Муниципальное бюджетное учреждение дополнительного образования "Центр детского творчества №2" г. Барнаула

ПРИКАЗ

«07» 10 2019 года № 93/1

Об утверждении документов, касающихся
обработки конфиденциальной информации

В целях выполнения «Специальных требований и рекомендаций по технической защите информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30 августа 2002 года № 282 и проведения аттестации автоматизированных систем, обрабатывающих конфиденциальную информацию, приказываю:

1. Утвердить Перечень защищаемых ресурсов в автоматизированных системах МБУ ДО "ЦДТ №2" г. Барнаула (Приложение №1);
2. Утвердить Список постоянных пользователей автоматизированного рабочего места для связи в ПФДО и установленные им права к информационным и техническим ресурсам. Матрица доступа (Приложение №2);
3. Утвердить Описание технологического процесса обработки информации на объекте информатизации «Автоматизированное рабочее место для обработки конфиденциальной информации» МБУ ДО "ЦДТ №2" г. Барнаула (Приложение №3);
4. Утвердить Инструкцию администратора информационной безопасности автоматизированной системы МБУ ДО "ЦДТ №2" г. Барнаула (Приложение № 4);
5. Утвердить Инструкцию по организации парольной защиты в МБУ ДО "ЦДТ №2" г. Барнаула (Приложение №5);
6. Утвердить Инструкцию по проведению антивирусного контроля в автоматизированной системе МБУ ДО "ЦДТ №2" г. Барнаула (Приложение №6);
7. Утвердить Инструкцию по работе пользователя автоматизированной системы МБУ ДО "ЦДТ №2" г. Барнаула (Приложение №7);
8. Утвердить План размещения основных и вспомогательных технических средств и систем в кабинете №7 (Приложение №8);
9. Утвердить План контролируемой зоны предприятия (Приложение №9);
10. Контроль за выполнением настоящего приказа оставляю за Администратором информационной безопасности.

Директор С.В. Панова

Приложение № 1 к приказу «Об утверждении документов, касающихся обработки конфиденциальной информации»
от «07» 10 2019 г № 93/1

Перечень защищаемых информационных ресурсов в автоматизированных системах
МБУ ДО "ЦДТ №2" г. Барнаула

Автоматизированная система МБУ ДО "ЦДТ №2" г. Барнаула

№ п/п	Название ресурса	Путь к ресурсу (место хранения)	Гриф	Группы пользователей имеющих доступ к ресурсу (права доступа)	Состав обрабатываемой информации	Количество субъектов персональных данных	Категория	Принадлежность
1	2	3	4	5	6	7	8	9
1	**ПФДО** (Персонифицированное дополнительное образование)	Кабинет хранилище	Конфиденциально	Администратор ИБ, Администратор АС, Пользователь	фамилия, имя, отчество, дата рождения, гражданство, место рождения, пол, адрес регистрации, наименование документа удостоверяющего личность, серия, номер, кем и когда выдан, номер телефона	менее 100 000	иные	Учащиеся

Приложение №2 к приказу «Об утверждении документов, касающихся обработки конфиденциальной информации»
от «07» 10 2019 г. №93/1

Муниципальное бюджетное учреждение дополнительного образования "Центр детского творчества №2" г. Барнаула

**Список постоянных пользователей автоматизированного рабочего места для связи в ПФДО
и установленные им права к информационным и техническим ресурсам.
Матрица доступа.**

Список постоянных пользователей автоматизированного рабочего места для связи в ПФДО и установленные им права к информационным и техническим ресурсам:

№ п/п	ФИО	Должность	Группа
1	Илюшина Ирина Александровна	Методист	Администратор ИБ
2	Илюшина Ирина Александровна	Методист	Пользователь ПФДО

Приложение №2 к приказу «Об утверждении документов, касающихся обработки конфиденциальной информации»
от «__» _____ 20__ г. №___

Матрица доступа к защищаемым ресурсам:

Группа	Ресурс	Место хранения	Полный доступ	Настройка	Изменение	Выполнение	Чтение	Запись
Администратор ИБ	Аппаратное обеспечение, программное обеспечение, ОС, СЗИ, СКЗИ,	Автоматизированное рабочее место для связи с ПФДО, кабинет хранилище	+	+	+	+	+	+
Администратор ИБ	ПФДО	Автоматизированное рабочее место для связи с ПФДО, кабинет хранилище	-	+	-	+	+	+
Пользователь ПФДО	ПФДО	Автоматизированное рабочее место для связи с ПФДО, кабинет хранилище	-	-	-	+	+	+

Приложение №3 к приказу «Об утверждении документов, касающихся обработки конфиденциальной информации»
от «07» 10 2019 г. №93/1

Описание технологического процесса обработки информации на объекте информатизации «Автоматизированное рабочее место для обработки конфиденциальной информации»

1. Общие сведения

Автоматизированное рабочее место (АРМ) для обработки конфиденциальной информации предназначено для обработки, хранения информации с высшим грифом «конфиденциально», при этом информация может поступать с других объектов информатизации, из сторонних организаций на usb-флеш-накопителях и через защищенные каналы передачи информации.

Субъектами доступа на АРМ является персонал, имеющий право обрабатывать информацию на основании разрешительной системы доступа персонала к защищаемым ресурсам АРМ.

Технологический процесс автоматизированной обработки защищаемой информации должен отвечать необходимому уровню безопасности в МБУ ДО "ЦДТ №2" г. Барнаула.

1.1 Основные задачи технологического процесса

Основными задачами технологического процесса являются:

– разграничение прав доступа пользователей к защищаемым информационным ресурсам автоматизированной системы;

– работа с файлами документов ограниченного доступа: создание документов, внесение корректировок в документы, размножение, уничтожение, хранение файлов;

– обеспечение сохранности защищаемых информационных ресурсов автоматизированной системы (резервное копирование и восстановление, антивирусная защита, обеспечение целостности);

– обеспечение безопасности информации при взаимодействии с сетями международного информационного обмена;

– обеспечение безопасности информации при ее размещении на съёмных внешних машинных носителях информации.

1.2 Используемые программные средства

Для осуществления технологического процесса обработки информации на АРМ используется ПО, представленное в таблице 1.

Приложение №3 к приказу «Об утверждении документов, касающихся обработки конфиденциальной информации»
от «07» 10 2013 г. №931

Таблица 1 – Список программного обеспечения

№ п/п	Наименование ПО	Классификация ПО
1.	2007 Microsoft Office Suite Service Pack 2 (SP2)	Офисное приложение
2.	7-Zip 9.20	Архиватор
3.	Adobe AIR	Кроссплатформенная среда
4.	Adobe Community Help	Помощник Adobe
5.	Adobe Community Help	Помощник Adobe
6.	Adobe Flash Player 32 NPAPI	Программа для просмотра и редактирования PDF-файлов
7.	Adobe Flash Player 32 PPAPI	Программа для просмотра и редактирования PDF-файлов
8.	Adobe Reader XI (11.0.23) - Russian [Русский (Россия)]	Программа для просмотра и редактирования PDF-файлов
9.	Adobe Refresh Manager	Программа для просмотра и редактирования PDF-файлов
10.	Intel(R) Management Engine Components	Встроенное программное обеспечение
11.	Intel(R) OpenCL CPU Runtime	Встроенное программное обеспечение
12.	Intel(R) Processor Graphics	Встроенное программное обеспечение
13.	Intel(R) Rapid Storage Technology	Встроенное программное обеспечение
14.	Intel(R) USB 3.0 eXtensible Host Controller Driver	Встроенное программное обеспечение
15.	Intel® Trusted Connect Service Client	Встроенное программное обеспечение
16.	K-Lite Mega Codec Pack 10.8.5	Универсальный набор кодеков и утилит для просмотра и обработки аудио- и видеофайлов
17.	Mozilla Firefox	Браузер
18.	Microsoft .NET Framework 4.6.1	Программа для создания приложений
19.	Microsoft Edge Update	Браузер
20.	Microsoft Edge	Браузер
21.	Microsoft Office Профессиональный плюс 2007	Офисное приложение
22.	Microsoft OneDrive	Облачное хранилище
23.	Microsoft Visual C++ 2010 x64 Redistributable - 10.0.30319	Компьютерная платформа
24.	Microsoft Visual C++ 2010 x86 Redistributable - 10.0.30319	Компьютерная платформа
25.	PxMergeModule	Встроенный драйвер
26.	Realtek Ethernet Controller Driver [Русский]	Встроенный драйвер

№ п/п	Наименование ПО	Классификация ПО
27.	Realtek High Definition Audio Driver [Русский]	Встроенный драйвер
28.	Realtek USB 2.0 Card Reader	Встроенный драйвер
29.	REALTEK Wireless LAN Driver [Русский]	Встроенный драйвер
30.	Synaptics Pointing Device Driver	Встроенный драйвер
31.	WinFlash	Фирменная утилита
32.	Yandex	Браузер
33.	Архиватор WinRAR	Архиватор
34.	СБИС3 Плагин [Русский (Россия)]	Декстоп-приложение

АРМ предназначено для работы в многопользовательском режиме, доступ исполнителей к работе осуществляется в соответствии с установленной разграничительной системой доступа, пользователи имеют разные права доступа к информации.

1.3 Защищаемые информационные ресурсы

Объектами доступа АС является сама АС в целом, в том числе:

– Несъемные МНИ (НЖМД) с информацией ограниченного доступа;

– Съёмные МНИ (usb-флэш-накопители) с информацией ограниченного доступа;

– Монитор АРМ с отображаемой на нем информацией ограниченного доступа;

– Оперативная память АРМ с информацией ограниченного доступа.

К информации ограниченного доступа (электронный вид) относятся:

– Исполняемые файлы программ, участвующие в процессе обработки информации ограниченного доступа, размещенные на базовом логическом диске «С» несъёмного жёсткого магнитного диска системного блока АС (операционная система; программы, предназначенные для разработки документов ограниченного доступа; программные средства, осуществляющие функции защиты информации, контроля и безопасности);

– Каталоги и файлы, размещенные на внешних машинных носителях информации.

1.4 Источники данных

Источниками данных являются:

– Данные, вводимые с помощью устройств ввода автоматизированной системы;

– Файлы документов и данных на съемных машинных носителях (usb-флеш-накопители).

1.5 Персонал АС

К работе на АРМ допущены следующие категории персонала:

– Кадровый состав МБУ ДО "ЦДТ №2" г. Барнаула, согласно приказу (утвержденному списку);

– Администратор информационной безопасности автоматизированной системы.

1.6 Доступ к информационным ресурсам

Пользователи имеют право постоянного хранения файлов с защищаемыми данными на жестких магнитных дисках в специально выделенных Администратором каталогах. Для хранения файлов с конфиденциальными данными могут также использоваться учтенные установленным порядком машинные носители информации.

Удаленные файлы, а также временные файлы на магнитных носителях уничтожаются специальной программой для очистки областей памяти на магнитных носителях информации, входящей в состав установленной на АРМ СЗИ от НСД Secret Net Studio 8.

Доступ к информационным ресурсам АРМ осуществляется по персональному паролю конкретного пользователя при этом пользователь получает установленные Администратором АРМ права доступа к устройствам, каталогам, файлам и программам.

2. Обработка информации

АРМ является автоматизированной системой, имеющей подключение к информационно-телекоммуникационным сетям международного информационного обмена.

АС реализовано как автоматизированное рабочее место, включающее ПЭВМ, функционирующий под управлением ОС с установленными СЗИ от НСД Secret Net Studio 8 и ПК ViPNet Client 4 (КС2).

2.1 Начало сеанса работы

После включения ПЭВМ при загрузке операционной системы выполняется контроль целостности исполняемых файлов СЗИ от НСД, происходит процедура идентификации пользователя по идентификатору (имени пользователя), зарегистрированному в СЗИ от НСД Secret Net Studio 8. В процессе аутентификации пользователь использует свой пароль.

В случае успешного завершения контроля целостности пользователь получает доступ к замкнутой программной среде с персональными настройками доступа к защищаемым ресурсам и может:

– Обрабатывать информацию на АС;

– Размножать (копировать) информацию на заранее учтённые МНИ (при необходимости).

В случае нарушения контроля целостности файлов СЗИ от НСД на экран монитора выдается сообщение об ошибке, и рабочая станция блокируется.

Администратор информационной безопасности назначает пароль каждому пользователю АС. Требования к порядку организации, уровню сложности и процедуре смены паролей определены в инструкции по организации парольной защиты АС.

2.2 Обработка информации ограниченного доступа

Обработка информации ограниченного доступа производится при помощи прикладного программного обеспечения, установленного на ПЭВМ.

Информация вводится пользователем с устройств ввода или копируется на жесткий диск со съемных учетных машинных носителей информации (usb-флеш-накопители). По завершении работ с документами, файлы подготовленных документов сохраняются в каталогах логического диска «С» ПЭВМ или при необходимости готовые файлы записываются на зарегистрированный МНИ (usb-флеш-накопитель).

Условием, необходимым для выполнения процедуры уничтожения файла документа, являются наличие у пользователя соответствующих прав доступа.

Передача защищаемой информации по информационно-телекоммуникационным сетям международного обмена без использования специально предназначенных для этого средств защиты информации, в том числе шифровальных (криптографических) средств, прошедших в установленном законодательство Российской Федерации порядке сертификацию в Федеральной службе безопасности Российской Федерации и (или) получивших подтверждение соответствия в Федеральной службе по техническому и экспортному контролю, не допускается.

2.3 Работа с машинными носителями информации

Учёт МНИ осуществляется согласно требованиям конфиденциального делопроизводства. Учетный МНИ хранятся у администратора информационной безопасности (или ответственного за обработку персональных данных) в защищенном хранилище.

Выведение из обращения учтённых МНИ и их уничтожение осуществляются в соответствии с требованиями конфиденциального делопроизводства.

2.4 Завершение сеанса работы

Завершение работы пользователь АС производит выполнением процедуры завершения сеанса работы в ОС и выключает питание ПЭВМ.

По окончании обработки информации ограниченного доступа учтённые носители информации сдаются на хранение администратору информационной безопасности или ответственному за защиту конфиденциальной информации.

3. Обеспечение безопасности информации

Физическая защита АС, машинных носителей информации и средств защиты информации обеспечивается контролем допуска в помещение, где расположена АС обработки конфиденциальной информации.

Внутри кабинета , где расположена АС, установлены датчики дыма и извещатели пожарной сигнализации.

Доступ должностных лиц в помещение осуществляется в соответствии с утвержденным директором МБУ ДО "ЦДТ №2" г. Барнаула списком сотрудников, имеющих право на получение (сдачу) ключей от режимных помещений.

Доступ посетителей, обслуживающего персонала и представителей сторонних организаций в помещения МБУ ДО "ЦДТ №2" г. Барнаула осуществляется в присутствии представителей МБУ ДО "ЦДТ №2" г. Барнаула.

Для обеспечения безопасности информации ограниченного доступа, обрабатываемой на АС, применяется комплекс организационных мер:

Приказом директора МБУ ДО "ЦДТ №2" г. Барнаула назначаются:

- комиссия по классификации АС;
- администратор информационной безопасности АС.

Директором утверждается организационно-распорядительная документация, закрепляющая порядок доступа на объект информатизации, порядок обработки и защиты информации на АС.

На АС установлено СЗИ от НСД Secret Net Studio 8 и средство защиты информации ViPNet Client 4 (КС2).

Основные функции, реализуемые СЗИ от НСД Secret Net Studio 8:

– контроль входа пользователей в систему;
– разграничение доступа пользователей к устройствам компьютера;
– создание для пользователей ограниченной замкнутой среды программного обеспечения компьютера (замкнутой программной среды);
– разграничение доступа пользователей к конфиденциальным данным;
– контроль целостности защищаемых ресурсов;
– контроль подключения и изменения устройств компьютера;
– уничтожение (затирание) содержимого файлов при их удалении;
– регистрация событий безопасности в журнале.

Порядок работы с СЗИ определен соответствующими инструкциями.

Контроль функционирования системы защиты информации АС проводится администратором информационной безопасности. Основными средствами контроля является просмотр системного журнала ОС и просмотр журнала безопасности СЗИ от НСД Secret Net Studio 8.

4. Обеспечение сохранности информационных ресурсов

4.1 Резервное копирование

Средствами восстановления СЗИ и программной среды АС являются дистрибутивы ОС, прикладного программного обеспечения, СЗИ от НСД Secret Net Studio 8. Акты установки и настройки СЗИ.

МНИ с дистрибутивами СЗИ и дистрибутивами ПО хранятся в помещении, где расположена АС в специальном защищенном хранилище.

Резервное копирование файлов документов, размещённых на жестком магнитном диске ПЭВМ, производится администратором информационной безопасности АС на учтённые МНИ (usb-флеш-накопители) не реже одного раза в месяц, с внесением соответствующей записи в журнал учета резервных копий.

Учет и хранение МНИ с резервными копиями информации ограниченного доступа (файлов документов), осуществляется в соответствии с требованиями конфиденциального делопроизводства.

4.2 Восстановление информации

В случае сбоев работы ПЭВМ, которые привели к искажению или потере информации, восстановление информации производится администратором информационной безопасности АС с резервных копий.

Приложение №3 к приказу «Об утверждении документов, касающихся обработки конфиденциальной информации»
от «07» 10 2019 г. № 93/1

Перечень сокращений

АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
МНИ	Машинный носитель информации
НЖМД	Накопитель на жестких магнитных дисках
НСД	Несанкционированный доступ
ПК	Программный комплекс
ПО	Программное обеспечение
ПЭВМ	Персональная электронно-вычислительная машина
СЗИ	Средство защиты информации
СКЗИ	Средство криптографической защиты информации
ФСБ	Федеральная служба безопасности
ФСТЭК	Федеральная служба по техническому и экспортному контролю

Приложение №4 к приказу «Об утверждении документов, касающихся обработки конфиденциальной информации»
от «07» 10 2019 г. №93/1

ИНСТРУКЦИЯ АДМИНИСТРАТОРА

информационной безопасности автоматизированной системы
Муниципальное бюджетное учреждение дополнительного образования "Центр детского творчества №2" г. Барнаула

1. Общие положения

1.1. Инструкция Администратора информационной безопасности автоматизированной системы МБУ ДО "ЦДТ №2" г. Барнаула (далее – Инструкция) определяет функции, права и обязанности Администратора информационной безопасности автоматизированной системы (далее – Администратор ИБ) по вопросам обеспечения информационной безопасности при подготовке и исполнении документов в АС МБУ ДО "ЦДТ №2" г. Барнаула.

1.2. Администратор ИБ назначается из числа работников МБУ ДО "ЦДТ №2" г. Барнаула приказом руководителя и обеспечивает правильность использования и нормальное функционирование установленной системы защиты АС МБУ ДО "ЦДТ №2" г. Барнаула.

1.3. Настоящая Инструкция является дополнением к действующим нормативным документам по вопросам обеспечения режима конфиденциальности и не исключает обязательного выполнения их требований.

1.4. Администратор ИБ обладает правами доступа к любым программно-аппаратным средствам защиты информации (далее – СЗИ) на технических средствах пользователей. Он несет ответственность за реализацию принятой политики безопасности.

2. Должностные обязанности

2.1. Администратор ИБ обязан:

2.1.1. Осуществлять учет и периодический контроль за составом и полномочиями пользователей АС МБУ ДО "ЦДТ №2" г. Барнаула.

2.1.2. Осуществлять оперативный контроль за работой пользователей АС МБУ ДО "ЦДТ №2" г. Барнаула, анализировать содержимое системных журналов средств вычислительной техники (далее – СВТ) и адекватно реагировать на возникающие нештатные ситуации. Обеспечивать своевременное архивирование системных журналов СВТ и надлежащий режим хранения данных архивов.

2.1.3. Осуществлять непосредственное управление режимами работы и административную поддержку функционирования применяемых в АС МБУ ДО "ЦДТ №2" г. Барнаула СЗИ.

2.1.4. Присутствовать при внесении изменений в конфигурацию (модификации) аппаратно-программных средств защищенных СВТ, обеспечивать и контролировать установку и настройку СЗИ.

2.1.5. Не реже одного раза в месяц проверять состояние используемых СЗИ, осуществлять проверку правильности их настройки (выборочное тестирование).

2.1.6. Управлять учётными записями пользователей, реализовывать правила разграничения доступа, а также осуществлять контроль соблюдения этих правил.

2.1.7. Управлять идентификаторами (осуществлять создание, присвоение и уничтожение идентификаторов пользователей и устройств) и средствами аутентификации (аутентификационной информацией) внутренних пользователей в АС МБУ ДО "ЦДТ №2" г. Барнаула, обеспечивать соблюдение правил идентификации и аутентификации пользователей и устройств.

2.1.8. Осуществлять контроль за хранением, выдачей, инициализацией, блокированием средств аутентификации и принятием мер в случае утраты и (или) компрометации средств аутентификации.

2.1.9. Осуществлять контроль не реже одного раза в три месяца установленного (инсталлированного) в АС МБУ ДО "ЦДТ №2" г. Барнаула программного обеспечения.

2.1.10. Осуществлять мониторинг и контроль применения мобильных технических средств на предмет выявления несанкционированного использования мобильных технических средств для доступа к объектам доступа АС.

2.1.11. Настраивать параметры журналов регистрации событий безопасности.

2.1.12. Проводить мониторинг и анализ результатов регистрации событий безопасности и реагирование на них не реже одного раза в неделю.

2.1.13. Управлять средствами антивирусной защиты в соответствии с «Инструкцией по проведению антивирусного контроля в МБУ ДО "ЦДТ №2" г. Барнаула.

2.1.14. Осуществлять контроль уровня защищенности информации, обрабатываемой в АС МБУ ДО "ЦДТ №2" г. Барнаула.

2.1.15. Осуществлять контроль выполнения условий и сроков действия сертификатов соответствия на СЗИ и принятие мер, направленных на устранение выявленных недостатков.

2.1.16. Обеспечивать сохранность СЗИ, эксплуатационной и технической документации к СЗИ, а также порядок обращения с СЗИ в процессе получения, хранения, доставки, передачи, встраивания в прикладные системы, тестирования в целях защиты информации, обрабатываемой с использованием средств автоматизации.

2.1.17. Проводить не реже одного раза в три месяца контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей.

2.1.18. Своевременно и точно отражать изменения в организационно-распорядительных документах по управлению СЗИ, установленных на СВТ АС МБУ ДО "ЦДТ №2" г. Барнаула.

2.1.19. Осуществлять поэкземплярный учет в соответствующем журнале:

– СЗИ (носителей дистрибутивов, системных блоков с установленными СЗИ);
– эксплуатационной и технической документации к СЗИ.

2.1.20. Осуществлять хранение:

– носителей дистрибутивов СЗИ;
– лицензий и сертификатов на СЗИ.

2.1.21. Не реже одного раза в месяц осуществлять проверки:

– состояния защищенности информационных ресурсов от сбоев в системе электропитания (система резервирования и автоматического ввода резерва);

– состояния линейно-кабельного оборудования локально-вычислительных сетей (наличие запирающих и опечатывающих устройств, оборудования распределительных шкафов).

2.1.22. Проводить первоначальный, плановый и внеплановый инструктаж обслуживающего и эксплуатирующего персонала АС МБУ ДО "ЦДТ №2" г. Барнаула по вопросам работы с СЗИ.

2.1.23. Отвечать на вопросы обслуживающего и эксплуатирующего персонала ИС МБУ ДО "ЦДТ №2" г. Барнаула, связанные с работой СЗИ.

2.1.24. Составлять инструкции по работе с СЗИ.

2.1.25. Докладывать руководству МБУ ДО "ЦДТ №2" г. Барнаула об имевших место попытках несанкционированного доступа к информации и техническим средствам ИС.

2.1.26. Участвовать в выявлении инцидентов информационной безопасности и реагировании на них.

2.1.27. Управлять конфигурацией АС МБУ ДО "ЦДТ №2" г. Барнаула и их системой защиты информации.

В ходе управления конфигурацией АС МБУ ДО "ЦДТ №2" г. Барнаула и ее системы защиты информации осуществляются:

– поддержание конфигурации АС МБУ ДО "ЦДТ №2" г. Барнаула и их системы защиты информации (структуры системы защиты информации АС МБУ ДО "ЦДТ №2" г. Барнаула, состава, мест установки и параметров настройки средств защиты информации, программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на систему защиты информации (поддержание базовой конфигурации АС МБУ ДО "ЦДТ №2" г. Барнаула и их системы защиты информации);

– управление изменениями базовой конфигурации АС МБУ ДО "ЦДТ №2" г. Барнаула и их системы защиты информации, в том числе определение типов возможных изменений базовой конфигурации АС МБУ ДО "ЦДТ №2" г. Барнаула и их системы защиты информации, санкционирование внесения изменений в базовую конфигурацию АС МБУ ДО "ЦДТ №2" г. Барнаула и их системы защиты информации, документирование действий по внесению изменений в базовую конфигурацию АС МБУ ДО "ЦДТ №2" г. Барнаула и их системы защиты информации, сохранение данных об изменениях базовой конфигурации АС МБУ ДО "ЦДТ №2" г. Барнаула и их системы защиты информации, контроль действий по внесению изменений в базовую конфигурацию АС МБУ ДО "ЦДТ №2" г. Барнаула и их системы защиты информации;

– анализ потенциального воздействия планируемых изменений в базовой конфигурации АС МБУ ДО "ЦДТ №2" г. Барнаула и их системы защиты информации на обеспечение защиты информации, возникновение дополнительных угроз безопасности информации и работоспособность АС МБУ ДО "ЦДТ №2" г. Барнаула;

– определение параметров настройки программного обеспечения, включая программное обеспечение средств защиты информации, состава и конфигурации технических средств и программного обеспечения до внесения изменений в базовую конфигурацию АС МБУ ДО "ЦДТ №2" г. Барнаула и их системы защиты информации;

– внесение информации (данных) об изменениях в базовой конфигурации АС МБУ ДО "ЦДТ №2" г. Барнаула и их системы защиты информации в эксплуатационную документацию на систему защиты информации МБУ ДО "ЦДТ №2" г. Барнаула.

2.1.28. В случае возникновения нештатных ситуаций и аварийных ситуаций принимать меры по реагированию в пределах функций и полномочий с целью ликвидации последствий. Оперативно докладывать вышестоящему руководству о случаях возникновения внештатных ситуаций и аварийных ситуаций. В кратчайшие сроки принимать меры по восстановлению работоспособности элементов АС МБУ ДО "ЦДТ №2" г. Барнаула. Предпринимаемые меры по возможности согласовывать с вышестоящим руководством.

3. Права

3.1. Администратор ИБ имеет право:

3.1.1. Проводить служебные расследования по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов АС МБУ ДО "ЦДТ №2" г. Барнаула.

3.1.2. Непосредственно обращаться к пользователям АРМ с требованием прекращения работы в АС МБУ ДО "ЦДТ №2" г. Барнаула при несоблюдении установленной технологии обработки информации и невыполнении требований по безопасности.

3.1.3. В пределах своей компетенции сообщать своему непосредственному руководителю обо всех недостатках в работе АС МБУ ДО "ЦДТ №2" г. Барнаула и их системы защиты.

3.1.4. Требовать от своего непосредственного руководителя обеспечения организационно-технических условий, необходимых для исполнения обязанностей.

3.1.5. Подписывать и визировать документы в пределах своих обязанностей в соответствии с настоящей Инструкцией.

3.1.6. Получать доступ к информации, материалам, техническим средствам, помещениям, необходимый для надлежащего исполнения своих прав и обязанностей (в т.ч. вести мониторинг действий пользователей и обслуживающего персонала АС МБУ ДО "ЦДТ №2" г. Барнаула).

3.1.7. Вносить свои предложения по совершенствованию мер защиты информации в АС МБУ ДО "ЦДТ №2" г. Барнаула.

4. Ответственность

4.1. Администратор ИБ АС МБУ ДО "ЦДТ №2" г. Барнаула несет ответственность:

4.1.1. За ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных настоящей Инструкцией, – в пределах, определенных действующим трудовым законодательством Российской Федерации.

4.1.2. За правонарушения, совершенные в процессе осуществления своей деятельности, – в пределах, определенных действующим административным, уголовным и гражданским законодательством Российской Федерации.

4.1.3. За причинение материального ущерба – в пределах, определенных действующим трудовым и гражданским законодательством Российской Федерации.

Приложение №4 к приказу «Об утверждении документов, касающихся обработки конфиденциальной информации»
от «07» 10 2019 г. №95/1

Лист ознакомления

с Инструкцией администратора информационной безопасности автоматизированной системы МБУ ДО "ЦДТ №2" г. Барнаула

№ п/п	ФИО	Должность	Дата ознакомления	Подпись
1.	07.10.2019	методист	07.10.19	
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				
19.				
20.				

Приложение № 5 к приказу «Об утверждении документов, касающихся обработки конфиденциальной информации»
от «07» 10 2019 г. № 93/1

ИНСТРУКЦИЯ

по организации парольной защиты в

1 Общие положения

Настоящая инструкция устанавливает основные правила введения парольной защиты автоматизированной системы Муниципального бюджетного учреждения дополнительного образования "Центр детского творчества №2" г. Барнаула (далее – Учреждение). Инструкция регламентирует организационно-техническое обеспечение генерации, смены и прекращения действия паролей в автоматизированной системе, а также контроль за действиями пользователей системы при работе с паролями. Настоящая инструкция оперирует следующими основными понятиями:

– **Идентификация** - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

– **ИСПДн –** информационная система персональных данных.

– **Компрометация**- факт доступа постороннего лица к защищаемой информации, а также подозрение на него.

– **Объект доступа** - единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

– **Пароль** – уникальный признак субъекта доступа, который является его (субъекта) секретом.

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

– **Субъект доступа** - лицо или процесс, действия которого регламентируются правилами разграничения доступа.

– **Несанкционированный доступ** - доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или АС.

2 Правила генерации паролей

Персональные пароли должны генерироваться специальными программными средствами административной службы.

2.1 Длина пароля должна быть не менее 8 символов.

2.2 В составе пароля должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы.

2.3 Пароль не должен включать в себя:

– легко вычисляемые сочетания символов;

– клавиатурные последовательности символов и знаков;

– общепринятые сокращения;

– аббревиатуры;

– номера телефонов, автомобилей;

– прочие сочетания букв и знаков, ассоциируемые с пользователем;

– при смене пароля новое сочетание символов должно отличаться от предыдущего не менее чем на 2 символа.

2.4 Допускается использование единого пароля для доступа субъекта доступа к различным информационным ресурсам одной ИСПДн объекта образования.

3 Порядок смены паролей

3.1 Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одно раза в месяц.

3.2 Полная внеплановая смена паролей всех пользователей должна производиться случае прекращения полномочий администраторов средств защиты или других сотрудников, которым по роду службы были предоставлены полномочия по управлению парольной зашитой.

3.3 Полная внеплановая смена паролей должна производиться в случае компрометации личного пароля одного из администраторов ИСПДн.

3.4 В случае компрометации личного пароля пользователя надлежит немедленно ограничить доступ к информации с данной учетной записи, до момента вступления в силу новой учетной записи пользователя или пароля.

4 Обязанности пользователей при работе с парольной защитой

4.1 При работе с парольной защитой пользователям запрещается:

– разглашать кому-либо персональный пароль и прочие идентифицирующие сведения;

– предоставлять доступ от своей учетной записи к информации, хранящейся в ИСПДн посторонним лицам;

– записывать пароли на бумаге, файле, электронных и прочих носителях информации, в том числе и на предметах.

4.2 Хранение пользователем своего пароля на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе.

4.3 При вводе пароля пользователь обязан исключить возможность его перехвата сторонними лицами и техническими средствами.

5 Случаи компрометации паролей

5.1 Под компрометацией следует понимать:

– физическая утеря носителя с информацией;

– передача идентификационной информации по открытым каналам связи;

– проникновение постороннего лица в помещение физического хранения носителя парольной информации или алгоритма или подозрение на него (срабатывание сигнализации, повреждение устройств контроля НСД (слепков печатей), повреждение замков и т. п.);

– визуальный осмотр носителя идентификационной информации посторонним лицом;

– перехват пароля при распределении идентификаторов;

– сознательная передача информации постороннему лицу.

5.2 Действия при компрометации пароля:

- скомпрометированный пароль сразу же выводится из действия, взамен его вводятся запасной или новый пароль;
- о компрометации немедленно оповещаются все участники обмена информацией. Пароль вносится в специальные списки, содержащие скомпрометированные пароли и учетные записи.

6 Ответственность пользователей при работе с парольной защитой

6.1 Повседневный контроль за действиями сотрудников Учреждения при работе с паролями, соблюдением порядка их смены, хранения и использования, возлагается на Администратора безопасности.

6.2 Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

6.3 Ответственность за организацию парольной защиты возлагается на Администратора безопасности.

6.4 Ответственность в случае несвоевременного уведомлении ответственного за систему защиты информации в информационной системе персональных данных о случаях утери, кражи, взлома или компрометации паролей возлагается на владельца взломанной учетной записи.

Приложение № 5 к приказу «Об утверждении документов, касающихся обработки конфиденциальной информации»
от «08» 10 2019 г. № 93/1

Лист ознакомления

с инструкцией по организации парольной защиты в МБУ ДО "ЦДТ №2" г. Барнаула

№ п/п	ФИО	Должность	Дата ознакомления	Подпись
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				
19.				
20.				

Приложение № 8 к приказу «Об утверждении документов, касающихся обработки конфиденциальной информации»
от «07» 10 2019 г. № 934

План размещения основных и вспомогательных технических средств и систем

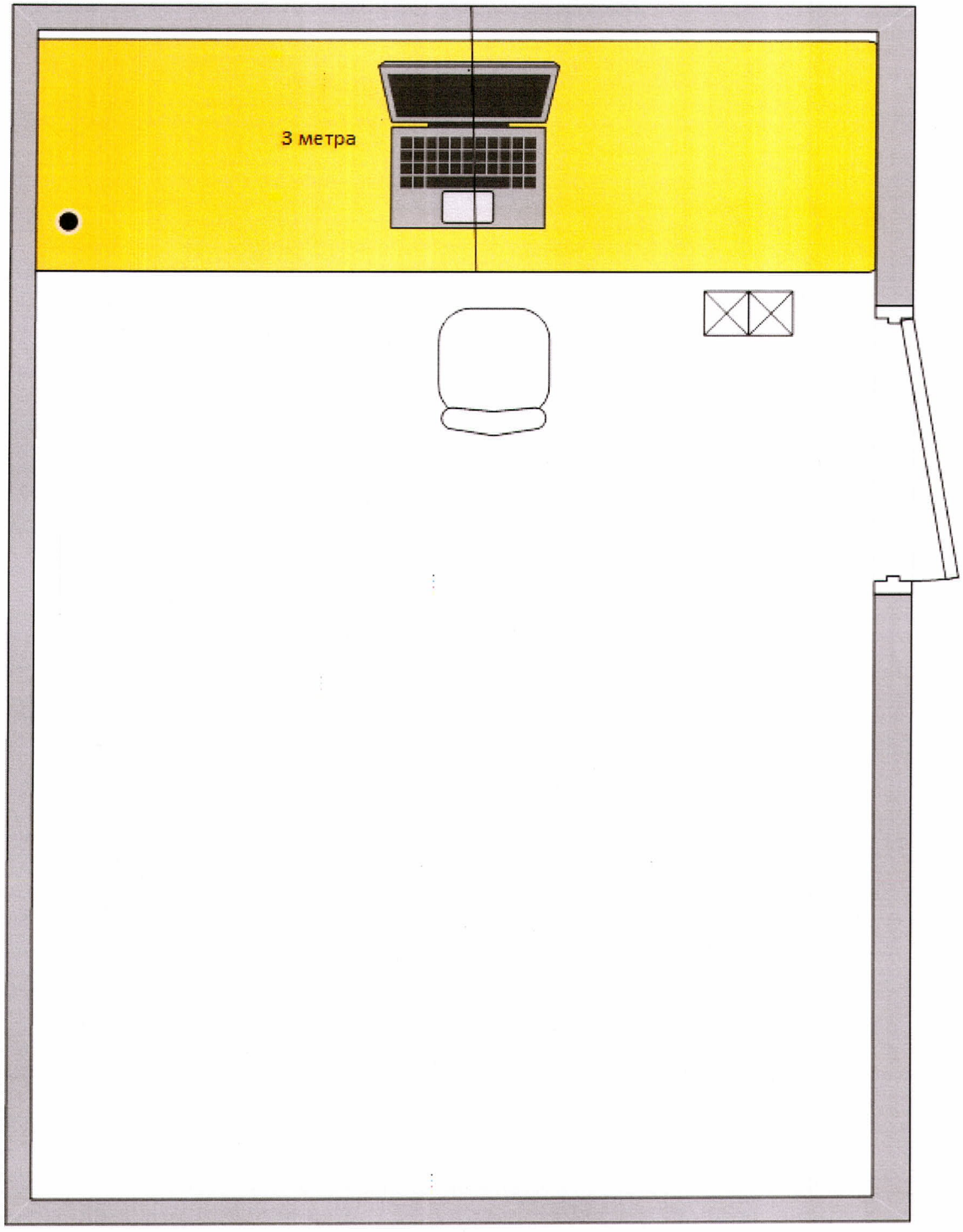

Рисунок 1 — Схема размещения ОТСС, ВТСС в Кабинете