Государственное бюджетное
дошкольное образовательное учреждение детский сад № 43
компенсирующего вида Приморского района Санкт-Петербурга

СОГЛАСОВАНО:
Профсоюзный комитет
ГБДОУ детский сад № 43
Протокол №28
от «23» июня 2022 г.
Председатель ПК
_____ О.А. Егорова

УТВЕРЖДАЮ:
Заведующий ГБДОУ
детского сада № 43
_____ Ж.Н. Курочкина
Приказ от 23.06.2022
№ 19-д

ИНСТРУКЦИЯ № 2-ИБ-22
о порядке учета, хранения и уничтожения носителей информации ограниченного доступа в Государственном бюджетном дошкольном образовательном учреждении детский сад № 43 компенсирующего вида Приморского района Санкт-Петербурга

Санкт-Петербург
2022

1. Общие положения

1.1.Настоящая Инструкция разработана для Государственного бюджетного дошкольного образовательного учреждения детский сал № 43 компенсирующего вида Приморского района Санкт-Петербурга (далее – ГБДОУ) в целях определения порядка учета, хранения и уничтожения носителей
информации ограниченного доступа с целью обеспечения информационной безопасности.
1.2. Выделяют сведения о субъектах, сохраняемые в бумажном и электронном виде.

2.Учет и контроль

2.1. Действия, связанные с эксплуатацией средствами криптографической защиты информации (СКЗИ), должны фиксироваться в «Журнале пользователя сети», который ведет лицо, ответственное за обеспечение информационной безопасности на АРМ. 2.2. 2.2.В журнал также заносятся факты компрометации ключевых документов, нештатные ситуации, происходящие в системе и связанные с использованием СКЗИ, проведение регламентных работ, данные о полученных у администратора безопасности организации ключевых носителях, нештатных ситуациях, произошедших на АРМ, с установленным ПО СКЗИ.
2.3.Пользователь (либо администратор безопасности) должен периодически (не реже одного раза в два месяца) проводить контроль целостности и легальности установленных копий ПО на всех АРМ со встроенной СКЗИ, а также проводить периодическое тестирование технических и программных средств защиты.
2.4.В случае обнаружения «посторонних» (не зарегистрированных) программ, нарушения целостности программного обеспечения либо выявления факта повреждения печатей на системных блоках работа на АРМ должна быть прекращена. По данному факту должно быть проведено служебное расследование комиссией, назначенной заведующим ГБДОУ, и организованы работы по анализу и ликвидации негативных последствий данного нарушения.

3.Электронное хранение

3.1.Электронное хранение предполагает создание защищенных ИСПДн, которые в автоматическом режиме фиксируют и обрабатывают большие массивы данных. Такое хранение не требует закрывающихся шкафов и сейфов, и не имеет риска риска кражи или утечки информации.
3.2.Электронное хранение требует оснащения современным программным обеспечением, потребность в постоянном создании резервных копий, а также регулярного обновления оборудования.
3.3.Федеральная служба по техническому и экспертному контролю определяет три вида таких носителей, которые требуют регистрации в журналах установленного образца:

- жесткие диски в стационарных компьютерах, серверах, моноблоках и т. д.;
- носители информации в различных портативных устройствах (ноутбуки, нетбуки, планшеты, фотоаппараты и т. д.);
- съемные машинные носители (флешки, съемные HDD, карты памяти).

4.Правила хранения информации на бумажных носителях

4.1.Бумажные носители предполагают размещение в сейфах в алфавитном порядке в зависимости от регистрационного номера. Информация размещается согласно внутреннему регламенту, работодатель может сам выбрать место для папок-накопителей, определить ответственных за безопасность сотрудников и установить ограничение доступа.
4.2. Правила хранения информации на бумажных носителях требуют наличие сейфов, потребность в свободном и защищенном пространстве.
4.3.Рекомендации к устройству хранилищ информации на бумажных носителях регламентируются Правилами из приказа Минкультуры от 31.03.2015 № 526.
4.4.Приказом заведующего ГБДОУ определяется режим доступа в помещения, где хранятся носители информации.
4.5.Приказом заведующего ГБДОУ устанавливается перечень лиц, которые имеют право доступа к месту хранения носители информации.

5.Правила хранения информации на электронных носителях

5.1.Защита документов в электронной базе данных требует чтобы к базе доступ получили только сотрудники с правом обрабатывать информацию на электронных носителях

5.2.Приказом заведующего ГБДОУ назначаются сотрудники с правом обрабатывать информацию и для каждого сотрудника создается индивидуальный логин и пароль.

5.3.Систематически создается резервная копия электронной базы, которую необходимо хранить на внешнем жестком диске.

6.Уничтожение носителей информации

6.1.Уничтожение бумажных носителей информации:

- Небольшой объем бумаг может быть уничтожен с помощью измельчителя (шредера) При уничтожении своими силами составляется акт в свободной форме;
- Крупные партии документов нужно доставить для уничтожения в специальные компании. К акту прилагается квитанция, выданная компанией-уничтожителем, о том, что документы приняты на утилизацию.

6.2.Уничтожение электронных носителей информации:

- документ, подлежащий уничтожению, необходимо уничтожить вместе с носителем (диском, флэш-картой).
- в том случае, если документ записан на жестком диске компьютера, простое нажатие кнопки «delete» и перемещение файла в корзину не гарантирует его уничтожения.
- уничтожать электронные файлы можно двумя способами: долгой перезаписью или утилизацией винчестера (допустимо электромагнитное излучение, химическое воздействие, физическое разрушение).