Утверждена приказом МАОУ ДО «ДЦК»
от 29.12.2018 № 173

Политика информационной безопасности в муниципальном автономном образовательном учреждении дополнительного образования «Детский центр культуры»

1. Общие положения

1.1. Политика информационной безопасности в муниципальном автономном образовательном учреждении дополнительного образования «Детский центр культуры» (далее – МАОУ ДО «ДЦК») 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 МАОУ ДО «ДЦК» при осуществлении своей деятельности.

1.2. Основной целью Политики информационной безопасности МАОУ ДО «ДЦК» является защита информации МАОУ ДО «ДЦК» 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 в управлении.

1.3. Политика информационной безопасности разработана в соответствии с: Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите и информации», Федеральным закон от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным закон от 10.01.2002 № 1-ФЗ «Об электронной цифровой подписи», Указом Президента Российской Федерации от 6.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера», Постановлением Правительства РФ № 781 от 17.11.2007 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», Постановлением 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 всех подразделений МАОУ ДО «ДЦК».

1.5. Ответственность за соблюдение информационной безопасности несет каждый сотрудник МАОУ ДО «ДЦК». На лиц, работающих по договорам гражданско-правового характера, положения настоящей политики распространяются в случае, если это обусловлено в таком договоре.

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 МАОУ ДО «ДЦК»;

-защита целостности информации с целью поддержания возможности МАОУ ДО «ДЦК» по оказанию услуг высокого качества и принятию эффективных управленческих решений;
- повышение осведомленности пользователей в области рисков, связанных с информационными ресурсами МАОУ ДО «ДЦК»;
- 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 МАОУ ДО «ДЦК»;
- выявление, оценка, прогнозирование и предотвращение реализации угроз ИБ МАОУ ДО «ДЦК»;
- организация антивирусной защиты информационных ресурсов МАОУ ДО «ДЦК»;
- защита информации МАОУ ДО «ДЦК» от несанкционированного доступа (далее – НСД) и утечки по техническим каналам связи;
- организация периодической проверки соблюдения информационной безопасности.

3. Концептуальная схема обеспечения информационной безопасности

3.1. Политика ИБ МАОУ ДО «ДЦК» направлена на защиту информационных ресурсов (активов) от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий сотрудников МАОУ ДО «ДЦК», 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. Риск аварий и технических сбоев в автоматизированных системах определяется состоянием аппаратного обеспечения, надежностью систем энергоснабжения и телекоммуникаций, квалификацией сотрудников и их способностью к адекватным и незамедлительным действиям в нештатной ситуации.

3.3. Стратегия обеспечения ИБ МАОУ ДО «ДЦК» 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 МАОУ ДО «ДЦК».

4. Объекты защиты

4.1. Объектами защиты с точки зрения ИБ являются:
- информационный процесс профессиональной деятельности;
- информационные активы МАОУ ДО «ДЦК».

4.2. Защищаемая информация делится на следующие виды:
- информация по финансово-экономической деятельности МАОУ ДО «ДЦК»;

- 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».

5. Требования по информационной безопасности

5.1. В отношении всех собственных информационных активов МАОУ ДО «ДЦК», активов, находящихся под контролем МАОУ ДО «ДЦК», а также активов, используемых для получения доступа к инфраструктуре МАОУ ДО «ДЦК», должна быть определена ответственность соответствующего сотрудника МАОУ ДО «ДЦК». Информация о смене владельцев активов, их распределении, изменениях в конфигурации и использовании за пределами МАОУ ДО «ДЦК» должна доводиться до сведения директора МАОУ ДО «ДЦК».

5.2. Все работы в пределах МАОУ ДО «ДЦК» должны выполняться в соответствии с официальными должностными обязанностями только на компьютерах, разрешенных к использованию.

5.3. Внос в здание и помещения МАОУ ДО «ДЦК» личных портативных компьютеров и внешних носителей информации (диски, дискеты, флэш-карты и т.п.), а также вынос их за пределы МАОУ ДО «ДЦК» производится только при согласовании с администрацией МАОУ ДО «ДЦК».

5.4.Все данные (конфиденциальные или строго конфиденциальные), составляющие тайну МАОУ ДО «ДЦК» и хранящиеся на жестких дисках портативных компьютеров, должны быть зашифрованы.

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

5.6. 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.

5.7. 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.

5.8. Сотрудникам, использующим в работе портативные компьютеры МАОУ ДО «ДЦК», может быть предоставлен удаленный доступ к сетевым ресурсам МАОУ ДО «ДЦК».

5.9. Сотрудникам, работающим за пределами МАОУ ДО «ДЦК» с использованием компьютера, не принадлежащего МАОУ ДО «ДЦК», запрещено копирование данных на компьютер, с которого осуществляется удаленный доступ.

5.10. Все компьютеры, подключаемые посредством удаленного доступа к информационной сети МАОУ ДО «ДЦК», должны иметь программное обеспечение антивирусной защиты, имеющее последние обновления.

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

Рекомендованные правила:

- сотрудникам МАОУ ДО «ДЦК» 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 МАОУ ДО «ДЦК» не должны использовать сеть Интернет для хранения корпоративных данных;
- сотрудники МАОУ ДО «ДЦК» перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов;
- запрещен доступ в Интернет через сеть МАОУ ДО «ДЦК» для всех лиц, не являющихся сотрудниками МАОУ ДО «ДЦК», включая членов семьи сотрудников МАОУ ДО «ДЦК».

5.12. Сотрудники должны постоянно помнить о необходимости обеспечения физической безопасности оборудования, на котором хранится информация МАОУ ДО «ДЦК».

5.13. Сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения производит техник МАОУ ДО «ДЦК».

5.14. 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 именуются "компьютерное оборудование". Компьютерное оборудование, предоставленное МАОУ ДО «ДЦК», является его собственностью и предназначено для использования исключительно в управленческих и образовательных целях.

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

5.16. 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 технику МАОУ ДО «ДЦК». 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, исключающая возможность восстановления данных.

5.17. При записи какой-либо информации на носитель для передачи субъектам, участвующим в информационном обмене, необходимо убедиться в том, что носитель чист, то есть не содержит никаких иных данных. Простое переформатирование носителя не дает гарантии полного удаления записанной на нем информации.

5.18. Все программное обеспечение, установленное на предоставленном МАОУ ДО «ДЦК» компьютерном оборудовании, является собственностью МАОУ ДО «ДЦК» и должно использоваться исключительно в целях обеспечения образовательного процесса.

5.19. Сотрудникам запрещается устанавливать на предоставленном в пользование компьютерном оборудовании нестандартное, нелицензионное программное обеспечение или программное обеспечение, не имеющее отношения к их деятельности. Если в ходе выполнения технического обслуживания будет обнаружено не разрешенное к установке программное обеспечение, оно будет удалено, а сообщение о нарушении будет направлено непосредственному руководителю сотрудника и директору МАОУ ДО «ДЦК».

5.20. Все компьютеры МАОУ ДО «ДЦК» должны быть оснащены системой антивирусной защиты.

5.21. Сотрудники МАОУ ДО «ДЦК» не должны:

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

5.22. Электронные сообщения должны строго соответствовать стандартам в области деловой этики. Использование электронной почты в личных целях не допускается. Строго конфиденциальная информация МАОУ ДО «ДЦК», ни при каких обстоятельствах, не подлежит пересылке третьим лицам по электронной почте. Пересылка информации, содержащей персональные данные, возможна только при условии использования систем защиты и шифрования таких данных.

5.23. Сотрудники МАОУ ДО «ДЦК» для обмена документами должны использовать только свой официальный адрес электронной почты. Использование сотрудниками МАОУ ДО «ДЦК» публичных почтовых ящиков электронной почты осуществляется только при согласовании с администрацией МАОУ ДО «ДЦК».

5.24. 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. Отправитель электронного сообщения, документа или лицо, которое его переадресовывает, должен указать свое имя и фамилию и тему сообщения.

5.24. Не допускается при использования электронной почты:

- рассылка сообщений личного характера;
- рассылка рекламных материалов;
- 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.

5.25. 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.

5.26. В случае кражи переносного компьютера следует незамедлительно сообщить администрации МАОУ ДО «ДЦК».

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

- проинформировать администрацию МАОУ ДО «ДЦК» и техника;
- не пользоваться и не включать зараженный компьютер;
- не подсоединять этот компьютер к компьютерной сети МАОУ ДО «ДЦК» до тех пор, пока на нем не будет произведено удаление обнаруженного вируса и полное антивирусное сканирование.

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

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

6. Управление информационной безопасностью

6.1. Управление ИБ МАОУ ДО «ДЦК» 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.

7. Контроль за соблюдением политики информационной безопасности

7.1. Текущий контроль за соблюдением выполнения требований Политики информационной безопасности МАОУ ДО «ДЦК» осуществляет директор.

7.2. Директор МАОУ ДО «ДЦК» на регулярной основе рассматривает реализацию и соблюдение отдельных положений Политики информационной безопасности, а также осуществляет последующий контроль за соблюдением ее требований.