МУНИЦИПАЛЬНОЕ УЧРЕЖДЕНИЕ КУЛЬТУРЫ
ГОРОДСКОГО ОКРУГА ПАВЛОВСКИЙ ПОСАД МОСКОВСКОЙ ОБЛАСТИ

« ЦЕНТРАЛИЗОВАННАЯ БИБЛИОТЕЧНАЯ СИСТЕМА»
142500, Московская область, г. Павловский Посад, ул. Выставкина, 1
Тел.: 8(496 43) 5-15 56
E-mail: bibliot-pp@mail.ru

ПРИКАЗ

№31/4 от 11.09.2019г.

Об утверждении Инструкции по
организации антивирусной защиты и
Регламента проведения резервного копирования

В целях исполнения в Муниципальном учреждении культуры городского округа Павловский Посад Московской области «Централизованная библиотечная система» Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных»,

ПРИКАЗЫВАЮ:

1. Утвердить Инструкцию по организации антивирусной защиты (Прилагается).
2. Утвердить Регламент проведения резервного копирования данных (Прилагается).
3. Контроль за исполнением настоящего приказа оставляю за собой.

Директор МУК «ЦБС» Ю.Г. Архипова

Приложение

К приказу МУК «ЦБС» от 11.09.2019г. № 31/4

«Об утверждении Инструкции по организации антивирусной защиты»

«Утверждаю»

Директор МУК «ЦБС»

Архипова Ю.Г.

11.09.2019г.

ИНСТРУКЦИЯ
по организации антивирусной защиты

1. Настоящая Инструкция определяет требования к организации защиты от разрушающего воздействия компьютерных вирусов и устанавливает ответственность руководителей и сотрудников Муниципального учреждения культуры городского округа Павловский Посад Московской области «Централизованная библиотечная система» за их выполнение.
2. К использованию в организации допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.
3. Установка средств антивирусного контроля на компьютерах осуществляется уполномоченным сотрудником организации. Настройка параметров средств антивирусного контроля в соответствии с руководствами по применению конкретных антивирусных средств.
4. Ежедневно в начале работы при загрузке компьютера в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов.
5. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (магнитных дисках, CD-ROM и т.п.).
6. Контроль входящей и исходящей информации на защищаемых серверах и персональных компьютерах (далее ПК) осуществляется непрерывно посредством постоянно работающего компонента антивирусного программного обеспечения («монитора»). Полная проверка информации, хранящейся на серверах и ПК должна осуществляться не реже одного раза в месяц.
7. Обновление баз вирусов антивирусного программного обеспечения, установленного на ПК и серверах, должно осуществляться еженедельно.
8. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера (локальной вычислительной сети), должна быть выполнена антивирусная проверка: на защищаемом автоматизированном рабочем месте (АРМ) ответственным за обеспечение информационной безопасности.
9. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.)

сотрудник организации самостоятельно или вместе с ответственным за антивирусную защиту организации должен провести внеочередной антивирусный контроль своей рабочей станции.

10. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники подразделений обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя и ответственного за антивирусную защиту организации, владельца зараженных файлов, а также сотрудников, использующих эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов.

11. Ответственность за антивирусный контроль в организации, в соответствии с требованиями настоящей Инструкции возлагается на руководителя организации.

12. Ответственность за проведение мероприятий антивирусного контроля в подразделении и соблюдение требований настоящей Инструкции возлагается на ответственного за антивирусную защиту и всех сотрудников, являющихся пользователями ПК.

13. Периодический контроль за состоянием антивирусной защиты, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции сотрудниками осуществляется ответственным за антивирусную защиту организации.

Приложение
к Приказу МУК «ЦБС»
от 11.09.2019 № 31/4

«Утверждаю»
Директор МУК «ЦБС»
_____ Ю.Г. Архипова
«11» сентября 2019г.

Регламент
проведения резервного копирования данных

1. Общие положения

1.1. Настоящий Регламент проведения резервного копирования (восстановления) программ и данных, хранящихся на автоматизированных рабочих местах и серверах Муниципального учреждения культуры городского округа Павловский Посад Московской области «Централизованная библиотечная система» (далее – учреждение) разработан с целью:

1.1.1. Определения порядка резервирования данных для последующего восстановления работоспособности информационной системы персональных данных (далее – ИСПДн) учреждения при полной или частичной потере информации, вызванной сбоями или отказами аппаратного или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т.д.);

1.1.2. Определения порядка восстановления информации в случае возникновения такой необходимости;

1.1.3. Упорядочения работы должностных лиц, связанной с резервным копированием и восстановлением информации.

1.2. Настоящий регламент отражает действия при выполнении следующих мероприятий:

1.2.1. Резервное копирование;

1.2.2. Контроль резервного копирования;

1.2.3. Хранение резервных копий;

1.2.4. Полное или частичное восстановление данных и приложений.

1.3. Резервному копированию подлежит информация следующих основных категорий:

1.3.1. Персональные данные субъектов;

1.3.2. Персональная информация пользователей (личные каталоги на файловых серверах);

1.3.3. Групповая информация пользователей (общие каталоги отделов);

1.3.4. Информация, необходимая для восстановления серверов и систем управления базами данных;

1.3.5. Персональные профили пользователей сети;

1.3.6. Информация автоматизированных систем, в т.ч. базы данных;

1.3.7. Рабочие копии установочных компонентов программного обеспечения рабочих станций;

1.3.8. Регистрационная информация системы информационной безопасности.

1.4. Машинным носителям информации, содержащим резервную копию, присваивается маркировка в соответствии с «Инструкцией по учету машинных носителей и регистрации их выдачи».

2. Порядок резервного копирования

2.1. Состав и объем копируемых данных, периодичность проведения резервного копирования определяется Перечнем информации для резервного копирования (Приложение №1). Максимальный срок хранения резервных копий 3 (три) месяца.

2.2. Система резервного копирования должна обеспечивать производительность, достаточную для сохранения информации, указанной в Перечне информации для резервного копирования, в установленные сроки и с заданной периодичностью. Методика проведения резервного копирования описана в Приложении №2.

2.3. О выявленных попытках несанкционированного доступа к резервируемой информации, а также иных нарушениях информационной безопасности произошедших в процессе резервного копирования, должно быть немедленно сообщено администратору безопасности ИСПДн, либо ответственному за обеспечение безопасности персональных данных учреждения.

3. Контроль результатов резервного копирования

3.1. Контроль результатов всех процедур резервного копирования осуществляется администратором безопасности ИСПДн.

3.2. На протяжении периода времени, когда система резервного копирования находится в аварийном состоянии, должно осуществляться ежедневное копирование информации, подлежащей резервированию, с использованием средств файловых систем серверов, располагающих необходимыми объемами дискового пространства для ее хранения.

4. Ротация носителей резервной копии

4.1. Система резервного копирования должна обеспечивать возможность периодической замены (выгрузки) резервных носителей без потерь информации на них, а также обеспечивать восстановление текущей информации ИСПДн в случае отказа любого из устройств резервного копирования. Все процедуры по загрузке, выгрузке носителей из системы резервного копирования, а также их перемещение, осуществляются администратором безопасности ИСПДн. В качестве новых носителей допускается повторно использовать те, у которых срок хранения содержащейся информации истек.

4.2. Носители с персональными данными, которые перестали использоваться в системе резервного копирования, должны стираться (форматироваться) с использованием специального программного обеспечения.

5. Восстановление информации из резервной копии

5.1. В случае необходимости, восстановление данных из резервных копий производится на основании заявки пользователя ИСПДн. Процедура восстановления информации из резервной копии осуществляется в соответствии с п. 5.2. настоящего Регламента. После поступления заявки, восстановление данных осуществляется в максимально сжатые сроки, ограниченные техническими возможностями системы, но не более одного рабочего дня.

5.2. Любое восстановление информации выполняется на основании заявки пользователя администратору безопасности ИСПДн или в случае необходимости восстановления утерянной или поврежденной информации, подлежащей резервированию. В процессе восстановления резервной копии следует руководствоваться инструкциями по восстановлению информации из резервных копий, описанных в документации, прилагающейся к системе резервного копирования ПО.

Приложение:

1. «Перечень резервируемой информации» на 1л. в 1экз.
2. «Методика резервного копирования» на 1л. в 1экз.
3. «Журнал учета отчуждаемых носителей информации резервного копирования» на 1л. в 1экз.

Приложение №1
к Регламенту резервного копирования данных

Перечень информации для резервного копирования

(_____)

Копируемый ресурс	Метод копирования	Тип копирования	Место размещения		Расписание копирования	Временные характеристики		Примечание
			Тип носителя	Периодичность смены		Срок хранения	Периодичность тестирования копий	

Приложение №2
к Регламенту резервного копирования данных

Методика резервного копирования

1. Для организации системы резервного копирования используются стандартные средства операционной системы.
2. Существует еженедельная копия. Срок хранения – три месяца.

Копии хранятся на внешнем НЖМД.

3. Различаются два принципиально разных источника информации, подлежащей резервированию:

– Информация, хранимая непосредственно в файловой системе - MS Windows;

– Базы данных ИСПДн.

4. Для резервирования информации, хранимой в базах данных ИСПДн учреждения, в качестве промежуточного звена автоматизации используются средства конфигурирования ИСПДн и архиваторы. В результате работы промежуточного звена автоматизации формируется каталог с резервной копией данных ИСПДн.

Приложение №3
к Регламенту резервного копирования данных

Журнал учета отчуждаемых носителей информации резервного копирования

Носитель копии	Передача на хранение			Выдача с хранения		
	Дата и время	Ответственное лицо, передавшее носитель		Дата и время	Ответственное лицо	
		ФИО	Подпись		ФИО	Подпись