Рассмотрено на заседании
Педагогического совета
Протокол № 1 от 23.07.2020

«УТВЕРЖДАЮ»
Директор МБУ ДО «ДЮСШ»
_____Ф.Н.Сафин
Приказ № 47 от 23.07.2021 г.

ПОЛОЖЕНИЕ
по информационной безопасности
МБУ ДО «Детско-юношеская спортивная школа»
Юргинского муниципального округа

1. Общие положения

1.1. Положение по информационной безопасности муниципального бюджетного учреждения дополнительного образования «Детско-юношеская спортивная школа» Юргинского муниципального округа (далее - Учреждение) определяет цели и задачи системы обеспечения информационной безопасности и устанавливает совокупность правил, практических приемов и требований в области информационной безопасности, которыми руководствуются работники Учреждения.

1.2. Основной целью информационной безопасности Учреждения является защита информации учреждения 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. Положение по информационной безопасности разработано в соответствии с: Федеральным законом от 27 июля 2006 № 149-ФЗ «Об информации, информационных технологиях и о защите и информации», Федеральным законом от 27 июля 2006 № 152-ФЗ «О персональных данных», Постановлением Правительства РФ №781 от 17.11.2007 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», а также рядом иных нормативных правовых актов в сфере защиты информации.

1.4. Информационная безопасность Учреждения направлена на защиту информационных ресурсов от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий сотрудников, неправильных технологических и организационных решений в процессах поиска, сбора хранения, обработки, предоставления и распространения информации и обеспечение эффективного и бесперебойного процесса деятельности.

1.5. Выполнение требований данного Положения является обязательным для всех сотрудников Учреждения.

1.6. Ответственность за соблюдение информационной безопасности несет каждый сотрудник Учреждения.

2. Цель и задачи информационной безопасности

2.1. Основной целью информационной безопасности Учреждения является: повышение уровня эффективности, непрерывности, контролируемости мер по защите

отреальных угроз информационной безопасности.

2.2. Основными задачами информационной безопасности являются:

- разработка требований по обеспечению информационной безопасности;
- контроль выполнения установленных требований по обеспечению информационнойбезопасности;
- разработка нормативных документов для обеспечения информационной безопасности;
- защита информации Учреждения от несанкционированного доступа и утечки по техническимканалам связи.

3. Основные принципы обеспечения информационной безопасности

3.1. Основными принципами обеспечения информационной безопасности Учреждения являются:

- своевременное обнаружение проблем, потенциально способных повлиять на информационную безопасность;
- разработка и внедрение защитных мер;
- персонификация и разделение ответственности между сотрудниками Учреждения за обеспечение информационной безопасности исходит из принципа персональной ответственности за совершаемые операции.

4.Объекты защиты

4.1. Объектами защиты с точки зрения информационной безопасности Учреждения являются: информационный процесс профессиональной деятельности; информационные активы учреждения.

4.2. Защищаемая информация делится на следующие виды:

- информация по финансово-экономической деятельности;
- 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 Учреждения, активов, находящихся под контролем Учреждения, а также активов, используемых для получения доступа к инфраструктуре Учреждения, должна быть определена ответственность соответствующего сотрудника (ов).

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

5.3. 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.

5.4. Каждый сотрудник обязан немедленно уведомить администрацию обо всех случаях предоставления доступа третьим лицам к информационным системам Учреждения. Доступ третьих лиц к информационным системам должен быть

обусловлен производственной необходимостью.

5.5. Правила использования сети Интернет в Учреждении:

- сотрудникам разрешается использовать сеть Интернет только в служебных целях;
- сотрудники обязаны соблюдать требования законодательства Российской Федерации об информации, информационных технологиях и о защите информации;
- сотрудники не должны использовать сеть Интернет для хранения корпоративных данных;
- работа сотрудников с Интернет-ресурсами допускается только в режиме просмотра информации, исключая возможность передачи информации Учреждения в сеть Интернет;
- сотрудники перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов;
- запрещен доступ в Интернет через сеть Учреждения для всех лиц, не являющихся сотрудниками, включая членов семьи сотрудников.

5.6. Все программное обеспечение, установленное на предоставленном Учреждением компьютерном оборудовании, является собственностью Учреждения и должно использоваться исключительно в служебных целях.

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

5.8. Все компьютеры Учреждения должны быть оснащены системой антивирусной защиты.

5.9. Сотрудники Учреждения не должны:

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

5.10. Электронные сообщения должны строго соответствовать стандартам в области деловой этики. Использование электронной почты в личных целях не допускается. Строго конфиденциальная информация Учреждения, ни при каких обстоятельствах, не подлежит пересылке третьим лицам по электронной почте.

5.11. Сотрудники Учреждения для обмена документами должны использовать только свойофициальный адрес электронной почты.

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

5.13. 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.

9. Порядок внесения изменений и дополнений в Положение по информационной безопасности

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

10. Контроль за соблюдением информационной безопасности

10.1. Текущий контроль за соблюдением выполнения требований Положения об информационной безопасности Учреждения возлагается на директора.