Приложение 1
к политике информационной
безопасности ГБУ ДО СК
«Комплексная спортивная школа»

ПОЛОЖЕНИЕ

о доступе к информационным ресурсам

1. Назначение и область действия

1.1. Настоящее Положение о доступе к информационным ресурсам (далее – Положение) разработано во исполнение Федерального закона от 27 июля 2006 г. № 152 «О персональных данных», Федерального закона от 27 июля 2006 г. № 149 «Об информации, информационных технологиях и о защите информации», приказа Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащиеся в государственных информационных системах», приказа Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.2. Настоящее Положение определяет основные правила и требования по обеспечению информационной безопасности информационных ресурсов государственного бюджетного учреждения дополнительного образования Ставропольского края «Комплексная спортивная школа» (далее – учреждение) от любых форм неавторизованного доступа, использования и раскрытия информации.

1.3. Распространяется на всех работников и третьих лиц, использующих информационные ресурсы и системы учреждения. Является обязательным для исполнения.

2. Основные требования

2.1. Получение пользователями доступа к информационным ресурсам основывается на аутентификации этих пользователей и разграничении доступа.

2.2. В качестве объектов доступа рассматриваются информационные ресурсы учреждения, в отношении которых имеет права владения, распоряжения, пользования: данные (информация), технические средства, программные средства, услуги (сервисы) информационных систем. Для каждой информационной системы учреждения существует регламент.

2.3. Каждому пользователю назначается учетная запись, присваиваются, по возможности, единые для различных объектов доступа учреждения атрибуты информационной безопасности: уникальный идентификатор пользователя, права доступа – с учетом их важности и ценности для деятельности учреждения.

2.4. В учреждении могут применяться виды аутентификации, основанные на знании пользователем пароля (базовый вид аутентификации), на владении физическим носителем «секрета» (смарт-карты, криптографические токены). При необходимости может использоваться комбинация двух или более видов.

2.5. Пользователи уведомляются об обязанностях по обращению с «секретами» аутентификации и сроках истечения их действия. «Секреты», в свою очередь передаются пользователям способом, исключающим несанкционированное ознакомление с ними. Передача пользователем личного «секрета» другому лицу запрещена.

2.6. Назначение прав доступа определяется, исходя из служебных обязанностей пользователя.

2.7. Категорически запрещен доступ к ресурсам по принципу «Всем – Полный доступ». Запрещен также неавторизованный (анонимный, гостевой) доступ к любым ресурсам, кроме общедоступных страниц веб-сайта учреждения.

2.8. Пересмотр прав доступа осуществляется при возникновении производственной необходимости и документируется.

2.9. Управление доступом к сетевым информационным ресурсам и услугам производится, в том числе, путем разделения информационной телекоммуникационной системы учреждения на отдельные логические и физические сетевые сегменты.

2.10. В учреждении должны использоваться средства контроля над соблюдением правил доступа к объектам доступа.

2.11. Служебный доступ к объектам доступа учреждения, осуществляемый по внешним каналам связи, должен защищаться с применением механизмов аутентификации и криптографической защиты информации.

2.12. Доступ к общедоступным страницам веб-сайта учреждения не требует соблюдения требований пункта 2.11.

2.13. Для снижения вероятности угроз несанкционированного доступа, необходимо минимизировать число устройств, имеющих легальные внешние IP-адреса сети Интернет. Оборудование, имеющее легальные внешние IP-адреса сети Интернет, должно проверяться на наличие уязвимостей и автоматически получать обновления безопасности.

2.14. Объекты доступа учреждения должны быть защищены от внешних угроз из сети Интернет и из локальной сети сетевыми брандмауэрами и штатными средствами защиты, входящими в состав операционной системы и приложений. Число открытых для доступа сервисов и ресурсов на этих объектах должно быть минимально необходимым.

2.15. При увольнении работника обеспечивается невозможность его доступа к объектам доступа учреждения.

2.16. При нарушении требований данного Положения доступ пользователя к информационным ресурсам может быть временно заблокирован ответственными лицами (см. пункт 3.2) до устранения нарушения.

2.17. Порядок работы с информационными ресурсами, содержащими сведения, отнесенные к персональным данным, защита которых организуется в соответствии с требованиями законодательства РФ, определяется соответствующими внутренними документами учреждения. Разработка и утверждение этих документов производится вне настоящего Положения.

3. Роли и ответственность

3.1. Ответственность за соблюдение данного Положения возлагается на всех работников учреждения. Ответственность третьих лиц, использующих информационные ресурсы и системы учреждения, определяется соответствующими соглашениями и регламентами.

3.2. Ответственность за реализацию данного Положения возлагается на руководителей подразделений учреждения; работников, ответственных за администрирование сегментов информационной телекоммуникационной системы учреждения; работников, выполняющих следующие функции: администраторов информационных систем, администраторов по обеспечению безопасности информации.