

Политика информационной безопасности

1. Настоящая политика определяет цели и принципы обеспечения информационной безопасности в краевом государственном бюджетном учреждении «Спортивная школа олимпийского резерва имени Б.Х. Сайтиева» (далее – Учреждение).

Настоящая политика применяется при работе с информацией Учреждения работниками Учреждения (далее – сотрудник) и иными лицами, в рамках заключенных договоров, контрактов, соглашений.

2. Под обеспечением информационной безопасности или защитой информации Учреждения понимается сохранение ее конфиденциальности, целостности и доступности.

Конфиденциальность информации Учреждения обеспечивается предоставлением доступа к данным только авторизованным лицам.

Целостность информации Учреждения обеспечивается внесением в данные исключительно авторизованных изменений.

Доступность информации Учреждения обеспечивается возможностью получения доступа к данным авторизованным лицам в нужное для них время.

3. Целями обеспечения информационной безопасности являются минимизация ущерба от реализации угроз информационной безопасности, улучшение деловой репутации и корпоративной культуры Учреждения.

4. Доступ к информации Учреждения предоставляется только лицам, которым он необходим для выполнения должностных или договорных (контрактных) обязательств в минимально возможном объеме.

5. Сотрудники Учреждения проходят регулярное обучение в области информационной безопасности.

6. Отдельные политики информационной безопасности утверждаются директором Учреждения.

7. Программист Учреждения отвечает за определение детальных требований информационной безопасности и контролирует их исполнение в Учреждении.

8. Меры защиты информации внедряются по результатам проведения оценки рисков информационной безопасности.

Оценка рисков информационной безопасности проводится не реже одного раза в три года, а также в случае значительных изменений в структуре Учреждения и его бизнес-процессах.

При оценке рисков учитывается влияние реализации угроз информационной безопасности на положение Учреждения в обществе и его репутацию.

Стоимость принимаемых мер не должна превышать возможный ущерб, возникающий при реализации угроз.

В настоящий момент для регулирования деятельности по технической защите информации в Учреждении используются следующие документы:

- Положение об обработке и защите персональных данных.
- Приказ № 112 от 16.11.2012 «О создании системы защиты персональных данных в КГБОУ ДОД «СДЮСШОР».
- Приказ № 75 от 21.05.2013 «Об организации работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных КГБОУ ДОД «СДЮСШОР».
- Инструкция администратора безопасности информационных систем персональных данных КГБОУ ДОД «СДЮСШОР».
- Инструкция пользователей информационных систем персональных данных КГБОУ ДОД «СДЮСШОР».
- Инструкция парольной защиты информационных систем персональных данных КГБОУ ДОД «СДЮСШОР».

- Организация порядка резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных КГБОУ ДОД «СДЮСШОР».
- Должностная инструкция ответственного за защиту информации.