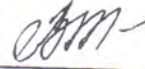


УТВЕРЖДЕНО  
приказом районного муниципального учреждения  
культуры «Межпоселенческий культурно-  
досуговый центр»

от « 15 » августа 2018 г. № 150-п



И.Б. Винникова

**ПОЛИТИКА**  
**информационной безопасности**  
**районного муниципального учреждения культуры**  
**«Межпоселенческий культурно-досуговый центр»**

г. Ейск  
2018

## **1. Общее положение.**

1.1. Политика информационной безопасности районного муниципального учреждения культуры «Межпоселенческий культурно-досуговый центр» (далее – РМУК «МКДЦ») определяет цели и задачи системы обеспечения информационной безопасности) и устанавливает совокупность правил, процедур, практических приемов, требований и руководящих принципов в области информационной безопасности (далее-ИБ), которыми руководствуются работники РМУК «МКДЦ» при осуществлении своей деятельности.

1.2. Основной целью Политики информационной безопасности РМУК «МКДЦ» является защита информации при осуществлении уставной деятельности, которая предусматривает принятие необходимых мер в целях защиты информации от случайного или преднамеренного изменения, раскрытия или уничтожения, а также в целях соблюдения конфиденциальности, целостности и доступности информации, обеспечения процесса автоматизированной обработки данных.

1.3. Политика информационной безопасности разработана в соответствии с: Федеральным законом от 27 июля 2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 № 152-ФЗ «О персональных данных», Федеральным законом от 06.04.2011 №631-ФЗ «Об электронной подписи», Указом Президента Российской Федерации от 06 марта 1997 № 188 «Об утверждении Перечня сведений конфиденциального характера», Постановление Правительства РФ №687 от 15.09.2008 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», а также рядом иных нормативных правовых актов в сфере защиты информации.

1.4.Выполнение требований Политики ИБ является обязательным для сотрудников РМУК «МКДЦ».

1.5.Ответственность за соблюдение информационной безопасности несет каждый сотрудник РМУК «МКДЦ».

## **2. Цель и задачи политики информационной безопасности.**

2.1.Основными целями политики ИБ являются:

- сохранение конфиденциальности критичных информационных ресурсов;
- обеспечение непрерывности доступа к информационным ресурсам РМУК «МКДЦ»;
- защита целостности информации с целью поддержания возможности РМУК «МКДЦ» по оказанию услуг высокого качества и принятию эффективных решений;
- повышение осведомленности пользователей в области рисков, связанных с информационными ресурсами;
- определение степени ответственности и обязанностей сотрудников по обеспечению информационной безопасности.
- повышение уровня эффективности, непрерывности, контролируемости мер по защите от реальных угроз ИБ;

-предотвращение и/или снижение ущерба от инцидентов ИБ.

2.2.Основными задачами политики ИБ являются:

- разработка требований по обеспечению ИБ;
- контроль выполнения установленных требований по обеспечению ИБ;
- повышение эффективности, непрерывности, контролируемости мероприятий по обеспечению и поддержанию ИБ;
- разработка нормативных документов для обеспечения ИБ в РМУК «МКДЦ»;
- выявление, оценка, прогнозирование и предотвращение реализации угроз ИБ в РМУК «МКДЦ»;
- организация антивирусной защиты информационных ресурсов в РМУК «МКДЦ»;
- защита информации в РМУК «МКДЦ» от несанкционированного доступа (далее-НСД) и утечки по техническим каналам связи;
- организация периодической проверки соблюдения информационной безопасности с последующим представлением отчета по результатам указанной проверки директору РМУК «МКДЦ».

### **3. Концептуальная схема обеспечения информационной безопасности.**

3.1.Политика ИБ в РМУК «МКДЦ» направлена на защиту информационных ресурсов от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий сотрудников РМУК «МКДЦ», технических сбоев автоматизированных систем, неправильных технологических и организационных решений в процессах поиска, сбора хранения, обработки, предоставления и распространения информации и обеспечение эффективного и бесперебойного процесса деятельности.

3.2.Наибольшими возможностями для нанесения ущерба обладает собственный персонал РМУК «МКДЦ». Риск аварий и технических сбоев определяется надежностью систем энергоснабжения и телекоммуникаций, квалификацией сотрудников и их способностью к адекватным и незамедлительным действиям в нештатной ситуации.

3.3.Стратегия обеспечения ИБ в РМУК «МКДЦ» заключается в использовании заранее разработанных мер противодействия атакам злоумышленников, а также программно-технических и организационных решений, позволяющих свести к минимуму возможные потери от технических аварий и ошибочных действий сотрудников РМУК «МКДЦ».

### **4. Основные принципы обеспечения информационной безопасности.**

4.1.Основными принципами обеспечения ИБ:

- постоянный и всесторонний анализ автоматизированных систем и трудового процесса с целью выявления уязвимости информационных активов РМУК «МКДЦ» (**информационный актив** – это информация с реквизитами, позволяющими ее идентифицировать; имеющая ценность для учреждения; находящаяся в распоряжении РМУК «МКДЦ» и представленная на любом

материальном носителе в пригодной для ее обработки, хранения или передачи форме);

-своевременное обнаружение проблем, потенциально способных повлиять на ИБ в РМУК «МКДЦ», корректировка моделей угроз и нарушителя;

-разработка и внедрение защитных мер;

-контроль эффективности принимаемых защитных мер;

-персонализация и разделение ролей и ответственности между сотрудниками РМУК «МКДЦ» за обеспечение ИБ в РМУК «МКДЦ» исходит из принципа персональной и единоличной ответственности за совершаемые операции.

#### **5. Объекты защиты.**

5.1. Объектами защиты с точки зрения ИБ в РМУК «МКДЦ» являются:

-информационный процесс профессиональной деятельности;

-информационные активы РМУК «МКДЦ».

5.2. Защищаемая информация делится на следующие виды:

-информация по финансово-экономической деятельности РМУК «МКДЦ»;

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

-другая информация, не относящаяся ни к одному из указанных выше видов, которая отмечена грифом «Для служебного пользования» или «Конфиденциально».

#### **6. Требования по информационной безопасности.**

6.1. В отношении всех собственных информационных активов РМУК «МКДЦ», активов, находящихся под контролем РМУК «МКДЦ», а также активов, используемых для получения доступа к инфраструктуре РМУК «МКДЦ», должна быть определена ответственность соответствующего сотрудника РМУК «МКДЦ».

Информация о смене владельцев активов, их распределении, изменениях в конфигурации и использовании за пределами РМУК «МКДЦ» должна доводиться до сведения директора РМУК «МКДЦ».

6.2. Все работы в пределах РМУК «МКДЦ» должны выполняться в соответствии с официальными должностными обязанностями только на компьютерах, разрешенных к использованию в РМУК «МКДЦ».

6.3. Внос в здание и помещения РМУК «МКДЦ» личных портативных компьютеров и внешних носителей информации (диски, дискеты, флэш-карты и т.п.), а также вынос их за пределы РМУК «МКДЦ» производится только при согласовании с администратором локально-вычислительной сети (далее – ЛВС).

6.4. Все данные (конфиденциальные или строго конфиденциальные), составляющие тайну РМУК «МКДЦ» и хранящиеся на жестких дисках портативных компьютеров, должны быть зашифрованы.

6.5.Руководители отделов должны периодически пересматривать права доступа своих сотрудников и других пользователей к соответствующим информационным ресурсам.

6.6.В целях обеспечения санкционированного доступа к информационному ресурсу, любой вход в систему должен осуществляться с использованием уникального имени пользователя и пароля.

6.7.Пользователи должны руководствоваться рекомендациями по защите своего пароля на этапе его выбора и последующего использования. Запрещается сообщать свой пароль другим лицам или предоставлять свою учетную запись другим, в том числе членам своей семьи и близким.

6.8.В процессе своей работы сотрудники обязаны постоянно использовать режим "Экранной заставки" с парольной защитой. Рекомендуется устанавливать максимальное время "простоя" компьютера до появления экранной заставки не дольше 15 минут.

6.9. Доступ третьих лиц к информационным системам РМУК «МКДЦ» должен быть обусловлен производственной необходимостью. В связи с этим, порядок доступа к информационным ресурсам РМУК «МКДЦ» должен быть четко определен, контролируем и защищен.

6.10.Доступ к сети Интернет обеспечивается только в производственных целях и не может использоваться для незаконной деятельности.

Рекомендованные правила:

-сотрудникам РМУК «МКДЦ» разрешается использовать сеть Интернет только в служебных целях;

-запрещается посещение любого сайта в сети Интернет, который считается оскорбительным для общественного мнения или содержит информацию сексуального характера, пропаганду расовой ненависти, комментарии по поводу различия/превосходства полов, дискредитирующие заявления или иные материалы с оскорбительными высказываниями по поводу чьего-либо возраста, сексуальной ориентации, религиозных или политических убеждений, национального происхождения или недееспособности;

-сотрудники РМУК «МКДЦ» не должны использовать сеть Интернет для хранения корпоративных данных;

-работа сотрудников РМУК «МКДЦ» с Интернет-ресурсами допускается только режимом просмотра информации, исключая возможность передачи информации РМУК «МКДЦ» в сеть Интернет;

-сотрудникам, имеющим личные учетные записи, предоставленные публичными провайдерами, не разрешается пользоваться ими на оборудовании, принадлежащем РМУК «МКДЦ»;

-сотрудники РМУК «МКДЦ» перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов;

-запрещен доступ в Интернет для всех лиц, не являющихся сотрудниками РМУК «МКДЦ», включая членов семьи сотрудников РМУК «МКДЦ».

6.11.Администратор ЛВС имеет право контролировать содержание всего потока информации, проходящей через канал связи к сети Интернет в обоих направлениях.

6.12. Сотрудники должны постоянно помнить о необходимости обеспечения физической безопасности оборудования, на котором хранится информация РМУК «МКДЦ».

6.13.Сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения производит администратор ЛВС.

6.14.Все компьютерное оборудование (серверы, стационарные и портативные компьютеры), периферийное оборудование (например, принтеры и сканеры), аксессуары (манипуляторы типа "мышь", шаровые манипуляторы, дисководы для CD-дисков), коммуникационное оборудование (например, факс-модемы, сетевые адаптеры и концентраторы), для целей настоящей политики вместе именуется "компьютерное оборудование". Компьютерное оборудование, предоставленное учреждением, является ее собственностью и предназначено для использования исключительно в производственных целях.

6.15.Каждый сотрудник, получивший в пользование портативный компьютер, обязан принять надлежащие меры по обеспечению его сохранности.

6.16.Все компьютеры должны защищаться паролем при загрузке системы, активации по горячей клавиши и после выхода из режима "Экранной заставки". Для установки режимов защиты пользователь должен обратиться к администратору ЛВС. Данные не должны быть скомпрометированы в случае халатности или небрежности приведшей к потере оборудования. Перед утилизацией все компоненты оборудования, в состав которых входят носители данных (включая жесткие диски), необходимо проверять, чтобы убедиться в отсутствии на них конфиденциальных данных и лицензионных продуктов. Должна выполняться процедура форматирования носителей информации, исключая возможность восстановления данных.

6.17.Порты передачи данных, в том числе FDD и CD дисководы в стационарных компьютерах сотрудников РМУК «МКДЦ» блокируются, за исключением тех случаев, когда сотрудником получено разрешение на запись администратора ЛВС.

6.18.Все программное обеспечение, установленное на предоставленном учреждением компьютерном оборудовании, является собственностью РМУК «МКДЦ» и должно использоваться исключительно в производственных целях.

6.19.Сотрудникам запрещается устанавливать на предоставленном в пользование компьютерном оборудовании нестандартное, нелицензионное программное обеспечение или программное обеспечение, не имеющее отношения к их деятельности.

6.20.На всех портативных компьютерах должны быть установлены программы, необходимые для обеспечения защиты информации:

- персональный межсетевой экран;

- антивирусное программное обеспечение;
- программное обеспечение шифрования жестких дисков;
- программное обеспечение шифрования почтовых сообщений.

6.21. Сотрудники РМУК «МКДЦ» не должны:

- блокировать антивирусное программное обеспечение;
- устанавливать другое антивирусное программное обеспечение;
- изменять настройки и конфигурацию антивирусного программного обеспечения.

6.22. Электронные сообщения должны строго соответствовать стандартам в области деловой этики. Использование электронной почты в личных целях не допускается. Сотрудникам запрещается направлять конфиденциальную информацию РМУК «МКДЦ» по электронной почте без использования систем шифрования. Строго конфиденциальная информация РМУК «МКДЦ», ни при каких обстоятельствах, не подлежит пересылке третьим лицам по электронной почте.

6.23. Использование сотрудниками РМУК «МКДЦ» публичных почтовых ящиков электронной почты осуществляется только при согласовании с ответственным за обеспечение безопасности информации ЛВС при условии применения механизмов шифрования.

6.24. Сотрудники РМУК «МКДЦ» для обмена документами должны использовать только свой официальный адрес электронной почты.

6.25. Сообщения, пересылаемые по электронной почте, представляют собой постоянно используемый инструмент для электронных коммуникаций, имеющих тот же статус, что и письма и факсимильные сообщения. Электронные сообщения подлежат такому же утверждению и хранению, что и прочие средства письменных коммуникаций.

В целях предотвращения ошибок при отправке сообщений пользователи перед отправкой должны внимательно проверить правильность написания имен и адресов получателей. В случае получения сообщения лицом, вниманию которого это сообщение не предназначается, такое сообщение необходимо переправить непосредственному получателю. Если полученная таким образом информация носит конфиденциальный характер, об этом следует незамедлительно проинформировать администратора ЛВС. Отправитель электронного сообщения, документа или лицо, которое его переадресовывает, должен указать свое имя и фамилию, служебный адрес и тему сообщения.

6.26. Не допускается при использовании электронной почты:

- рассылка сообщений личного характера, использующих значительные ресурсы электронной почты;
- рассылка рекламных материалов;
- подписка на рассылку, участие в дискуссиях и подобные услуги, использующие значительные ресурсы электронной почты в личных целях;
- поиск и чтение сообщений, направленных другим лицам (независимо от способа их хранения);

- пересылка любых материалов, как сообщений, так и приложений, содержание которых является противозаконным, непристойным, злонамеренным, оскорбительным, угрожающим, клеветническим, злобным или способствует поведению, которое может рассматриваться как уголовное преступление или административный проступок либо приводит к возникновению гражданско-правовой ответственности, беспорядков или противоречит стандартам в области этики.

6.27. Объем пересылаемого сообщения по электронной почте не должен превышать 2 Мбайт.

6.28. Все пользователи должны быть осведомлены о своей обязанности сообщать об известных или подозреваемых ими нарушениях информационной безопасности, а также должны быть проинформированы о том, что ни при каких обстоятельствах они не должны пытаться использовать ставшие им известными слабые стороны системы безопасности.

6.29. В случае кражи переносного компьютера следует незамедлительно сообщить администратору ЛВС.

6.30. Если имеется подозрение или выявлено наличие вирусов или иных разрушительных компьютерных кодов, то сразу после их обнаружения сотрудник обязан:

- проинформировать администратора ЛВС;

- не пользоваться и не выключать зараженный компьютер до тех пор, пока на нем не будет произведено удаление обнаруженного вируса и полное антивирусное сканирование администратором ЛВС.

6.31. Сотрудникам РМУК «МКДЦ» запрещается:

- нарушать информационную безопасность в РМУК «МКДЦ»;

- сканировать порты или систему безопасности;

- получать доступ к компьютеру, сети или учетной записи в обход системы идентификации пользователя или безопасности;

- использовать любые программы, скрипты, команды или передавать сообщения с целью вмешаться в работу или отключить пользователя оконечного устройства;

- передавать информацию о сотрудниках или списки сотрудников РМУК «МКДЦ» посторонним лицам;

- создавать, обновлять или распространять компьютерные вирусы и прочие разрушительное программное обеспечение.

6.32. Ответственность за сохранность данных на стационарных и портативных персональных компьютерах лежит на пользователях.

6.33. Необходимо регулярно делать резервные копии всех основных служебных данных и программного обеспечения.

6.34. Только администратор ЛВС на основании заявок начальников отделов может создавать и удалять совместно используемые сетевые ресурсы и папки общего пользования, а также управлять полномочиями доступа к ним.

6.35. Сотрудники имеют право создавать, модифицировать и удалять файлы и директории в совместно используемых сетевых ресурсах только на тех



участках, которые выделены лично для них, для их рабочих групп или к которым они имеют санкционированный доступ.

6.36. Все заявки на проведение технического обслуживания компьютеров должны направляться администратору ЛВС.

6.37. Все операционные процедуры и процедуры внесения изменений в информационные системы должны быть документированы, и согласованы с администратором ЛВС.

### **7. Управление информационной безопасностью.**

7.1. Управление ИБ в РМУК «МКДЦ» включает в себя:

- разработку и поддержание в актуальном состоянии Политики информационной безопасности;
- разработку и поддержание в актуальном состоянии нормативно-методических документов по обеспечению ИБ;
- обеспечение бесперебойного функционирования комплекса средств ИБ;
- осуществление контроля (мониторинга) функционирования системы ИБ;
- оценку рисков, связанных с нарушениями ИБ.

### **8. Реализация политики информационной безопасности**

8.1. Реализация Политики ИБ в РМУК «МКДЦ» осуществляется на основании документов, регламентирующих отдельные процедуры и процессы профессиональной деятельности в РМУК «МКДЦ».

### **9. Порядок внесения изменений и дополнений в политику информационной безопасности**

9.1. Внесение изменений и дополнений в Политику информационной безопасности производится не реже одного раза в три года с целью приведения в соответствие определенных Политикой защитных мер реальным жизненным условиям и текущим требованиям к защите информации.

### **10. Контроль за соблюдением политики информационной безопасности**

10.1. Текущий контроль за соблюдением выполнения требований Политики информационной безопасности в РМУК «МКДЦ» возлагается на сотрудника, назначенного приказом директора РМУК «МКДЦ».

10.2. Директор РМУК «МКДЦ» на регулярной основе рассматривает реализацию и соблюдение отдельных положений Политики информационной безопасности, а также осуществляет последующий контроль за соблюдением ее требований.

Директор районного муниципального учреждения «МКДЦ»



И.Б. Винникова