Утверждаю
Директор МБУ СШОР
«Велосипедный спорт»

_____ И.А. Архипова
«03» июня 20 17 г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ Муниципального бюджетного учреждения «Спортивная школа олимпийского резерва «Велосипедный спорт»

1. Общие положения

1.1. Политика информационной безопасности (далее – Политика) Муниципального бюджетного учреждения «Спортивная школа олимпийского резерва «Велосипедный спорт» (далее – Учреждение) является основополагающим документом, отражающим видение руководства Учреждения касательно обеспечения ИБ.

1.2. Политика Учреждения направлена на достижение следующих целей:

- защита информации от реальных и потенциальных угроз;
- минимизация и локализация последствий при воздействии угроз;
- развитие корпоративной культуры в области обеспечения ИБ.

1.3. Основными задачами Политики являются:

- выявление, предупреждение и нейтрализация реальных и потенциальных угроз ИБ, а также установление причин и условий их возникновения;
- совершенствование механизмов оперативного реагирования на угрозы ИБ;
- эффективное управление рисками ИБ;
- информирование и обучение работников Учреждения по вопросам ИБ.

2. Объекты защиты

2.1. Объектами защиты с точки зрения ИБ в Учреждении являются:

- информационный процесс профессиональной деятельности;
- информационные активы Учреждения.

2.2. Защищаемая информация делится на следующие виды:

- информация по финансово-экономической деятельности Учреждения;
- персональные данные;

– любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных;

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

1. Концептуальная схема обеспечения информационной безопасности

1.1. Защита информационных ресурсов в Учреждении, в общем виде, сводится:

– к исключению неправомерных или неосторожных действий со сведениями, относящимися к конфиденциальной и информации ограниченного распространения;

– к исключению материального, физического, морального или иного ущерба, нанесенного посредством случайного или преднамеренного воздействия на носители информации, процессы обработки и передачи.

2. Основные принципы деятельности в сфере обеспечения информационной безопасности

– Информационная безопасность в Учреждении осуществляется в соответствии со следующими основными принципами:

– законности;
– процессного подхода;
– комплексного использования способов, методов и средств защиты;
– следования лучшим практикам;
– разумной достаточности;
– персональной ответственности.

3. Меры, применяемые для обеспечения информационной безопасности

3.1. Стратегия обеспечения ИБ Учреждения заключается в использовании заранее разработанных мер, а также программно-технических и организационных решений, позволяющих свести к минимуму возможные потери от технических аварий и ошибочных действий работников Учреждения

3.2. В учреждении применяются следующие меры защиты:

– правовые (законодательные) - действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил;

– морально-этические - соблюдение моральных и этических норм поведения, которые традиционно сложились или складываются по мере распространения информационных технологий в обществе в целом и в Учреждении в частности, поддержание здорового морального климата в коллективе;

– технологические - технологические решения и приемы, направленные на уменьшение возможности совершения сотрудниками ошибок и нарушений в рамках предоставленных им прав и полномочий;

– организационные (административные) – документальная регламентация процессов функционирования системы обработки данных, использование ее ресурсов, деятельность обслуживающего персонала;

– физические - оснащение помещений замками, сейфами, окон – решетками, установка сигнализаций и домофона;

– технические (программные) – криптографическая защита документооборота, парольная защита, антивирусная защита.

4. Порядок подготовки персонала по вопросам информационной безопасности и допуска его к работе

4.1. Обучение работников Учреждения правилам обращения с конфиденциальной информацией, проводится путем:

– проведения инструктивных занятий с работниками, принимаемыми на работу в Учреждение;

– самостоятельного изучения работниками внутренних нормативных документов Учреждения.

4.2. Допуск персонала к работе с защищаемыми информационными ресурсами Учреждения осуществляется только после его ознакомления с соответствующими инструкциями. Согласие на соблюдение правил и требований подтверждается личной подписью работника.

5. Заключительные положения

5.1. Настоящая политика вступает в силу с момента ее утверждения директором Учреждения и действует без ограничения срока действия (до внесения соответствующих изменений).

5.2. Изменения в политику вносятся приказом директора Учреждения.

5.3. Актуализация Политики производится в обязательном порядке в следующих случаях:

– при изменении политики Российской Федерации в области информационной безопасности;

– при изменении внутренних нормативных документов (инструкций, положений, руководств), касающихся информационной безопасности Учреждения.

5.4. Политика признается утратившей силу в случаях:

– вступления в силу нового правового акта, регулирующего те же вопросы или содержащие те положения, которые содержатся в настоящей Политике (т.е. при фактической замене);

– противоречия настоящей Политики вследствие издания нового правового акта той же или большей юридической силы.

5.5. Контроль за соблюдением Политики осуществляет директор МБУ СШОР «Велосипедный спорт».