УТВЕРЖДАЮ
Заведующий МБДОУ ДС № 67 «Умка»
_____О.В.Щеголева
14 декабря 2020 года

ИНСТРУКЦИЯ

пользователя информационных систем муниципального бюджетного дошкольного образовательного учреждения детского сада № 67 «Умка»

1 ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая Инструкция пользователя (далее – Инструкция) устанавливает требования к организации обработки сведений ограниченного доступа (в том числе персональных данных) в информационных системах муниципального бюджетного дошкольного образовательного учреждения детского сада № 67 «Умка» (далее – Учреждение), позволяющие обеспечить безопасность обрабатываемых данных. Инструкция содержит правила работы в ИС и описывает права и обязанности пользователей информационных систем.

Пользователь ИС в своей работе обязан руководствоваться настоящей Инструкцией и утвержденными документами Учреждения, регламентирующими порядок обеспечения безопасности защищаемой информации.

К работе в ИС допускается сотрудник только после ознакомления с положениями настоящей Инструкции. Факт ознакомления регистрируется в Журнале учета доступа к работе в информационных системах Учреждения.

Методическое руководство работой пользователя информационной системы осуществляется лицами, ответственными за защиту информации: ответственным за организацию обработки персональных данных, ответственным за эксплуатацию информационной системы, администратором безопасности, ответственным за учет и хранение средств криптографической защиты информации.

2 ПРАВИЛА РАБОТЫ В ИНФОРМАЦИОННОЙ СИСТЕМЕ

2.1 Доступ к работе в информационной системе

При первичном допуске к работе на ПЭВМ, входящих в состав ИС, пользователь обязан ознакомиться с базой нормативно-методических документов, подготавливаемой ответственным за организацию обработки персональных данных, а также с разработанными организационно-распорядительными и техническими документами, применяемыми для защиты информации в Учреждении. Факт ознакомления регистрируется в Журнале учета доступа к работе в информационных системах Учреждения.

Для начала работы на ПЭВМ пользователь должен пройти первичный инструктаж по работе с установленными средствами защиты, получить личный идентификатор у администратора безопасности. В качестве идентификатора используется пара логин-пароль и/или электронный ключ.

Пользователь несет персональную ответственность за компрометацию своего личного идентификатора.

Безопасный доступ пользователя к ресурсам информационной системы реализуется сертифицированными средствами защиты от несанкционированного доступа, установленными на ПЭВМ (согласно Техническому паспорту объекта информатизации). В целях защиты от несанкционированного доступа к ресурсам ПЭВМ в СЗИ от НСД установлено ограничение на число неуспешных попыток входа в систему (пять попыток входа), а также блокирование сеанса работы после установленного времени бездействия (30 минут).

Пользователю запрещены любые действия на ПЭВМ до прохождения им процедур идентификации и аутентификации (кроме действий, необходимых для прохождения идентификации и аутентификации).

Запрещается:

- осуществлять вход в систему под чужой учетной записью;
- сообщать посторонним лицам свой логин и пароль;
- оставлять без присмотра электронный ключ;
- передавать посторонним лицам электронный ключ;
- приступать к работе на ПЭВМ, не пройдя инструктаж у администратора безопасности и ответственного за эксплуатацию информационной системы.

2.2 Общие требования к организации обработки защищаемой информации

Пользователь информационной системы в отведенное ему время решает поставленные задачи в соответствии с правами доступа к ресурсам ПЭВМ, присвоенными ему администратором безопасности.

Допуск пользователей в помещения информационной системы осуществляется согласно утвержденному Журналу учета доступа к работе в информационных системах Учреждения. Контроль за ведением журнала возлагается на администратора безопасности.

Уборка помещений, в которых размещены технические средства ИС, должна проводиться под наблюдением сотрудника, имеющего право доступа к работе в информационной системе.

Организация обработки защищаемой информации в помещениях, в которых располагается ИС, а также расположение средств отображения информации во время работы должны исключать случайное ознакомление с защищаемой информацией посторонними лицами.

В процессе обработки защищаемой информации пользователь должен использовать только штатные программные и технические средства, указанные в Техническом паспорте объекта информатизации.

Пользователь обязан осуществлять визуальный контроль целостности ОТСС и элементов контроля несанкционированного доступа (наклеек, пломб, защитных знаков).

Вывод на печать документов, содержащих обрабатываемую защищаемую информацию, возможен только на устройства печати, входящие в состав ОТСС ИС и находящиеся внутри помещений, в которых производится обработка таких данных. Распечатанные листы должны извлекаться из лотка устройств печати пользователем сразу после завершения процесса печати.

В случае оставления пользователем ПЭВМ из состава ИС в течение рабочего дня должно производиться блокирование компьютера сочетанием клавиш «Windows» + «L» либо с помощью меню «Пуск».

Запрещается:

- разглашать лицам, не допущенным к работе в ИС, сведения ограниченного доступа, в том числе сведения об установленных средствах защиты информации и принятых мерах защиты;
- покидать помещения информационной системы, не осуществив блокировку доступа к ПЭВМ или не выключив ПЭВМ;
- привлекать посторонних лиц для проведения ремонтных работ технических средств ИС без согласования с лицами, ответственными за защиту информации;
- самостоятельно проводить вскрытие или ремонт ОТСС, их блоков, частей, узлов;
- выполнять работы с документами, содержащими защищаемую информацию, на дому.

2.3 Учет и хранение защищаемой информации

При обработке защищаемой информации обеспечивается раздельное хранение баз данных, содержащих защищаемую информацию, обработка которых осуществляется в целях, несовместных между собой.

При этом для хранения файлов, содержащих защищаемую информацию, разрешается использовать только специально выделенные каталоги жестких магнитных дисков (расположение каталогов определяет администратор безопасности), а также съемные машинные носители информации, учтенные в установленном порядке.

Хранение защищаемой информации осуществляется не дольше, чем этого требуют цели обработки защищаемой информации. Обрабатываемая защищаемая информация подлежит уничтожению, либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей.

Документы, содержащие защищаемые данные и используемые в процессе обработки таких данных, должны убираться пользователем в запираемые (пломбируемые) шкафы или сейфы. Запрещается оставлять без присмотра документы, содержащие обрабатываемые сведения ограниченного доступа.

Все находящиеся на хранении и в обращении съемные машинные носители защищаемой информации подлежат учету. Все съемные машинные носители защищаемой информации должны быть промаркированы наклейкой с уникальным учетным номером. Уникальный учетный номер наносится специальным нестираемым маркером на материальные носители защищаемой информации, на которые наклеивание ярлыка недопустимо по техническим причинам (CD-диск и т.п.)

О фактах утраты машинных носителей защищаемой информации, а также документов, содержащих сведения ограниченного доступа, либо разглашения этой информации ставится в известность руководитель Учреждения и назначается комиссия для расследования обстоятельств утраты или разглашения. Результаты расследования докладываются руководителю Учреждения с последующим составлением акта о проведении служебного расследования.

2.4 Уничтожение защищаемой информации

Внешние машинные носители защищаемой информации, пришедшие в негодность или отслужившие установленный срок, подлежат уничтожению. Уничтожение машинных носителей

защищаемой информации осуществляется комиссией, утвержденной руководителем Учреждения. В результате уничтожения носителя составляется акт уничтожения внешних машинных носителей защищаемой информации.

Бумажные носители, содержащие защищаемые данные, непредназначенные для дальнейшего использования в процессе обработки информации, подлежат уничтожению путем их размельчения вручную либо с помощью специального оборудования для уничтожения бумажных носителей. Уничтожение бумажных носителей защищаемой информации осуществляется комиссией, утвержденной руководителем Учреждения. В результате уничтожения бумажных документов составляется акт о выделении к уничтожению документов, не подлежащих хранению.

В случае прекращения обработки защищаемой информации должны быть уничтожены все резервные копии такой информации.

В случае увольнения или оставления занимаемой должности пользователь обязан вернуть все выданные ему учтенные машинные носители информации, а также документы и материалы, относящиеся к обработке защищаемой информации.

Запрещается:

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

– вынос носителей защищаемой информации (в том числе бумажных) из служебных

помещений для работы с ними на дому и т.д.

2.5 Работа с машинными носителями информации

Для разработки и хранения документов, содержащих защищаемые данные, могут применяться машинные носители информации.

Все зарегистрированные машинные носители информации, предназначенные для хранения информации ограниченного доступа, пользователь получает у администратора безопасности и ставит отметку о получении носителя в журнале учета защищаемых машинных носителей.

Операции с машинными носителями информации проводятся только на ПЭВМ, входящих в состав ИС.

МНИ, содержащие защищаемую информацию, должны храниться в запираемых (пломбируемых) шкафах или сейфах, расположенных в местах, исключающих случайный доступ к ним посторонних лиц.

При подключении съемных МНИ к ПЭВМ, входящих в состав ИС, пользователем производится обязательная антивирусная проверка носителя.

Машинные носители защищаемой информации, непригодные для дальнейшего использования, подлежат передаче администратору безопасности для их уничтожения.

Запрещается:

– хранить на учтенных МНИ информацию, не относящуюся к защищаемой, а также использовать учтенные МНИ в личных целях;

– использовать неучтенные МНИ для обработки и хранения защищаемых данных;

– оставлять без присмотра учтенные МНИ, передавать их посторонним лицам;

– передавать выданные под роспись машинные носители информации другим сотрудникам для пользования.

2.6 Обеспечение неизменности технологического процесса, программных и технических средств информационной системы

Обеспечение неизменности программной среды и состава установленного оборудования, а также неизменности и целостности системы защиты информации в ИС является одним из основных требований при работе.

В случае необходимости внесения изменений в конфигурацию информационной системы и систему защиты информации (в целях замены оборудования, изменения перечня программного обеспечения) пользователь обязан сообщить об этом администратору безопасности.

Запрещается:

– самостоятельно устанавливать, модифицировать, обновлять программное обеспечение, в том числе ПО средств защиты информации, а также изменять установленный алгоритм работы ПО;

– осуществлять любые действия с BIOS/UEFI, в том числе осуществлять «откат» версии;

– нарушать целостность пломб на корпусах ПЭВМ, входящих в состав информационной системы;

– оставлять без присмотра учтенные машинные носители информации, а также другие материалы, содержащие защищаемые данные (журналы, распечатки и т.д.);

– пытаться отключать или блокировать работу средств защиты информации.

2.7 Организация парольной защиты

Для усиления функций идентификации пользователей при доступе к ресурсам ПЭВМ, входящих в состав ИС, установлены следующие требования:

– пароль не должен содержать имя учетной записи пользователя или его фрагменты пользователя длиной больше двух символов;

– пароль должен состоять из восьми символов;

– пароль должен содержать символы, относящиеся к трем из следующих четырех категорий: латинские заглавные буквы (A - Z), латинские строчные буквы (a - z), цифры (0 - 9), отличные от букв и цифр символы (например !, $, #, %);

– пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, дни рождения и другие памятные даты, номера телефонов, автомобилей, адреса места жительства, клички домашних животных, наименования ПЭВМ, общепринятые сокращения (ЭВМ, ЛВС, USER, SYSOP, GUEST, ADMINISTRATOR и т.д.)), а также другие данные, которые могут быть подобраны нарушителем путем анализа информации о пользователе;

– не использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;

– не использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);

– при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;

– запрещается хранение паролей на съемных машинных носителях информации.

Пользователь обязан менять пароль не реже одного раза в год, а также внепланово по требованию администратора безопасности.

На ПЭВМ, входящих в состав информационной системы, запрещается использование учетных записей «по умолчанию».

В целях защиты от несанкционированного доступа к ресурсам ПЭВМ установлено ограничение на число неуспешных попыток ввода пароля для входа в систему (пять попыток входа).

Пользователь несет ответственность за использование паролей, не соответствующих вышеперечисленным требованиям, а также за их разглашение.

Запрещается:

– сообщать посторонним лицам пароль для доступа к ПЭВМ, входящим в состав информационной системы;

– осуществлять ввод пароля для доступа в систему в присутствии посторонних лиц;

– записывать пароли в общедоступных местах (монитор, обратная сторона клавиатуры, отдельные листы бумаги, файлы ПЭВМ и т.д.);

– использовать повторно ранее использованные пароли.

2.8 Организация работы в сети Интернет

Работа в сетях общего доступа и/или международного информационного обмена (международная компьютерная сеть Интернет и другие сети, далее – Сеть) на ПЭВМ, входящих в состав информационной системы, должна проводиться при служебной необходимости.

Пользователям запрещена самостоятельная организация дополнительных точек доступа в Сеть (USB-модем и т.д.), не предусмотренная конфигурацией информационной системы.

Запрещается:

– осуществлять работу в Сети при отключенных средствах защиты информации (антивирусные средства, межсетевые экраны и пр.);

– передавать по Сети защищаемую информацию без использования средств шифрования;

– скачивать и запускать с сетевых ресурсов исполняемые файлы, плагины браузера без согласования с администратором безопасности;

– посещать «сомнительные» сайты, использующие незащищенное соединение и способные нанести вред системе.

2.9 Организация антивирусной защиты

При возникновении любых подозрений на наличие вредоносного программного обеспечения (нетипичная работа программ, появление графических и звуковых эффектов, искажение данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь обязан немедленно прекратить какие-либо действия на ПЭВМ и сообщить администратору безопасности о выявленной проблеме.

В случае отсутствия штатных функций антивирусного программного обеспечения, предусматривающих автоматическую проверку файлов, пользователь обязан осуществлять проверку всех файлов, получаемых:

- по электронной почте;
- по сети Интернет;
- на оптическом (магнитном) диске;
- на флеш-накопителе;
- на ином съемном носителе информации.

В случае обнаружения на съемном носителе информации вредоносного программного обеспечения, не поддающегося лечению, пользователь обязан прекратить их использование.

Запрещается:

- осуществлять действия, направленные на отключение антивирусного программного обеспечения;
- самостоятельно устанавливать программное обеспечение;
- запускать файлы, полученные по сети Интернет, по электронной почте или на съемных носителях информации, без предварительной их проверки антивирусной программой, даже если они получены от доверенного адресата.

3 ПОРЯДОК ДЕЙСТВИЙ В СЛУЧАЕ ВОЗНИКНОВЕНИЯ НЕШТАТНЫХ СИТУАЦИЙ

В случае превышения максимального количества попыток входа в систему пользователь обязан:

- не завершать работу ПЭВМ, не пытаться решить проблему самостоятельно;
- сообщить об инциденте администратору безопасности.

В случае обнаружения фактов непреднамеренной модификации/удаления защищаемой информации пользователь обязан:

- приостановить обработку защищаемой информации на ПЭВМ;
- поставить в известность лиц, ответственных за защиту информации;
- совместно с администратором безопасности произвести восстановление модифицированной/удаленной информации из последней резервной копии, согласно утвержденному Регламенту резервного копирования объекта информатизации.

В случае возникновения проблем с «лечением»/удалением зараженных файлов, а также при возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, исчезновение файлов, частое появление сообщений о системных ошибках и т.п.) пользователь обязан:

- немедленно сообщить о возникшей ситуации администратору безопасности;
- совместно с администратором безопасности провести мероприятия по устранению возникшей проблемы и выполнить внеочередной антивирусный мониторинг.

В случае возникновения отказа в работе технических средств ПЭВМ («мышь», клавиатура, монитор, принтер и т.д.) необходимо:

- не производить самостоятельную замену технических средств;
- поставить в известность администратора безопасности.

Действия в случае обнаружения нарушения целостности элементов контроля несанкционированного доступа к ПЭВМ (наклеек, пломб, защитных знаков):

- приостановить или не начинать обработку защищаемой информации на ПЭВМ;
- поставить в известность лиц, ответственных за защиту информации.

В случае возникновения сбоя или возникновения ошибок в работе установленных на ПЭВМ средств защиты информации или программного обеспечения, предназначенного для обработки защищаемой информации, следует:

- приостановить обработку защищаемой информации на ПЭВМ;
- поставить в известность администратора безопасности.

В случае выхода из строя учтенного машинного носителя информации пользователь обязан передать машинный носитель информации администратору безопасности.

В случае необходимости изменения состава установленного программного обеспечения пользователь обязан:

- в служебной записке на имя руководителя Учреждения изложить перечень устанавливаемого ПО и пояснить необходимость такой установки;
- передать на согласование служебную записку администратору безопасности.

В случае возникновения сбоя или возникновения ошибок в работе электронной почты, обнаружения подозрительных писем от посторонних адресатов необходимо:

- не открывать письма с сомнительным содержимым;
- приостановить обработку защищаемой информации на ПЭВМ;
- поставить в известность администратора безопасности.

В случае возникновения нештатных ситуаций, не предусмотренных настоящей инструкцией, пользователь обязан поставить в известность лиц, ответственных за защиту информации, с целью выработки совместных действий по устранению возникшей проблемы.

4 ПРАВА И ОТВЕТСТВЕННОСТЬ

Пользователь ИС имеет право:

- в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИС;
- участвовать в анализе ситуаций, касающихся функционирования системы защиты объекта информатизации и расследования фактов несанкционированного доступа к защищаемой информации;
- обращаться к администратору безопасности с просьбой об оказании технической и методической помощи в работе со средствами защиты информации, установленными программными средствами, необходимыми для исполнения своих должностных обязанностей;
- предлагать способы и методы совершенствования системы защиты ИС.

Пользователь несет ответственность в полном объеме по действующему законодательству Российской Федерации за разглашения ставших ему известных сведений, содержащих информацию ограниченного доступа, утерю съемных МНИ и документов, содержащих защищаемую информацию, а также преднамеренную модификацию, копирование и распространение защищаемой информации, обрабатываемой в ИС.

Невыполнение пользователями предъявленных требований может повлечь наступление гражданской, административной, дисциплинарной, либо иной ответственности.

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Защищаемая информация – информация, являющаяся предметом собственности и

подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Компрометация пароля – факт доступа постороннего лица к защищаемой информации, а также возможность такого доступа или подозрение на него.

Контролируемая зона – пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Несанкционированный доступ – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационной системой.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Пользователь информационной системы – сотрудник организации, в рамках своих функциональных обязанностей осуществляющий автоматизированную обработку защищаемой информации и имеющий доступ к программно-аппаратным средствам информационной системы.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов к объектам доступа.

Сертификат защиты – документ, удостоверяющий соответствие средства вычислительной техники или информационной системы набору определенных требований по защите от несанкционированного доступа к информации и дающий право разработчику на использование таких средств.

Система защиты информации – комплекс организационных мер и программно-аппаратных (в том числе криптографических) средств защиты от несанкционированного доступа к информации в информационной системе.

Средство защиты от несанкционированного доступа – программное, техническое или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа.