МУНИЦИПАЛЬНОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ
ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ
«ЦЕНТР ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ»

ПРИКАЗ

«30» декабря 2016 года г. Благодарный № 95

Об утверждении инструкций и перечней

В соответствии с Конституцией Российской Федерации, Трудовым Кодексом Российской Федерации, Федеральным законом от 27.07.2006 N149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 N152-ФЗ «О персональных данных», иными нормативно-правовыми актами, действующими на территории Российской Федерации

ПРИКАЗЫВАЮ:

1. Утвердить:

1.1. перечень должностных лиц МКУ ДО «ЦДО», доступ которых к персональным данным необходим для выполнения служебных (трудовых) обязанностей (приложение 1);

1.2. перечень неавтоматизированных систем, в которых обрабатываются персональные данные (приложение 2);

1.3. инструкцию администратора информационной безопасности информационных систем персональных данных (приложение 3);

1.4. инструкцию пользователям информационных систем персональных данных по действиям в нештатных ситуациях (приложение 4);

1.5. перечень мест хранения материальных носителей персональных данных (приложение 5);

1.6. инструкцию по установке, модификации и обслуживанию программного обеспечения и техническому обслуживанию аппаратных средств информационных систем персональных данных (приложение 6);

1.7. инструкцию пользователя информационной системы персональных данных (приложение 7).

2. Контроль за исполнением настоящего приказа оставляю за собой.

Директор муниципального казенного
учреждения дополнительного образования
«Центр дополнительного образования» Е.П. Косилова

Приложение 1
к приказу от 30 декабря 2016 года №95

Перечень должностных лиц
МКУ ДО «ЦДО», доступ которых к персональным данным необходим для выполнения служебных (трудовых) обязанностей

1. Директор МКУ ДО «ЦДО»
2. Заместитель директора МКУ ДО «ЦДО»
3. Секретарь-машинистка
4. Старшие педагоги дополнительного образования
5. Ответственный администратор ИС «Аверс»
6. Педагоги дополнительного образования
7. Ответственный за охрану труда
8. Заведующий хозяйством

Приложение 2
к приказу от 30 декабря 2016 года №95

Перечень неавтоматизированных систем, в которых обрабатываются персональные данные

№ п/п	Система	Виды персональных данных
1	Кадровый и бухгалтерский учет	ФИО, дата и место рождения, адрес, семейное, социальное и имущественное положение, образование и специальность, профессия, должность, заработная плата (оклад, премии, надбавки), судимости и/или наличие обязательств по исполнительным листам, паспортные данные, ИНН, информация о воинской обязанности, данные страхового полиса обязательного медицинского страхования, данные страхового полиса обязательного пенсионного страхования, личные дела, трудовой и общий стаж.
2	Учет договоров по оказанию услуг сторонними организациями (физическими лицами)	ФИО, дата и место рождения, адрес, имущественное положение, паспортные данные, ИНН, номера банковских расчетных счетов, номер страхового полиса обязательного пенсионного страхования
3	Охрана труда и техника безопасности	ФИО, дата и место рождения, адрес, семейное положение, образование и специальность, профессия, должность, фотография (только для удостоверений на отдельные специальности)
4	Деятельность профкома	ФИО, дата и место рождения, адрес, профессия, должность, фамилия, имя отчество, дата рождения детей.
5	Деятельность образовательных организаций	ФИО, дата и место рождения, адрес, имущественное положение, паспортные данные, ИНН, номера банковских расчетных счетов, номер страхового полиса обязательного пенсионного страхования

Приложение 3
к приказу от 30 декабря 2016 года №95

Инструкция
администратора информационной безопасности информационных систем персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Администратор информационной безопасности информационной системы персональных данных (ИСПДн) МКУ ДО «ЦДО» (далее – Учреждение) назначается приказом директора. Он руководствуется требованиями нормативных документов Российской Федерации, нормативных актов Учреждения, настоящей Инструкцией, а также другими распорядительными документами в части, его касающейся.

1.2. Администратор ИБ ИСПДн в пределах своих функциональных обязанностей обеспечивает работоспособность ИСПДн, безопасность персональных данных, обрабатываемой, передаваемой и хранимой при помощи средств вычислительной техники (СВТ) в ИСПДн Учреждения.

1.3. Должностные лица Учреждения, задействованные в обеспечении функционирования ИСПДн, могут быть ознакомлены с основными положениями и приложениями Инструкции в части, их касающейся, по мере необходимости.

1.4. В случае увольнения (снятия обязанностей), администратор ИБ ИСПДн Учреждения, обязан передать директору все носители защищаемой информации Учреждения (рукописи, черновики, чертежи, диски, дискеты, распечатки с принтеров, модели, материалы, изделия и пр.), которые находились в его распоряжении в связи с выполнением им служебных обязанностей во время работы в Учреждения.

2. ОБЯЗАННОСТИ АДМИНИСТРАТОРА ИБ ИСПДн

2.1. Администратор информационной безопасности ИСПДн обязан:

- знать перечень установленных в Учреждении средств вычислительной техники
- знать перечень задач, решаемых с использованием средств вычислительной техники;
- знать обо всех технологических процессах, производимых вычислительной техникой
- обеспечивать работоспособность средств вычислительной техники ИСПДн Учреждения;
- проводить организационно-технические мероприятия по обслуживанию и ремонту СВТ Учреждения, как собственными силами, так и

с привлечением (на договорной основе) сторонних организаций, имеющих лицензирование на право ремонта и обслуживания;

- устанавливать и настраивать элементы ИСПДн и средства защиты информации;
- рассматривать возможность применения новых технологий для повышения эффективности функционирования ИСПДн Учреждения;
- выполнять своевременное обновление программного обеспечения элементов ИСПДн и средств защиты персональных данных (СЗПДн) по мере появления таких обновлений;
- уметь выполнять резервное копирование и восстановление данных;
- обеспечивать контроль за выполнением пользователями требований «Инструкции пользователю ИСПДн»;
- осуществлять контроль за работой пользователей автоматизированных систем, выявление попыток НСД к защищаемым информационным ресурсам и техническим средствам ИСПДн Учреждения;
- осуществлять настройку средств защиты, выполнять другие действия по изменению элементов ИСПДн;
- осуществлять учет всех защищаемых носителей информации с помощью их любой маркировки и с занесением учетных данных в специальный журнал (учетную карточку). Учтенные носители информации выдавать пользователям под роспись;
- осуществлять текущий и периодический контроль работы средств и систем защиты информации;
- осуществлять текущий контроль технологического процесса обработки защищаемой информации;
- периодически, при изменении программной среды и смене персонала ИСПДн, осуществлять тестирование всех функций системы защиты с помощью тестовых программ, имитирующих попытки НСД,;
- в случае возникновения нештатных ситуаций (сбоев в работе СЗПДн) немедленно докладывать ответственному за обеспечение безопасности ПДн;
- участвовать в проведении служебных расследований фактов нарушения или угрозы нарушения безопасности защищаемой информации;
- участвовать в проведении работ по восстановлению работоспособности средств и систем защиты информации;
- вести «Журнал учета нештатных ситуаций». Форма журнала приведена в «Инструкции по действиям персонала в нештатных ситуациях»;
- вести учёт фактического вскрытия и опечатывания СВТ;
- вести учёт выполнения профилактических работ
- вести учёт установки и модификации программного обеспечения средств СВТ;
- вести учёт замены аппаратных компонентов СВТ;
- проводить инструктаж и обучение работников ГУП (пользователей СВТ) правилам работы с оргтехникой;

- проводить инструктаж уполномоченных работников ИСПДн правилам работы со средствами защиты информации с отметкой в карточке инструктажа (Приложение 2);
- участвовать в разработке нормативных и методических документов, связанных с функционированием ИСПДн и применением средств защиты персональных данных;
- регулярно анализировать работу любых элементов ИСПДн, электронных системных журналов средств защиты для выявления и устранения неисправностей, а также для оптимизации ее функционирования.
- выполнять иные возложенные на него задачи в соответствии с распорядительными, инструктивными и методическими материалами в части, его касающейся;

3. ПРАВА АДМИНИСТРАТОРА ИБ ИСПДн

3.1. Администратор ИБ ИСПДн имеет право:

- отключать любые элементы СЗПДн при изменении конфигурации, регламентном техническом обслуживании или устранении неисправностей в установленном порядке;
- в установленном порядке изменять конфигурацию элементов ИСПДн и СЗПДн;
- требовать от сотрудников Учреждения соблюдения правил работы в ИСПДн, приведенных в «Инструкции пользователя ИСПДн»;
- требовать от пользователей безусловного соблюдения установленной технологии обработки защищаемой информации и выполнения требований внутренних документов Учреждения, регламентирующих вопросы обеспечения безопасности и защиты персональных данных;
- обращаться к ответственному за обеспечение безопасности ПДн с требованием прекращении обработки информации в случаях нарушения установленной технологии обработки защищаемой информации или нарушения функционирования средств и систем защиты информации;
- вносить свои предложения по совершенствованию функционирования ИСПДн Учреждения;
- инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности в ИСПДн Учреждения.

4. ОТВЕТСТВЕННОСТЬ АДМИНИСТРАТОРА ИБ ИСПДн

4.1. Администратор ИБ ИСПДн несет ответственность:

- за ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей инструкцией, другими инструктивными документами в соответствии с действующим трудовым

законодательством Российской Федерации, за полноту и качество проводимых им работ по обеспечению защиты информации;

- за правонарушения, совершенные в процессе своей деятельности в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации;
- за разглашение сведений конфиденциального характера и другой защищаемой информации Учреждения в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации;
- на администратора ИБ ИСПДн возлагается персональная ответственность за работоспособность и надлежащее функционирование средств обработки ПДн в ИСПДн и средств защиты персональных данных Учреждения.

5. ПОРЯДОК ПЕРЕСМОТРА ИНСТРУКЦИИ

5.1. Инструкция подлежит полному пересмотру при изменении перечня решаемых задач, состава технических и программных средств ИСПДн Учреждения, приводящих к существенным изменениям технологии обработки информации, с целью проверки соответствия положений данного документа реальным условиям применения. Полный пересмотр данного документа проводит ответственный за обеспечение безопасности ПДн Учреждения.

5.2. В иных случаях Инструкция подлежит частичному пересмотру. Частичный пересмотр проводит ответственный за обеспечение безопасности ПДн Учреждения. Вносимые изменения не должны противоречить другим положениям Инструкции.

Приложение 4
к приказу от 30 декабря 2016 года № 95

Инструкция
пользователям информационных систем персональных данных по действиям в нештатных ситуациях

1. Общие положения

Настоящая Инструкция предназначена для определения порядка действий пользователей информационной системы персональных данных (ИСПДн) МКУ ДО «ЦДО» (далее – Учреждение) при возникновении нештатных ситуаций.

Нештатными ситуациям являются:

1) разглашение информации ограниченного доступа, не составляющей государственную тайну (далее защищаемая информация), сотрудниками Учреждения, имеющими к ней право доступа, в том числе:

- разглашение защищаемой информации лицам, не имеющим права доступа к защищаемой информации;
- передача защищаемой информации по открытым линиям связи;
- обработка защищаемой информации на незащищенных технических средствах обработки информации;
- опубликование защищаемой информации в открытой печати и других средствах массовой информации;
- передача носителя с защищаемой информации лицу, не имеющему права доступа к ней;
- утрата носителя с защищаемой информацией;

2) неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации:

- несанкционированное изменение защищаемой информации;
- несанкционированное копирование защищаемой информации.

3) Несанкционированный доступ к защищаемой информации:

- подключение технических средств к средствам и системам объекта информатизации;
- использование закладочных устройств;
- маскировка под зарегистрированного пользователя;
- использование дефектов программного обеспечения ИСПДн
- использование программных закладок;
- применение программных вирусов;
- хищение носителя защищаемой информации;
- нарушение функционирования технических средств обработки защищаемой информации;

- блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку;

4) дефекты, сбои, отказы, аварии ТС и систем ИСПДН;
5) дефекты, сбои и отказы программного обеспечения ИСПДН;
6) сбои, отказы и аварии систем обеспечения ИСПДН;
7) природные явления, стихийные бедствия:

- термические, климатические факторы (пожары, наводнения и т.д.);
- механические факторы (землетрясения и т.д.);
- электромагнитные факторы (грозовые разряды и т.д.).

В случае возникновения нештатной ситуации, порядок действий при которой не регламентирован настоящей инструкцией, лицами, ответственным за обеспечение безопасности персональных данных Учреждения, вырабатывается конкретный план действий с учетом сложившийся ситуации.

Для эффективной реализации мероприятий по реагированию в случае нештатных ситуаций должны проводиться регулярные тренировки по различным нештатным ситуациям. По результатам тренировки в случае необходимости проводится уточнение настоящей Инструкции.

Должностные лица Учреждения знакомятся с основными положениями и приложениями Инструкции в части, их касающейся, по мере необходимости.

Ознакомление с требованиями Инструкции сотрудников Учреждения осуществляет инженер-программист, или специалисты группы информационных систем Учреждения, под роспись, с выдачей электронных копий Инструкции непосредственно для повседневного использования в работе.

2. Порядок действий при обнаружении нештатных ситуаций

Классификация нештатных ситуаций

Нештатные ситуации классифицируются в соответствии с оценками, представленными в таблице 1.1.

Таблица 1.1. Оценки нештатных ситуаций

Нештатная ситуация		**Оценка ситуации (раздел Инструкции)**
Разглашение защищаемой информации сотрудниками, имеющими к ней право доступа		(0)
Неправомерные действия со стороны лиц, имеющих право	Несанкционированное копирование конфиденциальной информации	Обнаружился случившийся факт (0)
		Производится в текущий момент (0)

Нештатная ситуация		Оценка ситуации (раздел Инструкции)
доступа к защищаемой информации	Несанкционированное изменение конфиденциальной информации	Обнаружился случившийся факт (0)
		Производится в текущий момент (0)
Несанкционированный доступ к защищаемой информации	Подключение технических средств к техническим средствам ИСПДн	Обнаружился случившийся факт (0)
		Производится в текущий момент (0)
	Установка закладочных устройств	Обнаружение установленных (0)
		Устанавливаются в настоящий момент (0)
	Маскировка под зарегистрированного пользователя	Внешним злоумышленником в текущий момент (0)
		Внутренним злоумышленником, либо производилась в прошлом (0)
	Использование дефектов программного обеспечения ИСПДН	Внешним злоумышленником в текущий момент (0)
		Внутренним злоумышленником, либо производилось в прошлом (0)
	Использование программных закладок	Внешним злоумышленником в текущий момент (0)
		Внутренним злоумышленником, либо производилось в прошлом (0)
	Обнаружение программных вирусов	(0)
	Хищение носителя защищаемой информации	(0)
	Нарушение функционирования ТС обработки информации злоумышленником	Производится в текущий момент (0)
		Обнаружился случившийся факт (0)
	Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку	Производится в текущий момент внешним злоумышленником (0)
		Производится в текущий момент внутренним злоумышленником (0)
		Обнаружился случившийся факт (0)
Ошибки пользователей системы при эксплуатации программных и технических средств, средств и систем защиты информации		Ошибка повлекла утерю или повреждение защищаемой информации (0)
		Ошибка привела к нарушению работоспособности ТС и ПО (0)
Дефекты, сбои, отказы, аварии ТС, программных средств и систем ИСПДН		(0)
Сбои, отказы и аварии систем обеспечения ИСПДН		(0)
Природные явления, стихийные бедствия	Несущие угрозу жизни человека	(0)
	Не несущие угрозу жизни человека	(0)

Нештатные ситуации, которые повлекли утечку или повреждение защищаемой информации, либо созданы внутренним злоумышленником. При обнаружении нештатных ситуаций, которые повлекли утечку или повреждение защищаемой информации, либо созданы внутренним злоумышленником, создается комиссия.

В первую очередь инженером-программистом, и специалистами Учреждения предпринимаются действия по сбору и обеспечению сохранности улик незаметно для злоумышленника при нештатных ситуациях, связанных с:

- разглашением конфиденциальной информации;
- обнаружением несанкционированно скопированной или измененной конфиденциальной информации;
- обнаружением подключения технических средств к средствам и системам объекта информатизации;
- обнаружением закладочных устройств;
- маскировкой под зарегистрированного пользователя внутренним злоумышленником или обнаружением факта маскировки в прошлом (как внутренним, так и внешним злоумышленником);
- использованием дефектов программного обеспечения ИСПДН внутренним злоумышленником или обнаружением факта их использования в прошлом (как внутренним, так и внешним злоумышленником);
- использованием программных закладок внутренним злоумышленником или обнаружением факта их использования в прошлом (как внутренним, так и внешним злоумышленником);
- хищением носителя защищаемой информации.

Комиссия, дополнительно к общему порядку действий (в соответствии с разделом 3), должна:

- если это возможно, определить организации, в которые произошла утечка конфиденциальной информации;
- определить возможные контрмеры, призванные уменьшить потери от утечки информации.

3. Несанкционированное копирование или изменение конфиденциальной информации в текущий момент времени со стороны лиц, имеющих право доступа к ней

В случае обнаружения злоумышленника неправомерно копирующего, либо изменяющего защищаемую информацию выполняются следующие действия.

Первоочередные действия:

1. Инженер-программист Учреждения прерывает несанкционированный процесс.
2. Инженер-программист Учреждения блокирует доступ к ИСПДн Учреждения для злоумышленника.

3. Инженер-программист Учреждения совместно с ответственным за обеспечение безопасности ПДн Учреждения удаляют нарушителя от средств ИСПДн.
4. Ответственным за обеспечение безопасности ПДн совместно с инженером-программистом предпринимаются действия по сбору и обеспечению сохранности улик.

Последующие действия:

Создается комиссия для расследования инцидента.

Подключение технических средств к системам и средствам ИСПДН в текущий момент времени

В случае обнаружения злоумышленника, производящего подключение к техническим средствам и системам ИСПДН в текущий момент времени, выполняются следующие действия.

Первоочередные действия:

- специалисты Учреждения прерывают процесс работы нарушителя.
- В случае если нарушитель – пользователь ИСПДн, специалисты Учреждения блокируют доступ в ИСПДн Учреждения для нарушителя.

Последующие действия:

- Создается комиссия для расследования инцидента.

Установка закладочных устройств злоумышленником в текущий момент времени

В случае обнаружения злоумышленника, устанавливающего закладочные устройства, выполняются следующие действия.

Первоочередные действия:

- специалисты Учреждения принимают меры к задержанию злоумышленника.

Последующие действия:

- Создается комиссия для расследования инцидента.

Маскировка под зарегистрированного пользователя, внешним злоумышленником в текущий момент времени

В случае обнаружения внешнего злоумышленника маскирующегося под зарегистрированного пользователя выполняются следующие действия.

Первоочередные действия:

- специалисты Учреждения блокируют доступ к ИСПДн Учреждения для злоумышленника.

Последующие действия:

- Создается комиссия для расследования инцидента.

Использование дефектов программного обеспечения ИСПДН внешним нарушителем в текущий момент времени

В случае обнаружения использования дефектов программного обеспечения ИСПДН внешним нарушителем в текущий момент времени выполняются следующие действия.

Первоочередные действия:

- специалисты Учреждения блокируют доступ из внешних сетей к оборудованию, на котором используется уязвимое ПО.

Последующие действия:

- Создается комиссия для расследования инцидента.

Использование программных закладок внешним нарушителем в текущий момент времени

В случае обнаружения использования программных закладок внешним нарушителем в текущий момент времени выполняются следующие действия.

Первоочередные действия:

- специалисты Учреждения блокируют доступ из внешних сетей к оборудованию, на котором установлена программная закладка.

Последующие действия:

- специалисты Учреждения определяют возможный ущерб, нанесенный программной закладкой.
- специалисты Учреждения проводят мероприятия по обнаружению внедренных программных закладок и их нейтрализации, планируют и организуют мероприятия по предотвращению повторения, нейтрализации последствий инцидента.
- Составляется акт об инциденте.

Обнаружение программных вирусов

В случае обнаружения программных вирусов выполняются действия, предусмотренные Инструкцией по антивирусной защите.

Нарушение функционирования ТС обработки информации в текущий момент времени злоумышленником

В случае обнаружения злоумышленника нарушающего функционирование ТС обработки информации в текущий момент времени выполняются следующие действия.

Первоочередные действия:

- специалисты Учреждения принимают меры по немедленному удалению злоумышленника от средств вычислительной техники.

- В случае если злоумышленник является пользователем системы, специалисты Учреждения блокируют доступ к ИСПДн Учреждения для злоумышленника.

Последующие действия:

- В случае наличия повреждений специалисты Учреждения определяют ущерб, нанесенный ТС и информации.
- специалисты Учреждения производят восстановление работоспособности системы.
- Создается комиссия для расследования инцидента.

Обнаружение нарушения функционирования ТС обработки информации, произведенного злоумышленником

В случае обнаружения нарушений в функционировании ТС обработки информации, выполняются следующие действия.

1. Специалисты Учреждения определяют возможный круг лиц, причастных к нарушению функционирования ТС, определяет объем повреждений техническим и информационным ресурсам.
2. Специалисты Учреждения производят восстановление работоспособности системы.
3. Создается комиссия для расследования инцидента.

Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку внешним злоумышленником в текущий момент времени

В случае обнаружения внешней атаки, направленной на блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку в текущий момент времени, выполняются следующие действия.

Первоочередные действия:

- Специалисты Учреждения выявляют источник ложных заявок.
- Специалисты Учреждения вырабатывают решение по блокированию потока ложных заявок и реализуют выбранное решение.

Последующие действия:

- Специалисты Учреждения уведомляют провайдера, от которого идут ложные заявки, планируют и организуют мероприятия по предотвращению повторения, нейтрализации последствий инцидента.
- Специалисты Учреждения составляют акт об инциденте.

Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку внутренним злоумышленником в текущий момент времени

В случае обнаружения внутренней атаки, направленной на блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку в текущий момент времени, выполняются следующие действия:
- Специалисты Учреждения выявляют источник ложных заявок и блокирует доступ к ИСПДн Учреждения для злоумышленника.
- Создается комиссия для расследования инцидента.

Блокировка доступа к защищаемой информации, произошедшая в прошлом

При обнаружении факта блокировки доступа к защищаемой информации, произошедшей в прошлом, выполняются следующие действия:
- Специалисты Учреждения выявляют источник ложных заявок.
- В случае если злоумышленник является внешним, специалисты Учреждения уведомляют провайдера, от которого идут ложные заявки. Планируют и организуют мероприятия по предотвращению повторения, нейтрализации последствий инцидента.
- В случае если злоумышленник является внешним, специалисты Учреждения составляют акт об инциденте.
- Создается комиссия для расследования инцидента.

Ошибки пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие утерю или повреждение защищаемой информации

В случае обнаружения ошибок пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие утерю или повреждение защищаемой информации, выполняются следующие действия.
Первоочередные действия:
- Специалисты Учреждения проводят анализ и идентификацию причин инцидента.
- В случае возможности злоумышленных действий выполняется последовательность действий, предусмотренная в соответствующем разделе Инструкции.
- Специалисты Учреждения определяют ущерб, нанесенный нештатной ситуацией.
- Специалисты Учреждения проводят мероприятия по восстановлению работоспособности системы и информации.
Последующие действия:
- Проводится проверка знаний сотрудника, виновного в инциденте, а в случае необходимости его обучение.

- Специалисты Учреждения составляют акт об инциденте, в случае необходимости выносит предложение директору о применении дисциплинарных мер в отношении нарушителя.

Ошибки пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие нарушение работоспособности ТС и ПО

В случае обнаружения ошибок пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие нарушение работоспособности ТС и ПО, выполняются следующие действия.

Первоочередные действия:

- Специалисты Учреждения проводят анализ и идентификацию причин инцидента.
- В случае возможности злоумышленных действий выполняется последовательность действий, предусмотренная в соответствующем разделе Инструкции.

Последующие действия:

- Специалисты Учреждения определяют ущерб, нанесенный нештатной ситуацией, восстанавливают работоспособность системы.
- Специалисты Учреждения составляют акт об инциденте, в случае необходимости выносит предложение директору о применении дисциплинарных мер в отношении нарушителя.
- Проводится проверка знаний сотрудника виновного в инциденте, а в случае необходимости его обучение.

Дефекты, сбои, отказы, аварии ТС, программных средств и систем ИСПДн

В случае возникновения дефектов, сбоев, отказов, аварий ТС и систем ИСПДН выполняются следующие действия.

Первоочередные действия:

- Специалисты Учреждения выявляют возможные причины проявления дестабилизирующих факторов.
- В случае наличия злоумышленных действий, выполняется порядок действий соответствующего раздела Инструкции.

Последующие действия:

- Специалисты Учреждения восстанавливает работоспособность систем.
- В случае потери данных специалистами Учреждения по возможности проводится восстановление их из резервных копий.
- Специалистами Учреждения производится составление акта.

Сбои, отказы и аварии систем обеспечения ИСПДН

В случае сбоев, отказов и аварий систем электроснабжения, вентиляции, других обеспечивающих инженерных систем выполняется следующая последовательность действий:
- В случае если наблюдается продолжительное отключение электропитания. специалистами Учреждения производится отключение серверов до момента истечения резервов системы бесперебойного питания.
- Ответственным за материально-техническое обеспечение организуются работы по максимально быстрому восстановлению систем обеспечения.
- В случае потери защищаемых данных специалистами Учреждения по возможности проводится восстановление их из резервных копий.
- Ответственным за материально-техническое обеспечение производится составление акта.

Природные явления, стихийные бедствия, несущие угрозу жизни человека

В случае проявления стихийных бедствий и природных явлений, которые несут угрозу жизни человека, выполняются следующие действия:
1. Все сотрудники (руководители подразделений, в том числе) обязаны личные реквизиты защиты (например: металлические и/или электронные ключи, карты-идентификаторы, ключевые дискеты, печати и пр.) собрать и упаковать в водонепроницаемый пакет (непосредственный руководитель обеспечивает заранее) и лично обеспечивать сохранность этого пакета во время эвакуации.
2. По заранее разработанному и постоянно хранятся на рабочем месте «Списку имущества и документов, подлежащего эвакуации в первую очередь»(2 экз.), произвести сбор документов и технических средств в водонепроницаемую тару (обеспечивает заранее непосредственный руководитель). Упакованное имущество сотрудник передает под роспись (на своем экз. описи) лицам, обеспечивающим доставку имущества на эвакопункт, иначе - лично сопровождает груз во время его транспортировки.
3. Сотрудник вкладывает в вышеназванный пакет картонную табличку с указанием текущей даты, своих персональных данных (ФИО, наименование Учреждения, номер служебного телефона) и содержащую опись содержимого пакета, заверенную собственноручной подписью.
Руководители подразделений обязаны собрать в помещениях подразделения и лично упаковать, реквизиты защиты и документы согласно спискам первой очереди, сотрудников своего подразделения, отсутствующих на момент эвакуации на рабочих местах (болезнь, командировка, учеба, отпуск и т.д.).
Руководители обязаны:
- при подготовке к эвакуации проверить обеспеченность (а при отсутствии – обеспечить) сотрудников подразделения и/или администраторов упаковочным материалом, списками документов, дел и имущества, подлежащих эвакуации в первую очередь;

- перед выездом в эвакопункт – проконтролировать исполнение задач эвакуации, приняв соответствующие доклады от сотрудников о готовности к эвакуации, провести выборочную проверку готовности (комплектности) документов, дел, имущества подразделения и/или ИСПДн к эвакуации.

Природные явления, стихийные бедствия, не несущие угрозу жизни человека

В случае проявления стихийных бедствий и природных явлений, которые не несут угрозу жизни и/или человека, выполняются следующие действия:

1. Сотрудники Учреждения выключают свои персональные компьютеры.
2. Специалисты Учреждения выключают серверы и сетевое оборудование.
3. Специалисты Учреждения принимают меры к эвакуации резервных копий с информацией, системных блоков компьютеров, содержащих особо ценную информацию, документов и другого имущества. В первую очередь эвакуируется имущество по «Списку имущества и(или) документов в личном пользовании сотрудника, подлежащего эвакуации в первую очередь».
4. В случае локальных пожаров и частичных затоплений, лицом, ответственным за материально-техническое обеспечение организуются работы по ликвидации нештатной ситуации и ее последствий.

4. Проведение расследований

Для расследования опасных ситуаций в случаях, предусмотренных настоящей Инструкцией может создаваться комиссия. В состав комиссии должны входить:

- председатель;
- ответственный за обеспечение безопасности ПДн;
- инженер-программист;
- юрист;
- другие лица по решению председателя комиссии.

Деятельность комиссии должна по возможности происходить в режиме конфиденциальности.

Комиссия проводит:

- анализ и идентификацию причин инцидента, определение виновных;
- определение ущерба, нанесенного нештатной ситуацией;
- планирование мер для предотвращения повторения, нейтрализации последствий (если это возможно);
- анализ и сохранение доказательств, следов инцидента, улик и свидетельств;
- определение мер воздействия на виновного;

- взаимодействие, при необходимости, с правоохранительными органами.

При сохранении улик, если есть возможность, инженером – программистом или специалистами производится резервное копирование системной и защищаемой информации технических средств, вовлеченных в инцидент, включая логи (контрольные записи).

По результатам деятельности комиссии составляется акт с описанием ситуации. К акту прилагаются поясняющие материалы (копии экрана, распечатки журнала событий, и др.).

По результатам расследования инженером - программистом организуются мероприятия по реализации предложенных комиссией мер для предотвращения либо уменьшения вероятности проявления, подобных инцидентов в дальнейшем.

При проведении расследований, кроме того, необходимо ответить на следующие вопросы:

- можно ли было предупредить нештатную ситуацию?
- вызвана ли она слабостью средств защиты и регистрации?
- это первая кризисная ситуация такого рода?
- достаточно ли имеющегося резерва?
- есть ли необходимость пересмотра системы защиты?
- есть ли необходимость пересмотра настоящей инструкции?

5. Ответственные за контроль выполнения инструкции

Ответственными за постоянный контроль выполнения требований данной Инструкции являются:

- инженер – программист, а так же специалисты Учреждения в части задач, возложенных на них настоящей инструкцией;
- ответственный за обеспечение безопасности ПДн в части общего контроля информационной безопасности;
- ответственный за материально-техническое обеспечение, в части задач, возложенных на него настоящей инструкцией.

6. Порядок пересмотра инструкции

Инструкция подлежит полному пересмотру при изменении приоритетов угроз безопасности ИСПДн Учреждения. Кроме того, полный плановый пересмотр данного документа проводится регулярно, не реже одного раза в год, с целью проверки соответствия положений данного документа реальным условиям применения их в ИСПДн Учреждения.

Инструкция подлежит частичному пересмотру в следующих случаях:

- Изменений местоположения, состава и объема информационных ресурсов, подлежащих резервному копированию;

- Определении такой необходимости в выводах комиссии по результатам расследования нештатной ситуации;
- Необходимости повышения эффективности мероприятий, определенных в настоящей инструкции;
- Изменения состава, обязанностей и полномочий должностных лиц Учреждения, которые задействованы в мероприятиях настоящей Инструкции.

Полный пересмотр данного документа проводится ответственным за обеспечение безопасности ПДн Учреждения и инженером - программистом, с целью проверки соответствия определенных данным документом мер защиты реальным условиям применения их в ИСПДн Учреждения.

Частичный пересмотр данного документа проводится инженером - программистом. Частичный пересмотр должен проводиться регулярно, не реже одного раза в полгода. При этом могут быть добавлены, удалены или изменены приложения Инструкции с обязательным указанием оснований и внесенных изменений в «Листе регистрации изменений в Инструкции» (Приложение 4) без переутверждения всей Инструкции.

Приложение 5
к приказу от 30 декабря 2016 года № 95

Перечень
мест хранения материальных носителей персональных данных

№ п/п	Место хранения	Виды материального носителя персональных данных
1	Сейф №1 в кабинете директора	Трудовые книжки, журналы регистрации трудовых книжек, трудовых договоров
2	Сейф №2 в кабинете секретаря	Личные дела работников МКУ ДО «ЦДО», документы по воинскому учету, карточки Т2, журнал регистрации личных дел.

Приложение 6
к приказу от 30 декабря 2016 года №95

ИНСТРУКЦИЯ
по установке, модификации и обслуживанию программного обеспечения и техническому обслуживанию аппаратных средств информационных систем персональных данных в МКУ ДО «ЦДО»

1. Общие положения.

Инструкция по установке, модификации и обслуживанию программного обеспечения и техническому обслуживанию аппаратных средств информационных систем персональных данных (ИСПДн) муниципального казенного учреждения дополнительного образования «Центр дополнительного образования» (далее – Учреждение), включает в себя описание полного комплекса организационно-технических мер по проведению работ по данной тематике.

Требования настоящей Инструкции распространяются на всех должностных лиц и сотрудников подразделений Учреждения, использующих в работе ИСПДн, в которых осуществляется обработка информации ограниченного доступа, не составляющей государственной тайны.

Должностные лица Учреждения, задействованные в обеспечении функционирования ИСПДн, знакомятся с основными положениями и приложениями Инструкции в части, их касающейся, по мере необходимости.

Ознакомление с требованиями Инструкции пользователей ИСПДн осуществляется инженером-программистом , и специалистами Учреждения под роспись с выдачей электронных копий соответствующих приложений и разделов Инструкции непосредственно для повседневного использования в работе.

Непосредственное исполнение настоящей Инструкции определяется инженером-программистом, и специалистами Учреждения по согласованию с ответственным за обеспечение безопасности персональных данных (ПДн) Учреждения.

2.Порядок проведения работ

Все изменения конфигурации автоматизированных рабочих мест и состава программного обеспечения средств вычислительной техники Учреждения не аттестованных по требованиям безопасности персональных данных, производиться на основании обоснованных заявок руководителей структурных подразделений Учреждения, согласованных с директором. Производственная необходимость проведения указанных в заявке изменений подтверждается подписью руководителя структурного подразделения.

Те же действия, но в отношении аттестованных по требования безопасности персональных данных АРМ, дополнительно согласовываются с ответственным за безопасность информации Учреждения. Указанное должностное лицо, определяет необходимость повторной процедуры аттестации ИСПДн, о чем извещает директора.

Все изменения конфигурации технических средств рабочих станций и серверов, входящих в состав аттестованных по требованиям безопасности ИСПДн Учреждения, отражаются в Техническом паспорте объекта информатизации.

ЗАПРЕЩАЕТСЯ изменение состава (в том числе ввод новых) программных средств, осуществляющих обработку ПДн на объектах информатизации, аттестованных по требованиям безопасности информации.

После согласования заявка передается ответственному за обеспечение безопасности ПДн для исполнения работ по внесению изменений в конфигурацию конкретного АРМ Учреждения.

Право внесения изменений в конфигурацию аппаратно-программных средств рабочих станций ИСПДн Учреждения предоставляется ответственному за обеспечение безопасности ПДн. Изменение конфигурации аппаратно-программных средств рабочих станций и серверов кем-либо, кроме ответственного за обеспечение безопасности ПДн, ЗАПРЕЩЕНО.

Установка и настройка программного средства осуществляется ответственным за обеспечение безопасности ПДн согласно эксплуатационной документации.

Запрещается установка и использование на ПЭВМ (серверах) любого программного обеспечения (ПО), не входящего в перечень программного обеспечения, разрешенного к использованию в Учреждении.

Руководители структурных подразделений осуществляют контроль за отсутствием на ПЭВМ сотрудников подразделения программного обеспечения и данных, не связанных с выполнением должностных обязанностей.

Установка (обновление) ПО (системного, тестового и т.п.) на рабочих станциях и серверах производится с эталонных копий программных средств, хранящихся у инженера-программиста. Все добавляемые программные и аппаратные компоненты должны быть предварительно проверены на работоспособность, а также отсутствие вредоносного программного кода в соответствии с «Инструкцией по организации антивирусной защиты ИСПДнГУП в Учреждении».

После установки (обновления) программного обеспечения инженер-программист, должен произвести настройку средств управления доступом к компонентам данной задачи (программного средства) в соответствии с требованиями к системе защиты информации и, совместно с пользователем АРМ проверить правильность настройки средств защиты.

В случае обнаружения не декларированных (не описанных в документации) возможностей программного средства, сотрудники немедленно докладывают руководителю. В этом случае использование

программного средства до получения специальных указаний ЗАПРЕЩАЕТСЯ.

После завершения работ по внесению изменений в состав аппаратных средств защищенных ПЭВМ системный блок должен быть опечатан (опломбирован, защищен специальной наклейкой) ответственным за обеспечение безопасности ПДн. При изъятии ПЭВМ из состава рабочих станций, обрабатывающих информацию ограниченного распространения (защищаемая информация), ее передача на склад, в ремонт или в другое подразделение для решения иных задач осуществляется только после того, как ответственный за обеспечение безопасности ПДн снимет с данной ПЭВМ средства защиты и предпримет необходимые меры для затирания (уничтожения) защищаемой информации, которая хранилась на дисках компьютера. Факт уничтожения данных, находившихся на диске компьютера, оформляется актом за подписью ответственного за обеспечение безопасности ПДн.

Оригиналы заявок (документов), на основании которых производились изменения в составе технических или программных средств ПЭВМ с отметками о внесении изменений в состав аппаратно-программных средств должны храниться у ответственного за обеспечение безопасности ПДн.

3.Порядок пересмотра инструкции

Инструкция подлежит полному пересмотру при изменении перечня решаемых задач, состава технических и программных средств ИСПДн Учреждения, приводящих к существенным изменениям технологии обработки информации.

Инструкция подлежит частичному пересмотру в остальных случаях. Частичный пересмотр проводится ответственным за обеспечение безопасности ПДн Учреждения.

Полный пересмотр данного документа проводится ответственным за обеспечение безопасности ПДн Учреждения с целью проверки соответствия положений данного документа реальным условиям применения их в ИСПДн Учреждения.

Вносимые изменения не должны противоречить другим положениям Инструкции.

4.Ответственные за организацию и контроль выполнения инструкции

Ответственность за соблюдение требований настоящей Инструкции пользователями возлагается на всех сотрудников Учреждения.

Ответственность за организацию контрольных и проверочных мероприятий по вопросам установки, модификации технических и программных средств возлагается на ответственного за обеспечение безопасности ПДн и специалистов Учреждения.

Ответственность за общий контроль информационной безопасности возлагается на ответственного за обеспечение безопасности ПДн Учреждения.

Приложение 7
к приказу от 30 декабря 2016 года №95

ИНСТРУКЦИЯ
пользователя информационной системы персональных данных
МКУ ДО «ЦДО»

1. Общие положения

1.1. Пользователь ИСПДн (далее – Пользователь) осуществляет обработку персональных данных в информационной системе персональных данных.

1.2. Пользователем является каждый сотрудник Учреждения, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты.

1.3. Пользователь несет персональную ответственность за свои действия.

1.4. Пользователь в своей работе руководствуется настоящей инструкцией, Концепцией и Политикой информационной безопасности, руководящими и нормативными документами ФСТЭК России и регламентирующими документами Учреждения.

1.5. Методическое руководство работой пользователя осуществляется ответственным за обеспечение защиты персональных данных.

2. Должностные обязанности

Пользователь обязан:

2.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

2.2. Выполнять на автоматизированном рабочем месте (АРМ) только те процедуры, которые определены для него в Положении о разграничении прав доступа к обрабатываемым персональным данным.

2.3. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов.

2.4. Соблюдать требования парольной политики (раздел 3).

2.5. Соблюдать правила при работе в сетях общего доступа и (или) международного обмена – Интернет и других (раздел 4).

2.6. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

2.7. Для получения консультаций по вопросам работы и настройке элементов ИСПДн необходимо обращаться к Администратору ИСПДн.

2.8. Пользователям запрещается:

Разглашать защищаемую информацию третьим лицам.

Копировать защищаемую информацию на внешние носители без разрешения своего руководителя.

Самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств.

Несанкционированно открывать общий доступ к папкам на своей рабочей станции.

Запрещено подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства.

Отключать (блокировать) средства защиты информации.

Обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн.

Сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн.

Привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение защиты персональных данных.

2.10. При отсутствии визуального контроля за рабочей станцией: доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>

2.11. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в рамках возложенных, в пределах возложенных на него функций.

3. Организация парольной защиты

3.1 Личные пароли доступа к элементам ИСПДн выдаются пользователям Администратором информационной безопасности, Администратором ИСПДн или создаются самостоятельно.

3.2. Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 3 месяца.

3.3. Правила формирования пароля:

Пароль не может содержать имя учетной записи пользователя или какую-либо его часть.

Пароль должен состоять не менее чем из 8 символов.

В пароле должны присутствовать символы трех категорий из числа следующих четырех:

а) прописные буквы английского алфавита от A до Z;

б) строчные буквы английского алфавита от a до z;

в) десятичные цифры (от 0 до 9);

г) символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #, %).

Запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а так же имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе.

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

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

Запрещается выбирать пароли, которые уже использовались ранее.

3.4. Правила ввода пароля:

Ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан.

Во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

3.5. Правила хранение пароля:

Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах.

Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

3.6. Лица, использующие паролирование, обязаны:

четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по паролированию.

своевременно сообщать Администратору информационной безопасности об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

4. Правила работы в сетях общего доступа и (или) международного обмена

4.1. Работа в сетях общего доступа и (или) международного обмена (сети Интернет и других) (далее – Сеть) на элементах ИСПДн, должна проводиться при служебной необходимости.

4.2. При работе в Сети запрещается:

Осуществлять работу при отключенных средствах защиты (антивирус и других).

Передавать по Сети защищаемую информацию без использования средств шифрования.

Запрещается скачивать из Сети программное обеспечение и другие файлы.

Запрещается посещение сайтов сомнительной репутации (порно-сайты, сайты содержащие нелегально распространяемое ПО и другие).

Запрещается нецелевое использование подключения к Сети.