УТВЕРЖДАЮ
Директор МБОУДО ДЮЦ
_____ Г.Е. Агапитова
«24» декабря 2017 г.

Политика информационной безопасности Муниципального бюджетного образовательного учреждения дополнительного образования ДЕТСКО-ЮНОШЕСКИЙ ЦЕНТР

1. Общие положения

1.1.Политика информационной безопасности МБОУДО ДЮЦ (далее – Политика) 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 МБОУДО ДЮЦ при осуществлении своей деятельности.

1.2.Основной целью Политики информационной безопасности МБОУДО ДЮЦ является защита информации МБОУДО ДЮЦ 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 июля 2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите и информации», Федеральным закон от 27 июля 2006г. № 152-ФЗ «О персональных данных», Федеральным закон от 10 января 2002г. № 1-ФЗ «Об электронной цифровой подписи», Указом Президента Российской Федерации от 6 марта 1997г. № 188 «Об утверждении Перечня сведений конфиденциального характера», Постановлением Правительства РФ №781 от 17.11.07г. «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», Постановление Правительства РФ №687 от 15.09.08г. «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 структурных подразделений МБОУДО ДЮЦ.

1.5.Ответственность за соблюдение информационной безопасности несет каждый сотрудник МБОУДО ДЮЦ. 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 МБОУДО ДЮЦ;

-защита целостности информации с целью поддержания возможности МБОУДО ДЮЦ по оказанию услуг высокого качества и принятию эффективных управленческих решений;

-повышение осведомленности пользователей в области рисков, связанных с информационными ресурсами МБОУДО ДЮЦ;

-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:

-контроль выполнения установленных требований по обеспечению ИБ;

-повышение эффективности, непрерывности, контролируемости мероприятий по обеспечению и поддержанию ИБ;

-разработка нормативных документов для обеспечения ИБ МБОУДО ДЮЦ;

-выявление, оценка, прогнозирование и предотвращение реализации угроз ИБ МБОУДО ДЮЦ;

-организация антивирусной защиты информационных ресурсов МБОУДО ДЮЦ;

-защита информации МБОУДО ДЮЦ от несанкционированного доступа и утечки по техническим каналам связи;

- организация периодической проверки соблюдения информационной безопасности.

3. Концептуальная схема обеспечения информационной безопасности

3.1.Политика ИБ МБОУДО ДЮЦ 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 МБОУДО ДЮЦ, 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.Стратегия обеспечения ИБ МБОУДО ДЮЦ 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 МБОУДО ДЮЦ.

4.Объекты защиты

4.1.Объектами защиты с точки зрения ИБ в управлении являются:

-информационный процесс профессиональной деятельности;

-информационная система учёта обучающихся МБОУДО ДЮЦ.

4.2.Защищаемая информация делится на следующие виды:

- информация по финансово-экономической деятельности МБОУДО ДЮЦ;

- 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. Все работы в пределах МБОУДО ДЮЦ должны выполняться в соответствии с официальными должностными обязанностями только на компьютерах, разрешенных к использованию.

5.2.Руководители структурных подразделений должны периодически пересматривать права доступа своих сотрудников и других пользователей к соответствующим информационным ресурсам.

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

5.4.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.

5.5.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.

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

Рекомендованные правила:

- сотрудникам МБОУДО ДЮЦ 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 МБОУДО ДЮЦ перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов;
- запрещен доступ в Интернет через сеть МБОУДО ДЮЦ для всех лиц, не являющихся сотрудниками МБОУДО ДЮЦ.

5.7. Сотрудники МБОУДО ДЮЦ должны постоянно помнить о необходимости обеспечения физической безопасности оборудования, на котором хранится информация.

5.8.Сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения производит техник МБОУДО ДЮЦ.

5.9.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 МБОУДО ДЮЦ, является ее собственностью и предназначено для использования исключительно в производственных целях.

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

5.11.Все компьютеры, содержащие конфиденциальную информацию, должны защищаться паролем при загрузке системы, активации по горячей клавиши и после выхода из режима "Экранной заставки". 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.

5.12.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.

5.13.Все программное обеспечение, установленное на предоставленном МБОУДО ДЮЦ компьютерном оборудовании, является собственностью МБОУДО ДЮЦ и должно использоваться исключительно в производственных целях.

5.14.На всех портативных компьютерах должны быть установлены антивирусные программы, необходимые для обеспечения защиты информации.

5.15.Сотрудники МБОУДО ДЮЦ не должны:

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

5.16.Электронные сообщения должны строго соответствовать стандартам в области деловой этики. Использование электронной почты в личных целях не допускается.

Сотрудникам запрещается направлять конфиденциальную информацию МБОУДО ДЮЦ по электронной почте без использования систем шифрования. Строго конфиденциальная информация МБОУДО ДЮЦ, ни при каких обстоятельствах, не подлежит пересылке третьим лицам по электронной почте.

5.17.Сотрудники МБОУДО ДЮЦ для обмена документами должны использовать только свой официальный адрес электронной почты.

5.18.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.

5.19.В случае кражи переносного компьютера следует незамедлительно сообщить администратору и/или директору МБОУДО ДЮЦ.

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

-проинформировать техника;

- не использовать и не включать зараженный компьютер;

-не подсоединять этот компьютер к компьютерной сети МБОУДО ДЮЦ до тех пор, пока на нем не будет произведено удаление обнаруженного вируса и полное антивирусное сканирование техником.

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

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

6.Управление информационной безопасностью

7.1.Управление ИБ МБОУДО ДЮЦ 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.