|  |  |
| --- | --- |
|  | Приложение 10  к приказу комитета  по культуре города Барнаула  от 29 июля 2021г. №64 |

ПОРЯДОК

организации работы с электронными носителями конфиденциальной информации

Перечень используемых определений, обозначений и сокращений

АИБ – администратор информационной безопасности.

КИ – конфиденциальная информация.

НЖМД – накопитель на жёстких магнитных дисках.

СВТ – средства вычислительной техники.

ПДн – персональные данные.

ИС – информационная система.

ИСПДн – информационная система персональных данных.

Администратор информационной безопасности – специалист или группа специалистов организации, осуществляющих контроль за обеспечением защиты информации в ИС, в том числе ИСПДн, а также осуществляющие организацию работ по выявлению и предупреждению возможных каналов утечки информации, потенциальных возможностей осуществления НСД к защищаемой информации.

1. Общие положения

1.1. Порядок организации работы с электронными носителями конфиденциальной информации (далее – Порядок) устанавливает основные требования к организации учета, использования, передачи и уничтожения электронных носителей информации (далее – носители), предназначенных для обработки КИ, в том числе ПДн (далее – КИ), в комитете по культуре города Барнаула (далее –комитет).

1.2. Под электронными носителям информации в данном документе понимаются: гибкие магнитные диски, CD- и DVD-диски, USB флеш-диски, НЖМД и др.

1.3. Ответственность за организацию учета, использования, передачи и уничтожения носителей, предназначенных для обработки и хранения КИ, затирание (удаление) информации возлагается АИБа.

1.4. Положения Порядка обязательны для выполнения всеми сотрудниками комитета, которые в ходе выполнения своих должностных обязанностей используют носители КИ, а также имеющими допуск к обработке КИ.

2. Учёт и хранение электронных носителей информации

2.1. Учёту подлежат все носители информации, находящиеся в распоряжении комитета и предназначенные для хранения КИ.

2.2. Носители учитываются в специальном «Журнале регистрации и учета электронных носителей конфиденциальной информации» в котором производится непосредственно регистрация и учёт носителей.

2.3. Регистрация и учет носителей информации осуществляется АИБом.

2.4. Учётный номер носителя состоит из сокращенного наименования подразделения (отдела) и порядкового номера по журналу регистрации через дефис (пример: уч. № ОБ-1/К, где ОБ – отдел бухгалтерии, 1 – порядковый номер в журнале, К – «Конфиденциально»).

2.5. В случае отсутствия утвержденных сокращений названий подразделений учетный номер носителя состоит из порядкового номера по журналу регистрации (пример: уч. № 01/К, где 01 – порядковый номер в журнале, К – «Конфиденциально»).

2.6. Каждый носитель информации, применяемый при обработке информации на СВТ, должен иметь гриф конфиденциальности, соответствующий записанной на нём информации: конфиденциальной информации - «К». Исключается хранение на одном носителе информации разных грифов конфиденциальности, а также хранение информации, имеющей разные цели обработки.

2.7. 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.

2.8. Каждому носителю в журнале должна соответствовать отдельная строка.

2.9. НЖМД в серверах и системных блоках компьютеров учитываются в паспорте (формуляре) на поставляемое оборудование с указанием марки носителя информации и его серийного номера.

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

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

2.12. АИБ не реже одного раза в год осуществляет проверку условий хранения носителей КИ.

3. Хранение носителей

3.1. Не допускается:

хранение съемных носителей с КИ вместе с носителями открытой информации, на рабочих столах, либо оставление их без присмотра или передача на хранение другим лицам;

вынос съемных носителей с КИ из служебных помещений для работы с ними на дому, в гостиницах и т. д.

4. Выдача/сдача и передача носителей

4.1.Носители, как правило, выдаются только непосредственно на время работы с данным носителем и сдаются сотрудником АИБу сразу по завершению таких работ.

4.2.Носители, которые выдаются сотруднику, должны пройти проверку на отсутствие записанной на ней информации. В случаи наличия какой-либо информации на выдаваемом носителе, АИБ обязан удалить (затереть) информацию согласно п. 4. настоящего Порядка.

4.3. В случае повреждения носителей, содержащих КИ, сотрудник, в пользовании которого они находятся, обязан сообщить о случившемся руководителю своего структурного подразделения (отдела) и АИБу.

4.4. 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. Данное передвижение (передача) носителей КИ регистрируется в «Журнале передачи носителей конфиденциальной 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 комитета, то у адресата, необходимо взять расписку о получении носителя.

4.5. 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), либо путём полного трехкратного его форматирования. Если невозможно произвести данные действия (поломка жесткого диска или ПЭВМ), то отправка такой ПЭВМ в ремонт возможна только по письменному разрешению председателя комитета.

5. Порядок уничтожения носителей, затирания

информации на носителях

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

5.2. 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), либо путём полного трехкратного его форматирования, если это позволяют физические принципы работы носителя.

5.3. Уничтожение носителей, затирания (уничтожении) информации с носителей производиться комиссией из 3 человек, назначенной Решением Председателя комитета по культуре города Барнаула в состав комиссии должен входить АИБ.

5.4. 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 конфиденциальной информации». Подписанный Акт должен храниться у АИБа.