УТВЕРЖДЕНО
МДОУ ДС «Морошка»
приказом № 23 - Д от 18.11.2022 г.

ИНСТРУКЦИЯ
администратора безопасности информационных систем персональных данных МДОУ ДС «Морошка»

Приложение **№ 10** к приказу № 23 – ОД от 18.11.2022 г.

ИНСТРУКЦИЯ
администратора безопасности информационных систем персональных данных МДОУ «Морошка»

1. Общие положения

1.1. Настоящий документ разработан в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а также другими нормативными правовыми актами по защите информации, и определяет порядок обеспечения безопасности информации при проведении работ администратором безопасности информации (далее - АБИ) в информационных системах персональных данных МДОУ (далее - ИСПД, МДОУ).

1.2. Субъектами доступа к ресурсам ИСПД являются пользователи, администраторы и обслуживающий персонал (сотрудники, осуществляющие техническое обслуживание, ремонт), в соответствии с утвержденным перечнем.

1.3. Обрабатываемая в ИСПД информация относится к сведениям, составляющим персональные данные.

1.4. Машинные носители с защищаемой информацией имеют пометку «персональные данные» (далее- ПД).

1.5. АБИ назначается приказом МДОУ и получает неограниченные права на доступ к ресурсам ИСПД.

1.6. АБИ осуществляет общее руководство и контроль за обеспечением безопасности информации при работе пользователей ИСПД и обслуживающего персонала.

1.7. Методическое руководство по информационной безопасности объектов информатизации осуществляет АБИ.

1.8. АБИ имеет право вносить предложения по изменению и дополнению комплекта организационно-распорядительной документации по защите персональных данных.

1.9. Изменения и дополнения к данной Инструкции утверждаются в установленном порядке.

2. Обязанности администратора безопасности информации

2.1. АБИ обязан знать и выполнять требования комплекта организационно-распорядительной документации по защите персональных данных.

2.2. АБИ, не ознакомленный с данной Инструкцией, а также с изменениями и дополнениями к ней, к работе с ресурсами ИСПД не допускается.

2.3. АБИ осуществляет учет съемных машинных носителей информации, их уничтожение, либо контроль процедуры их уничтожения.

2.4. АБИ обязан немедленно реагировать на сообщения пользователей о любых неисправностях в работе основных и вспомогательных средств и систем (далее - ОТСС и ВТСС), средств защиты информации (далее - СЗИ), системного и прикладного программного обеспечения (далее - ПО) ИСПД.

2.5. АБИ обязан немедленно ставить в известность ответственного по защите информации Администрации обо всех неисправностях аппаратно-программных средств

ИСПД.

2.6. АБИ обязан ставить в известность ответственного по защите информации МДОУ о необходимости проведения работ по администрированию СЗИ.

2.7. АБИ имеет право проводить внеплановые проверки работоспособности СЗИ и соблюдения пользователями технологии обработки персональных данных.

2.8. АБИ разрабатывает планы мероприятий по администрированию и техническому обслуживанию аппаратных и программных средств ИСПД МДОУ.

2.9. АБИ обязан в случае отказа технических средств или программного обеспечения элементов ИСПД, в том числе СЗИ, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

2.10. АБИ имеет право требовать прекращения обработки персональных данных как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПД или СЗИ.

2.11. АБИ присутствует при выполнении технического обслуживания элементов ИСПД сторонними специалистами на территории МДОУ.

2.12. АБИ осуществляет разбирательства и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с техническими и программными средствами ИСПД, в том числе с СЗИ, или по другим нарушениям, которые могут привести к снижению уровня защищенности персональных данных.

2.13. В ходе управления (администрирования) системой защиты ИСПД АБИ обязан осуществлять:

– заведение и удаление учетных записей пользователей, управление полномочиями пользователей ИСПД и поддержание правил разграничения доступа в ИСПД;

– управление СЗИ в ИСПД, в том числе параметрами настройки программного обеспечения, включая программное обеспечение СЗИ, управление учетными записями пользователей, восстановление работоспособности СЗИ, генерацию, смену и восстановление паролей;

– изменение аутентификационной информации (средств аутентификации), заданной их производителями и (или) используемой при внедрении системы защиты информации ИСПД;

– установку обновлений программного обеспечения, включая программное обеспечение СЗИ, выпускаемых разработчиками (производителями) СЗИ или по их поручению;

– централизованное управление системой защиты информации ИСПД (при необходимости);

– регистрацию и анализ событий в ИСПД, связанных с защитой информации;

– информирование пользователей об угрозах безопасности информации, о правилах эксплуатации системы защиты информации ИСПД и отдельных СЗИ, а также их обучение;

– сопровождение функционирования системы защиты информации ИСПД в ходе ее эксплуатации, включая корректировку эксплуатационной документации на нее и организационно-распорядительных документов по защите информации.

2.14. В ходе выявления инцидентов и реагирования на них АБИ обязан осуществлять:

– обнаружение и идентификацию инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и СЗИ, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

– своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в ИСПД;

– анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;

– планирование и принятие мер по устранению инцидентов, в том числе по восстановлению ИСПД и ее сегментов в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных

действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

– планирование и принятие мер по предотвращению повторного возникновения инцидентов.

2.15. В ходе контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в ИСПД, АБИ обязан осуществлять:

– анализ и оценку функционирования системы защиты информации ИСПД, включая выявление, анализ и устранение недостатков в функционировании системы защиты информации ИСПД;

– проверку работоспособности и параметров настройки программного обеспечения, аппаратных и программных СЗИ ИСПД;

– проверку состава технических средств, программного обеспечения и СЗИ;

– контроль целостности печатей (пломб, наклеек) технических средств, используемых для обработки персональных данных;

– еженедельное отслеживание появления новых видов уязвимостей ПО ИСПД. По необходимости АБИ производит устранение уязвимостей согласно рекомендациям разработчика;

– периодический анализ изменения угроз безопасности информации в ИСПД, возникающих в ходе ее эксплуатации, и принятие мер защиты информации в случае возникновения новых угроз безопасности информации;

– контроль за событиями безопасности и действиями пользователей в ИСПД. В частности, АБИ обязан осуществлять постоянный контроль за выполнением пользователями установленного комплекса мероприятий по обеспечению безопасности информации;

– контроль (анализ) защищенности информации, содержащейся в ИСПД;

– документирование процедур и результатов контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в ИСПД;

– принятие решения по результатам контроля (мониторинга) за обеспечением уровня защищенности информации о доработке (модернизации) системы защиты информации ИСПД, повторной аттестации ИСПД или проведении дополнительных аттестационных испытаний.

3. Доступ к ресурсам ИСПД

3.1. Обязательными условиями получения доступа к ресурсам ИСПД являются:

– право доступа в помещение;
– наличие допуска к персональным данным;
– право доступа к ИСПД;
– знание технологии обработки информации в ИСПД с учетом требований информационной безопасности.

3.2. Идентификация АБИ в ИСПД осуществляется по уникальному имени и персональному идентификатору (при его наличии).

3.3.Длина пароля АБИ и всех пользователей - не менее 8 буквенно-цифровых символов.

3.4. Уникальное имя, персональный идентификатор (при его наличии) и пароль АБИ получает в установленном порядке. АБИ обязан их помнить и не допускать раскрытия, не допускается запись на каких-либо носителях в целях напоминания. Во время ввода пароля на клавиатуре должна быть исключена возможность его просмотра другими лицами. Не допускается оставление без присмотра и передача другим лицам персонального идентификатора (при его наличии).

3.5. При утере или подозрении на утечку своего имени, пароля или персонального идентификатора АБИ должен немедленно изменить свои идентификационные данные и проконтролировать возможные изменения в настройках СЗИ.

3.6. Регистрация пользователя осуществляется АБИ в соответствии с Инструкцией по организации парольной защиты и состоит в определении имени регистрируемого пользователя, присвоении ему персонального идентификатора (при его наличии) и назначении пароля.

3.7. При заведении новой учетной записи АБИ должен проверить личность

пользователя и его должностные обязанности.

3.8. Предоставление пользователям прав доступа к объектам доступа ИСПД должно осуществляться на основании задач, решаемых пользователями.

3.9. АБИ не имеет права требовать у пользователей раскрытия их паролей, а также передачи ему персональных идентификаторов (при их наличии), кроме случая изменения идентификационных данных.

3.10. АБИ имеет право требовать у пользователя изменения его пароля, но не имеет права самостоятельно изменять его пароль.

4. Порядок работы с ресурсами ИСПД

4.1. Проверка работоспособности и настройка системы доступа. АБИ присваивает пользователям идентификационные данные к ресурсам ИСПД. При этом должны выполняться следующие требования:

– АБИ определяет политику изменения учетных данных пользователей и периодически контролирует ее соблюдение;

– АБИ сообщает пользователю его уникальное имя и предоставляет возможность задать пароль, далее кодирует персональный идентификатор (при его наличии) пользователя;

– изменение учетных данных пользователя производится АБИ по указанию ответственного за обеспечение безопасности персональных данных Департамента образования, а также периодически по утвержденному плану и в случае увольнения сотрудника.

4.2. Проверка работоспособности и настройка аппаратных и программных средств защиты информации (СЗИ).

АБИ обязан перед началом работ включить и убедиться в работоспособности аппаратных СЗИ, в случае сбоя- работы прекратить.

В случае сбоя СЗИ, таких, как неправильная идентификация пользователей, АБИ обязан приостановить обработку защищаемой информации до устранения неисправности. В случае производственной необходимости- отключить СЗИ и лично контролировать проведение работ пользователями.

4.3. Антивирусная защита ресурсов ИСПД АБИ разрабатывает и контролирует реализацию антивирусной политики, а именно:

– настраивает параметры антивирусной программы;

– контролирует работоспособность антивирусной программы;

– немедленно реагирует на сообщения пользователей о подозрительном поведении ПО, а также о появлении любых сообщений антивирусной программы и принимает соответствующие меры;

– имеет право на проведение внеплановой проверки на наличие вирусов;

– периодически (один раз в неделю) контролирует корректность процесса обновления антивирусных баз, а также исполняемых модулей антивирусной программы.

4.4. Хранение дистрибутивов программного обеспечения СЗИ. АБИ должен хранить дистрибутивы программного обеспечения СЗИ и прикладного программного обеспечения, установленного в ИСПД Департамента образования в месте, исключающем доступ посторонних лиц.

4.5. Проверка целостности системного и прикладного ПО.

Контролю целостности подлежат файлы программного обеспечения ИСПД с расширениями: *.exe, *.cot, * .dll, *.sys, *.vxd,*.drv.

4.6. Резервное копирование и восстановление информации.

Резервное копирование производится регулярно с заданной периодичностью, а также в случае производственной необходимости. При этом необходимо выполнять следующие требования:

– обязательное резервное копирование производится в случае обнаружения неисправностей в работе ПЭВМ или отчуждаемых машинных носителей информации (далее - МНИ);

– допускается обоснованное внеплановое резервное копирование информации как по

инициативе пользователя, так и АБИ, если это не нарушает технологию обработки информации;

– резервные копии пользовательской информации и информации операционной системы хранятся на учтенных внешних МНИ;

– ответственным лицом за хранение резервных копий является АБИ.

По мере устранения неисправностей ПЭВМ АБИ производит восстановление информации ограниченного доступа с резервных копий.

АБИ разрешаются действия в обход установленных процедур идентификации и аутентификации, необходимые только для восстановления функционирования информационной системы в случае сбоев в работе или выходе из строя отдельных технических средств (устройств).

4.7. Конфигурирование ИСПД.

Конфигурационной единицей являются услуги, оборудование, программное обеспечение, здания, люди, документы и пр.

Управление изменениями конфигурации осуществляет ответственный по защите информации. Планирование реализации и непосредственно реализация необходимых изменений возлагается на АБИ.

В ходе управления конфигурацией аттестованной информационной системы и ее системы защиты информации АБИ обязан осуществлять:

– поддержание конфигурации ИСПД и ее системы защиты информации (структуры системы защиты информации ИСПД, состава, мест установки и параметров настройки СЗИ, программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на систему защиты информации (поддержание базовой конфигурации ИСПД и ее системы защиты информации);

– управление изменениями базовой конфигурации ИСПД и ее системы защиты информации, в том числе определение типов возможных изменений базовой конфигурации ИСПД и ее системы защиты информации, санкционирование внесения изменений в базовую конфигурацию ИСПД и ее системы защиты информации, документирование действий по внесению изменений в базовую конфигурацию ИСПД и ее системы защиты информации, сохранение данных об изменениях базовой конфигурации ИСПД и ее системы защиты информации, контроль действий по внесению изменений в базовую конфигурацию ИСПД и ее системы защиты информации;

– анализ потенциального воздействия планируемых изменений в базовой конфигурации ИСПД и ее системы защиты информации на обеспечение защиты информации, возникновение дополнительных угроз безопасности информации и работоспособность ИСПД;

– определение параметров настройки программного обеспечения, включая программное обеспечение СЗИ, состава и конфигурации технических средств и программного обеспечения до внесения изменений в базовую конфигурацию ИСПД и ее системы защиты информации;

– внесение информации (данных) об изменениях в базовой конфигурации ИСПД и ее системы защиты информации в документацию на систему защиты информации ИСПД;

– принятие решения по результатам управления конфигурацией о повторной аттестации ИСПД или проведении дополнительных аттестационных испытаний.

Обязанности по управлению изменениями в аппаратном и программном обеспечении и всех элементах документации, которые связаны с работой, поддержкой и сопровождением систем, находящихся в эксплуатации, возлагаются на АБИ. При возникновении необходимости изменения конфигурации ИСПД, аттестованной по требованиям безопасности информации, АБИ согласовывает планируемые изменения с предприятием-лицензиатом, проводившим аттестационные испытания.

4.8. Вывод ресурсов ИСПД из эксплуатации.

При невозможности ремонта различных ресурсов ИСПД АБИ обязан:

– физически уничтожать любые МНИ, независимо от содержащейся на них информации; картриджи принтера, иные комплектующие могут быть использованы за пределами ИСПД;

– факт выхода из строя и замены оборудования должен быть отражен в Техническом

паспорте на ИСПД.

4.9. Реагирование на сбои при регистрации событий безопасности.

Реагирование на сбои при регистрации событий безопасности осуществляется АБИ путем изменения параметров сбора, записи и хранения информации о событиях безопасности в журналах СЗИ от НСД, в том числе отключение записи информации о событиях безопасности от части компонентов ИСПД, запись поверх устаревших хранимых записей событий безопасности.

В случае выявления признаков инцидентов безопасности АБИ обязан:

– немедленно доложить ответственному по защите информации о данном факте;

– по возможности в максимально сжатые сроки установить причину возникновения инцидента и исключить возможность его повторения;

– восстановить работоспособность ИСПД;

– по окончании работ по восстановлению работоспособности ИСПД произвести запись в Журнал регистрации событий информационной безопасности и мер, принятых для устранения попыток несанкционированного системного доступа по форме согласно приложению, к настоящей Инструкции.

5. Действия при обнаружении попыток несанкционированного доступа

5.1. К попыткам несанкционированного доступа относятся:

– сеансы работы с ИСПД незарегистрированных пользователей, пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истек, или превышающих свои полномочия по доступу к данным;

– действия постороннего лица, пытающегося получить доступ (или уже получившего доступ) к ИСПД, при использовании учетной записи администратора или другого пользователя ИСПД, методом подбора пароля, использования пароля, разглашенного владельцем учетной записи или любым другим методом.

5.2. При выявлении факта несанкционированного доступа АБИ обязан:

– пресечь дальнейший несанкционированный доступ к ИСПД;

– доложить ответственному по защите информации Департамента образования служебной запиской о факте несанкционированного доступа, его результате (успешный/неуспешный) и предпринятых действиях;

– известить руководителя структурного подразделения, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка несанкционированного доступа, о факте несанкционированного доступа.

6. Ответственность

6.1. АБИ несет персональную ответственность:

– за сохранность носителей информации и содержащейся на них информации в рабочее время;

– за несоблюдение требований данной Инструкции и неправомерное использование ресурсов ИСПД;

– за правильную работу установленных в ИСПД Департамента образования средств защиты информации;

– за качество проводимых работ по обеспечению безопасности персональных данных и за все действия, совершенные от имени учетной записи АБИ в ИСПД, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования учетной записи.

6.2. АБИ при нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несет дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации