращенного наименования подразделения (отдела) и порядкового номера по журналу регистрации через дефис (пример: уч. № ОБ-1/ЗИ, где ОБ – отдел бухгалтерии, 1 – порядковый номер в журнале, ЗИ – «Защищаемая информаци»).
   5. В случае отсутствия утвержденных сокращений названий подразделений учетный номер носителя состоит из порядкового номера по журналу регистрации (пример: уч. № 01/ЗИ, где 01 – порядковый номер в журнале, ЗИ – «Защищаемая информация»).
   6. Каждый носитель информации, применяемый при обработке информации на СВТ, должен иметь пометку, соответствующую записанной на нём информации: защищаемая информация – «ЗИ». Исключается хранение на одном носителе информации, имеющей разные цели обработки.
   7. Для съемных носителей информации реквизиты наносятся непосредственно на носитель (корпус). Если невозможно маркировать непосредственно носитель (корпус), то применяется маркировка упаковки, в которой хранится носитель или другие доступные способы маркировки (бирки, брелоки и т.п.). Надпись реквизитов делается разборчиво и аккуратно. На дискеты и футляры носителей допускается наклеивать заранее заготовленную этикетку.
   8. Каждому носителю в журнале должна соответствовать отдельная строка.
   9. НЖМД в серверах и системных блоках компьютеров учитываются в «Журнале регистрации и учета электронных носителей защищаемой информации» с указанием марки носителя информации и его серийного номера.
   10. Хранение носителей информации осуществляется в условиях (закрываемые шкафы, сейфы и т.п.), исключающих возможность хищения, приведения в негодность или уничтожения содержащейся на них информации.
   11. О фактах утраты носителей необходимо незамедлительно докладывать руководителю своего структурного подразделения.
   12. АИБ не реже одного раза в год осуществляет проверку условий хранения носителей ЗИ.
3. Хранение носителей
   1. Не допускается:
      * хранение съемных носителей с ЗИ вместе с носителями открытой информации, на рабочих столах, либо оставление их без присмотра или передача на хранение другим лицам;
      * вынос съемных носителей с ЗИ из служебных помещений для работы с ними на дому, в гостиницах и т. д.
4. Выдача/сдача и передача носителей
   1. Носители, как правило, выдаются только непосредственно на время работы с данным носителем и сдаются специалистом АИБу сразу по завершению таких работ.
   2. Носители, которые выдаются специалисту, должны пройти проверку на отсутствие записанной на ней информации. В случае наличия какой-либо информации на выдаваемом носителе, АИБ обязан удалить (затереть) информацию методом, не позволяющим повторное восстановление защищаемой информации (средствами, осуществляющими безвозвратное удаление информации).
   3. В случае повреждения носителей, содержащих ЗИ, сотрудник, в пользовании которого они находятся, обязан сообщить о случившемся руководителю своего структурного подразделения (отдела) и АИБу.
   4. При передаче в другие организации носители информации должны, по возможности, быть упакованы в пакет/конверт, обеспечивающий сохранность (работоспособность) передаваемого носителя. При этом носители информации передаются с сопроводительным письмом, в котором указывается, какая информация содержится на данном носителе, а для подтверждения достоверности информации прилагается таблица с реквизитами файлов (допускается прикладывать скриншот окна архиватора/проводника). Данное передвижение (передача) носителей ЗИ регистрируется в «Журнале передачи носителей защищаемой информации» где делается отметка об отправке (куда отправлен (реквизиты адресата), исходящий номер сопроводительного письма, дата отправки, способ отправки (курьер, заказная почта и т.п.)) и отметка о получении (номер «Уведомления о вручении» или «Накладной»). В случае если передача носителей осуществляется лично сотрудником Администрации района, то у адресата, необходимо взять расписку о получении носителя.
   5. Для исключения утечки информации, находящейся на жестких дисках компьютеров, при необходимости ремонта компьютера в сервисном центре, жесткий диск с компьютера демонтируется и компьютер отправляется в ремонт без жесткого диска. При необходимости диагностирования самого жесткого диска информация должна быть предварительно скопирована на резервный носитель и затем стёрта с направляемого в ремонт винчестера с использованием специальных средств (сертифицированные программные или программно-аппаратные средства защиты информации, обеспечивающие невозможность восстановления информации). Если невозможно произвести данные действия (поломка жесткого диска или ПЭВМ), то отправка такой ПЭВМ в ремонт возможна только по письменному разрешению главы района.
5. Порядок уничтожения носителей, затирания информации на носителях
   1. Уничтожение носителей информации, пришедших в негодность или утративших практическую ценность, производится путем их физического разрушения без возможности дальнейшего восстановления.
   2. 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), если это позволяют физические принципы работы носителя.
   3. Уничтожение носителей, затирания (уничтожении) информации с носителей производиться комиссией из 3 человек, назначенной распоряжением главы района, в состав комиссии должен входить АИБ (далее- администратор информационной безопасности).
   4. По факту уничтожения носителей, а также затирания (уничтожения) информации на носителях, комиссией составляется Акт. 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 регистрации и учета электронных носителей защищаемой информации». Подписанный Акт должен храниться у АИБа.