РОССИЙСКАЯ ФЕДЕРАЦИЯ
АДМИНИСТРАЦИЯ МУНИЦИПАЛЬНОГО ОБРАЗОВАНИЯ
КУРГАНИНСКИЙ РАЙОН
ОТДЕЛ КУЛЬТУРЫ
МКУК «КУРГАНИНСКАЯ МЦБС»

П Р И К А З

От 13 ноября 2020 года № 176
г. Курганинск

О мерах информационной безопасности обеспечивающих защиту от несанкционированного доступа к информационным ресурсам в муниципальном казенном учреждении культуры «Курганинская межпоселенческая централизованная библиотечная система»

На основании Федерального закона от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановления Правительства Российской Федерации от 11 февраля 2017 года № 176 «Об утверждении требований к антитеррористической защищенности объектов (территорий) в сфере культуры и формы паспорта безопасности этих объектов (территорий), приказываю:

1. Утвердить Положение об информационной безопасности в муниципальном казенном учреждении культуры «Курганинская межпоселенческая централизованная библиотечная система» (далее МКУК «Курганинская МЦБС») (Приложение № 1 к приказу).
2. Утвердить Инструкцию по организации антивирусной защиты в МКУК «Курганинская МЦБС» (Приложение № 2 к приказу).
3. Утвердить Инструкцию по безопасной работе в сети Интернет и порядок работы с носителями ключевой информации в МКУК «Курганинская МЦБС» (Приложение № 3 к приказу).
4. Назначить ответственным за информационную безопасность в МКУК «Курганинская МЦБС» инженера-программиста – Павлова Федора Николаевича.
5. Назначить ответственной за антитеррористическую безопасность в МКУК «Курганинская МЦБС» заместителя директора по административно-хозяйственной работе – Бычкову Ирину Николаевну.

Директор _____ Л. Н. Глазунова
(должность) (подпись) (расшифровка)

М.П.

С приказом ознакомлен:
Заместитель директора _____ И.Н. Бычкова «13» ноября 2020 г.
(должность) (подпись) (расшифровка)
Инженер-программист _____ Ф.Н. Павлов «13» ноября 2020 г.
(должность) (подпись) (расшифровка)

Приложение № 1
к Приказу № 176 от 13.11.2020 г.

УТВЕРЖДАЮ
Директор
МКУК «Курганинская МЦБС»
_____ Л. Н. Глазунова

ПОЛОЖЕНИЕ
об информационной безопасности в муниципальном казенном учреждении культуры «Курганинская межпоселенческая централизованная библиотечная система»

1. Общие положения

1.1. Положение об информационной безопасности обеспечивающих защиту от несанкционированного доступа к информационным ресурсам (далее по тексту-Положение) муниципального казенного учреждения культуры «Курганинская межпоселенческая централизованная библиотечная система» (далее МКУК «Курганиская МЦБС») определяет организацию, осуществление и контроль мероприятий информационной безопасности, обеспечивающих защиту от несанкционированного доступа к информационным ресурсам (далее МКУК «Курганиская МЦБС»).

1.2. Положение разработано в соответствии с Постановлением Правительства РФ от 11 февраля 2017 года № 176 «Об утверждении требований к антитеррористической защищенности объектов (территорий) в сфере культуры и формы паспорта безопасности этих объектов (территорий)», с целью осуществления мероприятий информационной безопасности, обеспечивающих защиту от несанкционированного доступа к информационным ресурсам МКУК «Курганиская МЦБС».

1.3. Для обеспечения информационной безопасности МКУК «Курганиская МЦБС», приказом директора МКУК «Курганиская МЦБС» назначаются ответственные лица за обеспечение информационной безопасности МКУК «Курганиская МЦБС», которые в своей работе руководствуются данным Положением.

1.4. Срок действия данного Положения не ограничен. Положение действует до принятия нового.

2. Цели и задачи информационной безопасности МКУК «Курганиская МЦБС»:

2.1. Цель: осуществление мероприятий информационной безопасности. обеспечивающих защиту от несанкционированного доступа к информационным ресурсам МКУК «Курганиская МЦБС»;

2.2. Основными задачами обеспечения информационной безопасности являются:

- обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования. блокирования, копирования, предоставления,

распространения, а также от иных неправомерных действий в отношении такой информации;
- соблюдение конфиденциальности информации ограниченного доступа; - реализация права на доступ к информации;
- организация эксплуатации технических и программных средств защиты информации;
- текущий контроль работы средств систем защиты информации;
- организация и контроль резервного копирования информации.
3. Ответственные лица за обеспечение информационной безопасности МКУК «Курганиская МЦБС» (далее по тексту ответственные лица) в пределах своих функциональных обязанностей обеспечивают безопасность информации обрабатываемой, передаваемой и хранимой при помощи информационных средств в МКУК «Курганиская МЦБС»:
3.1. Ответственные лица за информационную безопасность выполняют следующие основные функции:
- разработка инструкций по информационной безопасности, инструкции по организации антивирусной защиты, инструкции по безопасной работе в Интернете. обучение работников-пользователей персональных компьютеров (далее по тексту - ПК) правилам безопасной обработки информации и правилам работы со средствами защиты информации;
- организация антивирусного контроля магнитных носителей информации и файлов электронной почты, поступающих в МКУК «Курганиская МЦБС»;
- текущий контроль работоспособности и эффективности функционирования эксплуатируемых программных и технических средств защиты информации. контроль целостности эксплуатируемого на ПК программного обеспечения с целью выявления несанкционированных изменений в нём;
- контроль за санкционированным изменением программного обеспечения, заменой и ремонтом МКУК «Курганиская МЦБС»;
- контроль пользования Интернетом.
4. Обязанности ответственных лиц за обеспечение информационной безопасности МКУК «Курганиская МЦБС»:
4.1. обеспечивать функционирование и поддерживать работоспособность средств и систем защиты информации в пределах, возложенных на них обязанностей. Немедленно докладывать директору МКУК «Курганиская МЦБС» о выявленных нарушениях и несанкционированных действиях работников пользователей ПК, а также принимать необходимые меры по устранению нарушений;
4.2. проводить инструктаж работников-пользователей ПК по правилам работы с используемыми средствами и системами защиты информации;
4.3. отслеживать работу антивирусных программ, проводить один раз в неделю полную проверку компьютеров на наличие вирусов;
4.4. контролировать регулярное резервное копирование данных (не реже чем один раз в неделю) всеми пользователями ПК, иметь возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
4.5. предотвращать несанкционированный доступ к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

4.6. своевременно выявлять факты несанкционированного доступа к информации;
4.7. предупреждать возможности неблагоприятных последствий нарушения порядка доступа к информации;
4.8. не допускать воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
4. 9. постоянно контролировать обеспечение высокого уровня защищенности информации в МКУК «Курганиская МЦБС».
5. Права ответственных лиц за обеспечение информационной безопасности МКУК «Курганиская МЦБС»:
5.1. требовать от работников-пользователей ПК безусловного соблюдения установленной технологии и выполнения инструкций по обеспечению безопасности и защиты информации, содержащей сведения ограниченного распространения;
6. Ответственность ответственных лиц за информационную безопасность МКУК «Курганиская МЦБС»:
6.1. на ответственных лиц за информационную безопасность МКУК «Курганиская МЦБС» возлагается персональная ответственность за качество проводимых ими работ по обеспечению информационной безопасности МКУК «Курганиская МЦБС», защиты информации в соответствии с функциональными обязанностями, определёнными настоящим Положением.

Приложение № 2
к Приказу № 176 от 13.11.2020 г.

УТВЕРЖДАЮ
Директор
МКУК «Курганинская МЦБС»

_____ Л. Г. Глазунова

ИНСТРУКЦИЯ
по организации антивирусной защиты в муниципальном казенном учреждении культуры «Курганинская межпоселенческая централизованная библиотечная система»

Настоящая Инструкция определяет требования к организации защиты от разрушающего воздействия компьютерных вирусов и устанавливает ответственность руководителей и сотрудников муниципального казенного учреждении культуры «Курганинская межпоселенческая централизованная библиотечная система» (далее МКУК «Курганинская МЦБС») за их выполнение.

1. К использованию в организации допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.
2. Установка средств антивирусного контроля на компьютерах осуществляется уполномоченным сотрудником организации. Настройка параметров средств антивирусного контроля в соответствии с руководствами по применению конкретных антивирусных средств.
3. Ежедневно в начале работы при загрузке компьютера в автоматическом режиме должен проводиться антивирусный контроль всех дисков и файлов.
4. 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.).
5. 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 ГК должна осуществляться не реже одного раза в месяц.
6. Обновление баз вирусов антивирусного программного обеспечения, установленного на ПК и серверах, должно осуществляться еженедельно.
7. 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.

8. 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.

9. 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.

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

11. 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.

12. 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 № 3
к Приказу № 176 от 13.11.2020 г.

УТВЕРЖДАЮ
Директор
МКУК «Курганинская МЦБС»
_____ Л. П. Глазунова

ИНСТРУКЦИЯ
по безопасной работе в сети Интернет и порядок работы с носителями ключевой информации в муниципальном казенном учреждении культуры «Курганинская межпоселенческая централизованная библиотечная система»

1. Безопасная работа в сети интернет

1.1. Ресурсы сети Интернет могут использоваться для осуществления выполнения требований законодательства Российской Федерации. дистанционного обслуживания, получения и распространения информации, связанной с деятельностью организации (в том числе, путем создания информационного web-сайта), информационно-аналитической работы в интересах организации, обмена почтовыми сообщениями, а также ведения собственной хозяйственной деятельности. Иное использование ресурсов сети Интернет, решение о котором не принято руководством организации в установленном порядке, рассматривается как нарушение информационной безопасности.

1.2. С целью ограничения использования сети Интернет в неустановленных целях выделяется ограниченное число пакетов, содержащих перечень сервисов и ресурсов сети Интернет, доступных для пользователей. Наделение работников организации правами пользователя конкретного пакета выполняется в соответствии с его должностными обязанностями.

1.3. Особенности использования сети Интернет:

сеть Интернет не имеет единого органа управления (за исключением службы управления пространством имен и адресов) и не является юридическим лицом, с которым можно было бы заключить договор (соглашение). Провайдеры (посредники) сети Интернет могут обеспечить только те услуги, которые реализуются непосредственно ими, гарантии по обеспечению информационной безопасности при использовании сети Интернет никаким органом не предоставляются.

1.4. При осуществлении электронного документооборота, в связи с повышенными рисками информационной безопасности при взаимодействии с сетью Интернет организация применяет соответствующие средства защиты информации (межсетевые экраны, антивирусные средства, средства криптографической защиты информации и пр.), обеспечивающие прием и передачу информации только в установленном формате и только для конкретной технологии.

1.5. Почтовый обмен конфиденциальной информацией через сеть Интернет осуществляется с использованием защитных мер.

1.6. Электронная почта организации подлежит периодической архивации. Доступ к архиву разрешен только подразделению (лицу) в организации, ответственному за обеспечение информационной безопасности. Изменения в архиве не допускаются.

1.7. При взаимодействии с сетью Интернет Департамент информационных технологий обеспечивает программными и аппаратными средствами противодействие атакам хакеров и распространению спама.

1.8. При пользовании ресурсами сети Интернет запрещается:

- использовать на рабочем месте иные каналы доступа персонального компьютера к сети Интернет, кроме установленного;
- проводить самостоятельное изменение конфигурации технического и программного обеспечения персонального компьютера, подключенной к сети Интернет;
- осуществлять отправку электронных почтовых сообщений, содержащих конфиденциальную информацию, по открытым каналам;
- использовать иные, кроме служебных, почтовые ящики для электронной переписки;
- открывать файлы, пришедшие вместе с почтовым сообщением, если не известен источник этого сообщения;
- осуществлять перенос полученной по сети Интернет документированной информации в электронном виде на другие компьютеры без проверки ее антивирусными программами;
- скачивать из сети Интернет, в том числе средствами электронной почты, информацию, содержащую исполняемые модули, программы, драйверы и т.п., без предварительного согласования с Департаментом информационных технологий;
- использовать сеть Интернет вне служебных задач, посещать интернет - сайты, не связанные с выполнением должностных обязанностей.

2. Порядок работы с носителями ключевой информации:

2.1. В некоторых подсистемах организации для обеспечения контроля за целостностью передаваемых по технологическим каналам электронных документов (далее ЭД), а также для подтверждения их подлинности и авторства могут использоваться средства электронной подписи (ЭЦП).

2.2. Работнику организации (владельцу ключа ЭЦП, которому в соответствии с его должностными обязанностями предоставлено право постановки на ЭД его ЭЦП, выдается персональный ключевой носитель информации, на который записана уникальная ключевая информация (ключ ЭЦП), относящаяся к категории сведений ограниченного распространения.

2.3. Ключевые носители маркируются соответствующими этикетками, на которых отражается: регистрационный номер носителя и, при возможности размещения, дата изготовления и подпись уполномоченного сотрудника, изготовившего носитель, вид ключевой информации эталон или рабочая копия, фамилия, имя, отчество и подпись владельца ключа ЭЦП.

2.4. Персональные ключевые носители (эталон и рабочую копию) владелец ключа ЭЦП должен хранить в специальном месте, гарантирующем их сохранность.

2.5. Ключи проверки ЭЦП установленным порядком регистрируются в справочнике ключей, используемом при проверке подлинности документов по установленным на них ЭЦП.

2.6. Владелец ключа обязан:

- использовать для работы только рабочую копию своего ключевого носителя;
- сдавать свой персональный ключевой носитель на временное хранение руководителю подразделения или ответственному за информационную безопасность в период отсутствия на рабочем месте (например, на время отпуска или командировки);
- в случае порчи рабочей копии ключевого носителя (например, при ошибке чтения) владелец ЭЦП обязан передать его уполномоченному сотруднику, который должен в присутствии исполнителя сделать новую рабочую копию ключевого носителя с имеющегося эталона и выдать его взамен испорченного. Испорченная рабочая копия ключевого носителя должна быть уничтожена.

2.7. Владельцу ключа ЭЦП запрещается:

- оставлять ключевой носитель без личного присмотра;
- передавать свой ключевой носитель (эталонную или рабочую копию) другим лицам (кроме как для хранения руководителю подразделения или ответственному за информационную безопасность);
- делать неучтенные копии ключевого носителя, распечатывать или переписывать с него файлы на иной носитель информации (например, жесткий диск персонального компьютера), снимать защиту от записи, вносить изменения в файлы, находящиеся на ключевом носителе;
- использовать ключевой носитель на заведомо неисправном дисководе и/или персональном компьютере;
- подписывать своим персональным ключом ЭЦП любые электронные сообщения и документы, кроме тех видов документов, которые регламентированы технологическим процессом;
- сообщать третьим лицам информацию о владении ключом ЭЦП для данного технологического процесса.

2.8. Действия при компрометации ключей:

2.8.1. Если у владельца ключа ЭЦП появилось подозрение, что его ключевой носитель попал или мог попасть в чужие руки (был скомпрометирован), он обязан немедленно прекратить (не возобновлять) работу с ключевым носителем, сообщить об этом в Департамент информационных технологий и Департамент экономической безопасности, сдать скомпрометированный ключевой носитель с пометкой в журнале учета ключевых носителей о причине компрометации, написать служебную записку о факте компрометации персонального ключевого носителя на имя руководителя подразделения.

2.8.2. В случае утери ключевого носителя владелец ключа ЭЦП обязан немедленно сообщить об этом в Департамент информационных технологий и Департамент экономической безопасности, написать объяснительную записку об утере ключевого носителя на имя руководителя подразделения и принять участие в служебной проверке по факту утери ключевого носителя.

2.8.3. Ответственный за информационную безопасность обязан немедленно оповестить о факте утраты или компрометации ключевого носителя

руководителю организации для принятия действий по блокированию ключей для ЭЦП указанного исполнителя.

2.8.4. По решению руководства организации установленным порядком владелец ключа ЭЦП может получить новый комплект персональных ключевых носителей взамен скомпрометированных,

2.8.5. В случае перевода владельца ключа ЭЦП на другую работу, увольнения или прекращения трудовых отношений иным образом он обязан сдать (сразу по окончании последнего сеанса работы) свой ключевой носитель ответственному за информационную безопасность.