Приложение № 1
к приказу №133 от 28.11 23г

ИНСТРУКЦИЯ

об организации и обеспечении безопасности эксплуатации программно-аппаратных комплексов, машинных носителей информации в целях обеспечения безопасности при обработке персональных данных в МКДОУ детский сад № 22

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Информационная безопасность - защита конфиденциальности, целостности и доступности информации.

Конфиденциальность - обеспечение доступа к информации только авторизованным пользователям.

Целостность - обеспечение достоверности и полноты информации и методов ее обработки.

Доступность - обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости. Безопасность информации - состояние защищенности информации, характеризуемое способностью работников, технических средств и информационных технологий обеспечивать конфиденциальность, т.е. сохранение в тайне от субъектов, не имеющих полномочий на ознакомление с ней, целостность и доступность информации при ее обработке техническими средствами.

Доступ к информации (доступ) - ознакомление с информацией, ее обработка, в частности копирование, модификация или уничтожение информации.

Автоматизированная система (АС) - система, состоящая из работников и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций Защита информации от несанкционированного доступа (защита от НСД) или воздействия - деятельность, направленная на предотвращение или существенное затруднение несанкционированного доступа к информации (или воздействия на информацию).

Конфиденциальная информация - информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Несанкционированный доступ (НСД) - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств.

Доступность информации - состояние информации, характеризуемое способностью АС обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия.

2.ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПРИ РАБОТЕ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

2.1. К работе в АС МКДОУ детский сад № 22 допускаются только пользователи (сотрудники) МКДОУ детский сад № 22 (далее Учреждение).

2.2. Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам АС. Полномочия пользователей определяются в соответствии с его должностными инструкциями. При этом для хранения информации, содержащей конфиденциальные сведения, разрешается использовать только машинные носители информации, учтенные в Журнале учета, хранения и уничтожения машинных носителей.

2.3. Пользователь несет ответственность за правильность включения и выключения средств вычислительной техники (СВТ), входа в систему и все действия при работе в АС.

2.4. Вход пользователем в систему осуществляется по выдаваемому ему персональному паролю.

2.5. При работе со съемными машинными носителями информации пользователь каждый раз перед началом работы обязан проверить их на отсутствие вирусов с использованием штатных антивирусных программ, установленных на компьютерах АС. В случае обнаружения вирусов пользователь обязан незамедлительно прекратить их использование и действовать в соответствие с правилами при обнаружении вирусов (пункт 4).

2.6. Каждый пользователь, участвующий в рамках своих функциональных обязанностей в процессах обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным АС, несет персональную ответственность за свои действия и обязан:

- строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами АС;
- знать и строго выполнять правила работы со средствами защиты информации, установленными на компьютерах АС;
-незамедлительно извещать заведующего при подозрении компрометации личного пароля, а также при обнаружении:
- нарушения целостности пломб на соответствующих узлах и блоках СВТ или иных фактов совершения в его отсутствие попыток несанкционированного доступа (НСД) к данным защищаемым СВТ;
- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию СВТ, выхода из строя или неустойчивого функционирования узлов СВТ или периферийных устройств (сканера, принтера и т.п.), а также перебоев в системе электроснабжения;
- некорректного функционирования установленных на компьютеры технических средств защиты;
- непредусмотренных отводов кабелей и подключенных устройств.

2.7. Пользователю категорически запрещается:
- использовать компоненты программного и аппаратного обеспечения ПЭВМ в неслужебных целях;
- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств АС или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения;
- осуществлять обработку конфиденциальных данных в присутствии посторонних (не допущенных к данной информации) лиц;
- записывать и хранить конфиденциальную информацию (содержащую сведения ограниченного распространения) на неучтенных машинных носителях информации (гибких магнитных дисках и т.п.);
- оставлять включенным без присмотра компьютер, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);
- оставлять без личного присмотра на рабочем месте или где бы то ни было свое персональное устройство идентификации, машинные носители и бумажные документы, содержащие защищаемую информацию (сведения ограниченного распространения);
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации;
- размещать средства АС так, чтобы с них отсутствовала возможность визуального считывания информации;
- проносить на территорию управления образованием регистрирующую аппаратуру, множительную и вычислительную технику личного пользования;
- оставлять без контроля вычислительные средства, на которых эксплуатируются СКЗИ, после ввода ключевой информации либо иной конфиденциальной информации;
- вносить какие либо изменения в программное обеспечение СКЗИ;
- осуществлять несанкционированное копирование ключевых носителей;
- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и т.п.иные средства отображения информации;
- использовать ключевые носители в режимах не предусмотренных функционированием СКЗИ;
- записывать на ключевые носители постороннюю информацию;
- осуществлять несанкционированное вскрытие системных блоков ПЭВМ;
2.8. Заведующий Учреждения имеет право:
- требовать от сотрудников соблюдения установленной технологии обработки информации и выполнения инструкций по обеспечению безопасности и защите информации в АС;
- инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, модификации, порчи защищаемой информации и технических компонентов АС;

- требовать прекращения обработки информации в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации;
- участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа.

3. ТРЕБОВАНИЯ К ЗАЩИТЕ ИНФОРМАЦИИ ХРАНЯЩЕЙСЯ НА ПЕРСОНАЛЬНЫХ КОМПЬЮТЕРАХ

3.1. Персональные компьютеры (ноутбуки) пользователей должны быть физически защищены от вскрытия.

3.2. Физическая защита должна включать в себя мероприятия, предотвращающие вскрытие персональных компьютеров с целью получения доступа к носителям информации, находящимся в корпусе системного блока, а также для изменения конфигурации компьютера и любых его настроек.

3.3. В целях организации физической защиты системных блоков рабочих станций, применяется метод опечатывания.

3.4. Правила опечатывания системных блоков рабочих станций пользователей:

- Системный блок подлежит опечатыванию. Данная процедура служит защитой от несанкционированного вскрытия персонального компьютера с целью изменения конфигурации компьютера;
- Обязательному опечатыванию пломбами подлежат все системные блоки рабочих станций, находящиеся на балансе управления образованием, вновь приобретаемые, передаваемые на баланс из других организаций или вскрытые для проведения ремонта;
- Пломбирование системных блоков рабочих станций выполняется с помощью пломб, при снятии которых происходит разрыв пломбы;
- Снятие установленной пломбы с системного блока осуществляется только уполномоченными Заведующим Учреждения сотрудником сотрудниками, назначенных в случае:
- настройке параметров рабочих станций;
- проведения ремонтных или профилактических работ системного блока;
- установки новых устройств в системный блок;
- составления, списания устаревших, неисправных системных блоков;
- необходимости отключения периферийных устройств на рабочих станциях.

3.5 Регистрация информации о первичном пломбировании производиться в Журнале учета пломбирования рабочих станций, системных блоков (Приложение №1). При пломбировании фиксируется местоположение системного блока, его конфигурация, серийный номер, инвентарный номер, номер пломбы. Нарушать пломбу имеют право только назначенные начальником управления образования сотрудники, с обязательной отметкой даты и причины вскрытия системного блока в Журнале учета пломбирования.

3.6. Пользователь обязан регулярно проверять целостность пломбы. При обнаружении нарушения пломбы Пользователь должен немедленно сообщить об этом заведующему Учреждением. По факту несанкционированного вскрытия системного назначается служебное расследование. Служебное

расследование проводится комиссией назначаемой заведующим Учреждения. Председателем комиссии является заведующий Учреждения.

3.7. По результатам служебного расследования готовятся предложения по разрешению возникшей ситуации. Решение о принятии мер дисциплинарного характера к виновным остается за заведующим Учреждения.

3.8. На персональных компьютерах на которых предусмотрено использование СКЗИ необходимо применять следующие меры безопасности: - необходимо предусмотреть меры, максимально ограничивающие доступ к следующим ресурсам системы:

-системный реестр;

-файлы и каталоги;

- временные файлы;

- журналы системы;

- файлы подкачки;

- кэшируемая информация (пароли и т.п.);

- отладочная информация.

- организовать стирание (по окончании сеанса работы СКЗИ) временных файлов и файлов подкачки, формируемых или модифицируемых в процессе работы СКЗИ. Если это не выполнимо, то на жесткий диск должны распространяться требования, предъявляемые к ключевым носителям, должно быть исключено попадание в систему программ, позволяющих, пользуясь ошибками ОС, повышать предоставленные привилегии;

- в случае подключения ПЭВМ с установленными СКЗИ к общедоступным сетям передачи данных, необходимо исключить возможность открытия и исполнения файлов и скриптовых объектов, полученных из общедоступных сетей передачи данных, без проведения соответствующих проверок на предмет содержания в них программных закладок и вирусов, загружаемых из сети. При использовании СКЗИ на ПЭВМ, подключенных к общедоступным сетям связи, с целью исключения возможности несанкционированного доступа к системным ресурсам используемых операционных систем, к программному обеспечению, в окружении которого функционирует СКЗИ, и к компонентам СКЗИ со стороны указанных сетей, должны использоваться дополнительные методы и средства защиты (например установка межсетевого экрана и т.п.).

5. ПРАВИЛА АНТИВИРУСНОЙ ЗАЩИТЫ

5.1. К использованию на компьютерах допускаются только лицензионные антивирусные средства.

5.2. Необходимо осуществлять периодическое обновление антивирусных пакетов и контроль их работоспособности.

5.3. Ярлык для запуска антивирусной программы должен быть доступен всем пользователям информационной системы.

5.4. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, лентах, CD-ROM и т.п.).

5.5. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. На компьютеры запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

5.6. 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 сообщает о ситуации руководителю учреждения, приостанавливает обработку данных в АС.

6. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

6.1. Сотрудники Учреждения должны быть ознакомлены под расписку с перечисленными выше требованиями и предупреждены об ответственности за не соблюдение данных требований, а также за разглашение обрабатываемой информации.

6.2. Пользователи за несоблюдение или нарушение парольной защиты несут ответственность в соответствии с действующим законодательством Российской Федерации.