Приложение к приказу 126-О от 25.10.2022 г.
Зав [подпись]

Инструкция Администратора безопасности ИСПД по обеспечению безопасности информации при обработке персональных данных в МБДОУ ДС ОВ № 42

1. Общие положения

1.1.Инструкция Администратора безопасности ИСПД по обеспечению безопасности информации при обработке персональных данных в администрации муниципального образования Северский район (далее Инструкция) разработана в соответствии с типовой инструкцией, одобренной решением Межведомственной комиссией по защите государственной тайны от 9 октября 2009 года № 172, доведенной письмом заместителя управляющего делами, директора социально-производственного департамента администрации Краснодарского края от 2 марта 2010 года №44с.

1.2. В настоящей Инструкции используются следующие основные понятия:

Автоматизированная система (АС) – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций;

Администратор безопасности информационных систем персональных данных (Администратор безопасности ИСПД) – начальник Управления образования администрации муниципального образования Северский район, ответственный за защиту ИСПД, содержащих информационные системы персональных данных;

Аттестация объектов информатизации – комплексная проверка (аттестационные испытания) защищаемого объекта информатизации в реальных условиях эксплуатации с целью оценки соответствия применяемого комплекса мер и средств защиты требуемому уровню безопасности информации;

Безопасность информации – состояние защищенности информации, обрабатываемой средствами вычислительной техники и средствами автоматизации от внутренних и внешних угроз;

Вспомогательные технические средства и системы (ВТСС) - технические средства и системы, не предназначенные для передачи, обработки и хранения информации, содержащей персональные данные, устанавливаемые совместно с основными техническими средствами;

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

Защита информации - деятельность по предотвращению утечки защищаемой информации, несанкционированных и преднамеренных и непреднамеренных воздействий на защищаемую информацию;

Информационные ресурсы - отдельные документы и отдельные массивы документов, документы и массивы документов, содержащиеся в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах), а также машинные носители информации (жёсткие магнитные диски, гибкие магнитные диски, оптические диски и т.п.);

Информационные системы персональных данных (ИСПД) - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;

Контролируемая зона (КЗ) - пространство (территория, здание, часть здания и т.п.), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или временного пропуска;

Мероприятия по защите информации - совокупность действий, направленных на разработку и/или практическое применение методов, способов и средств защиты информации;

Несанкционированный доступ к информации (НСД) - доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами;

Носитель информации - физическое лицо или материальный объект, в том числе физические поля, в которых информация находит своё отображение в виде символов, образов, сигналов, технических решений, процессов и количественных характеристик физических величин;

Объект информатизации - совокупность информационных ресурсов, основных технических средств и систем обработки информации, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, средств), в которых они установлены;

Обработка информации - совокупность операций сбора, накопления, ввода-вывода, приема-передачи, записи, хранения, регистрации, уничтожения, преобразования и отображения, осуществляемых над информацией;

Объект защиты информации - информация, носитель информации или информационный процесс, которые необходимо защищать в соответствии с поставленной целью защиты информации;

Организационно-технические мероприятия по обеспечению защиты информации - совокупность действий, направленных на применение организационных мер и программно-технических способов защиты информации, на объекте информатизации;

Основные технические средства и системы (ОТСС) технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи информации, содержащей персональные данные;

Персональные данные (ПД) – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

Пользователь ИСПД – сотрудник структурного подразделения администрации муниципального образования Северский район, пользующийся информацией, полученной от её собственника, владельца или посредника (персональными данными) в соответствии с установленными правами и правилами доступа к информации;

Режимное помещение - помещение, в котором располагается АС, содержащая ИСПД и/или хранятся в нерабочее время носители сведений, составляющие конфиденциальную информацию, и обеспечивается сохранность указанных сведений;

Система защиты информации ИСПД - совокупность технических, программных и программно-технических средств защиты информации и средств контроля эффективности защиты информации;

Средства вычислительной техники (СВТ) - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем;

Средства защиты информации (СЗИ) - технические, криптографические, программные и другие средства, предназначенные для защиты информации в ИСПД, в которых они реализованы, также средства контроля эффективности защиты информации.

1.3. Инструкция определяет обязанности должностных лиц, а также требования к содержанию и порядку осуществления мероприятий по обеспечению защиты информации в ИСПД, применительно к следующим категориям сотрудников:

- начальник Управления образования;
- первый заместитель начальника Управления образования;
-заместитель начальника Управления образования;
- Пользователи ИСПД.

1.4. Инструкция устанавливает единый порядок и основные требования при подготовке к обработке и при обработке информации в ИСПД в Управлении образования администрации муниципального образования Северский район (далее Управление).

1.5. К ознакомлению с Инструкцией в полном объёме допускаются все пользователи ИСПД.

1.6. Обработка информации в ИСПД осуществляется на аттестованной по требованиям безопасности информации АС, реализующей заданную

технологию обработки информации.

1.7. Основные мероприятия по обеспечению защиты в ИСПД, проводятся в соответствии с «Положением о методах и способах защиты информации в информационных системах персональных данных», утвержденных Федеральной службой по техническому и экспортному контролю Приказом от 5 февраля 2010 года №58.

1.8. Ответственность за организацию обеспечения защиты информации в ИСПД при её обработке, возлагается на начальника Управления образования или должностное лицо его замещающее.

1.9. Ответственными за осуществление мероприятий по защите информации в ИСПД, при её обработке в Управлении назначаются:

- первый заместитель начальника Управления «Администратор безопасности ИСПД - 1»;
- заместитель начальника Управления - «Администратор безопасности ИСПД - 2»;

1.10. Должностные лица, допустившие нарушения требований руководящих и нормативных документов по вопросам защиты (обеспечения безопасности) информации в ИСПД, привлекаются к дисциплинарной, административной или уголовной ответственности в соответствии с законодательством Российской Федерации.

1.11. Обработка информации в ИСПД допускается только после проведения в установленном порядке аттестации АС на соответствие обязательным требованиям по безопасности информации и ввода их в эксплуатацию.

1.12. По фактам и попыткам несанкционированного доступа к информации в ИСПД, а также случаям утечки обрабатываемой с использованием СВТ информации, должны проводиться служебные расследования. До завершения служебного расследования обработка информации в АС запрещается.

2. Требования к содержанию и порядку осуществления мероприятий по защите (обеспечению безопасности) информации в ИСПД, в Управлении образования администрации муниципального образования Северский район

2.1. Организацию подготовки АС, предназначенных для обработки информации в ИСПД к аттестации по требованиям безопасности информации осуществляет Администратор безопасности ИСПД.

2.2. Состав программного обеспечения, технических средств и средств автоматизации, предназначенных для обработки информации в ИСПД, должен соответствовать номенклатуре, объёму и сложности задач, решаемых с использованием СВТ, а также в соответствии с классом ИСПД.

2.3. В состав программного обеспечения АС, предназначенной для обработки информации в ИСПД, помимо общего (операционные системы, текстовые и графические редакторы, средства архивации данных, средства

доступа к файловой системе, средства мультимедиа и др.) и специального (прикладного) программного обеспечения обязательно включается сертифицированный по требованиям безопасности информации антивирусный программный продукт.

2.4. Из состава технических средств и систем АС, предназначенных для обработки информации в ИСПД должны быть исключены (заблокированы) избыточные элементы и, в первую очередь, устройства ввода/вывода информации на внешние носители.

2.5. Размещение и монтаж ОТСС, предназначенных для отображения и создания копий документов на бумажных носителях (видеотерминалов, печатающих устройств, графопостроителей и т.п.) необходимо проводить с учётом максимального затруднения визуального просмотра информации посторонними лицами (шторы и/или жалюзи на окнах, непрозрачные экраны и т.п.).

2.6. АС, предназначенные для обработки информации в ИСПД класса 1 и 2, должны пройти специальные исследования и иметь предписания на эксплуатацию (аттестаты соответствия требованиям по безопасности информации).

2.7. На АС, содержащих ИСПД класса 3, в соответствии с «Положением о методах и способах защиты информации в информационных системах персональных данных», утвержденных Федеральной службой по техническому и экспортному контролю Приказом от 5 февраля 2010 года №58 должны быть проведены соответствующие мероприятия по защите информации и утверждена Декларация соответствия АС требованиям безопасности (далее Декларация). Декларацию утверждает Рабочая группа по проведению классификации ИСПД и аттестации ИСПД классом 3 подписанием соответствующего акта (далее Рабочая группа).

2.8. Защита информации в ИСПД, обрабатываемой с использованием АС, должна осуществляться посредством выполнения комплекса мероприятий по предотвращению утечки информации по техническим каналам, за счёт несанкционированного доступа к ней, а также по предупреждению преднамеренных программно-технических воздействий на информацию с целью нарушения её конфиденциальности и доступности в процессе её обработки, передачи и хранения.

2.9. Отладочные и экспериментальные работы (опробование программ, формирование массивов информации и др.) проводятся до ввода автоматизированной системы в эксплуатацию под руководством Администратора безопасности ИСПД.

2.10. Все СЗИ, применяемые для защиты информации в ИСПД, должны иметь сертификаты соответствия по требованиям безопасности информации, а эффективность применяемых технических и/или организационных решений, направленных на обеспечение конфиденциальности, целостности и доступности информации, должна быть подтверждена результатами аттестационных испытаний АС.

2.11. Технические и организационные решения для конкретной информационной технологии разрабатываются организацией, имеющей соответствующие лицензии органа, уполномоченного на ведение лицензионной деятельности.

2.12. При проведении технического обслуживания и ремонта СВТ непосредственно на объекте информатизации допуск сотрудников сервисных (ремонтных) организаций осуществляется в установленном порядке при наличии у них соответствующей лицензии и предписания на осуществление работ (услуг).

2.13. При проведении технического обслуживания и ремонта запрещается передавать ремонтным организациям узлы и блоки с элементами накопления и хранения информации, содержащей ПД. Вышедшие из строя элементы и блоки СВТ заменяются на элементы и блоки, прошедшие специальные исследования, при этом осуществляется контроль эффективности защиты информации (от утечек по техническим каналам) и при необходимости проводится переаттестация по требованиям безопасности информации.

2.14. Ответственность за обеспечение защиты информации в ИСПД возлагается на руководителя Управления, в чьем ведомстве располагается АС, обрабатывающая ИСПД.

2.15. Допуск Пользователей ИСПД к работе на аттестованной по требованиям безопасности информации АС осуществляется после ввода её в эксплуатацию приказом Управления образования и назначения лиц, ответственных за эксплуатацию АС.

2.16. Контроль допуска к автоматизированной обработке информации осуществляет Администратор безопасности ИСПД.

2.17. После решения задач с использованием АС вся информация в ИСПД, не предназначенная для дальнейшего использования, должна быть стёрта со всех машинных носителей информации. Стирание информации должно производиться либо специальными программами, сертифицированными по требованиям безопасности информации, либо средствами, входящими в состав сертифицированных средств защиты информации, обеспечивающими невозможность восстановления и просмотра информации с помощью любых программных средств, на штатном оборудовании аттестованной по требованиям безопасности информации АС.

2.18. При эксплуатации АС, предназначенной для обработки информации в ИСПД запрещается:

- проводить обработку информации без выполнения обязательных мероприятий по её защите;
- вносить изменения в состав, конструкцию, конфигурацию и размещение технических средств в аттестованной по требованиям безопасности информации АС;
- вносить изменения в состав программного обеспечения, структуру файловой системы АС без письменного разрешения, согласованного с Администратором безопасности ИСПД;

- осуществлять попытки несанкционированного доступа к резервам информационной системы и других пользователей;

- подключать АС к информационным сетям общего пользования и другим АС;

- отключать (блокировать) средства защиты информации АС;

- использовать неисправные машинные носители информации для её хранения и обработки;

- производить запуск АС с системных дискет или загрузочных CD дисков без письменного Администратора безопасности ИСПД;

- разглашать сведения о реализованном в АС комплексе средств защиты информации;

- накапливать на машинных носителях информации данные, надобность в которых миновала;

- хранить машинные носители информации вблизи сильных источников электромагнитных излучений;

- оставлять АС при выходе Пользователя ИСПД из помещения, в котором она установлена, не убедившись, что она заблокирована средствами защиты или отключена.

2.19. При внесении изменений в состав программного обеспечения, структуру файловой системы АС, содержащей ИСПД класса 3, необходимо провести дополнительные мероприятия по защите информации, внести изменения в Декларацию и утвердить ее повторно Рабочей.

2.20. При внесении изменений в состав программного обеспечения, структуру файловой системы АС, содержащей ИСПД класса 1 и 2, специалистами организаций, имеющих соответствующие лицензии проводится переаттестация АС.

3. Должностные обязанности сотрудников Управления образования муниципального образования Северский район, ответственных за осуществление мероприятий по обеспечению защиты информации в ИСПД

3.1. Администратор безопасности ИСПД отвечает за соблюдение на объекте информатизации требований по обеспечению безопасности информации и правильность применения средств защиты информации от НСД.

Он обязан:

- разрабатывать предложения по составу общесистемных программных средств, обеспечивающих функционирование АС, подлежащей аттестации по требованиям безопасности информации;

- разрабатывать матрицу доступа пользователей к защищаемым информационным ресурсам ИСПД, подлежащей аттестации по требованиям безопасности информации;

- определять класс ИСПД, подлежащей аттестации по требованиям безопасности информации, от НСД ;

- составлять и представлять на утверждение начальнику Управления образования список сотрудников, доступ которых к персональным данным, обрабатываемым в ИСПД, необходим для выполнения служебных (трудовых) обязанностей;

- вести «Журнал учета лиц, допущенных к работе с персональными данными в ИСПД»;

- участвовать и контролировать проведение аттестационных испытаний АС;

- знать способы, методы и средства защиты информации в ИСПД от НСД;

- знать перечень задач, решаемых с использованием АС и Пользователей ИСПД, допущенных к их решению;

- осуществлять допуск пользователей к техническим средствам АС и информации в соответствии с разрешительной системой доступа;

- ежегодно проводить занятия, доводить основные положения нормативных, правовых и руководящих документов по вопросам защиты (обеспечения безопасности) информации в ИСПД;

- проводить разбирательства по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных;

- контролировать своевременность представления списков пользователей, допускаемых к защищаемым ресурсам АС, с целью закрепления за ними паролей, а также прав пользования ресурсами СВТ;

- обеспечивать (осуществлять) смену и ввод пароля разграничения доступа к информационным ресурсам пользователей ИСПД с периодичностью не реже одного раза в квартал;

- периодически, не реже двух раз в год, тестировать все функции системы разграничения доступа к информации, обрабатываемой с использованием АС;

- планировать мероприятия по обеспечению защиты (обеспечению безопасности) информации в ИСПД;

- осуществлять визуальный контроль целостности компонентов СВТ, а также целостность элементов контроля НСД (наклеек, пломб, защитных знаков) к внутренним узлам и блокам СВТ;

- осуществлять проверку АС на наличие компьютерных «вирусов»;

- своевременно обновлять базы антивирусных программ;

- контролировать правильность применения и работоспособность средств защиты информации от НСД на объекте информатизации;

- вести учёт, хранение, закрепление и выдачу паролей доступа к техническим средствам и информационным ресурсам АС;

- докладывать начальнику Управления образования о нарушениях или невыполнении пользователями ИСПД требований по защите (обеспечению безопасности) информации и правил обращения со съёмными машинными

носителями информации;

- организовывать разработку (уточнение) Инструкции и обеспечивать её строгое выполнение;

- разрабатывать и представлять на утверждение начальнику Управления образования предложения о назначении ответственных за защиту (обеспечение безопасности) информации в ИСПД;

- производить приостановку предоставления персональных данных пользователям информационной системы при обнаружении нарушений порядка предоставления персональных данных;

- регулярно создавать резервные копии системных файлов и обрабатываемых данных, подлежащих хранению, на специально учтённых в режимном помещении съёмных машинных носителях информации.

- составлять списки Пользователей ИСПД, допущенных к обработке ПД на АС и представляют их на утверждение начальнику Управления;

- подготавливают организационные и технические документы, необходимые для проведения классификации ИСПД ;

3.3. Пользователь ИСПД отвечает за техническое состояние АС, установленный порядок использования программного обеспечения, а также применение технических и программных СЗИ.

Он обязан:

- знать перечень задач, решаемых с использованием аттестованных по требованиям безопасности информации АС, сроки их выполнения;

- вести учёт аттестованных по требованиям безопасности информации объектов информатизации, СВТ и оргтехники, прошедшей специальную проверку и имеющих предписания на эксплуатацию;

- знать требования руководящих документов по защите (обеспечению безопасности) информации и Инструкции;

- осуществлять работы с использованием АС только после получения разрешения Администратора ИСПД на автоматизированную обработку информации;

- соблюдать утверждённую матрицу доступа пользователей к защищаемым информационным ресурсам ИСПД, обрабатываемой с использованием АС ;

- осуществлять визуальный контроль целостности компонентов АС, а также целостность элементов контроля НСД (наклеек, пломб, защитных знаков) к внутренним узлам и блокам СВТ;

- докладывать Администратору безопасности ИСПД и информировать начальника Управления образования о выявленных изменениях в конфигурации технических средств и программного обеспечения АС;

- немедленно докладывать Администратору безопасности ИСПД и информировать начальника Управления о фактах и попытках НСД к обрабатываемой (хранящейся) в АС информации.

С инструкцией ознакомлены: