Приложение № 9
к политике информационной безопасности
ГБУ ДО СК «Комплексная спортивная школа»

ПОЛОЖЕНИЕ

о физической защите информационных ресурсов

1. Назначение и область действия

1.1. Положение о физической защите информационных ресурсов (далее – «Положение») разработано во исполнение Федерального закона от 27 июля 2006 года № 152 «О персональных данных», Федерального закона от 27 июля 2006 года № 149 «Об информации, информационных технологиях и о защите информации», приказа Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 № 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 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» и определяет основные правила и требования по обеспечению информационной безопасности ГБУ ДО СК «Комплексная спортивная школа» (далее – «Учреждение») от угроз, связанных с физическим воздействием на информационные ресурсы Учреждения.

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

2. Основные требования

2.1. Работники Учреждения и лица, работающие по договорам, должны постоянно помнить о необходимости обеспечения физической безопасности оборудования, на котором хранится, передаётся или обрабатывается информация Учреждения.

2.2. Оборудование, поддерживающее функционирование критичных информационных систем, должно быть установлено в отдельных помещениях. Помещения должны быть доступны только уполномоченному персоналу и защищены от преднамеренного или случайного повреждения.

2.3. Руководители подразделений Учреждения, а также назначенные ответственные лица должны быть осведомлены обо всех местах установки и хранения компьютерного оборудования.

2.4. Все места установки и хранения компьютерного оборудования должны быть защищены от воздействия окружающей среды и обеспечивать уровень физического доступа, соответствующий степени важности оборудования и хранящейся на нём информации.

2.5. Компьютерное оборудование Учреждения должно быть защищено от угроз, связанных с отказами и сбоями систем обеспечения.

2.6. Силовые и телекоммуникационные кабельные сети, по которым передаются данные или поддерживаются информационные услуги, должны быть защищены от перехвата информации и повреждения.

2.7. Конфиденциальную информацию и оборудование либо программное обеспечение, предназначенное для обработки или защиты конфиденциальной информации, разрешается выносить за пределы территории Учреждения только на основании соответствующего разрешения.

2.8. Должен существовать процесс предоставления и блокирования физического доступа к серверным комнатам, к центрам обработки или хранения данных.

2.9. При обеспечении безопасности оборудования, используемого вне места его постоянной эксплуатации, должны учитываться риски, связанные с работой вне помещений Учреждения.

2.10. При передаче (списании) оборудования, все носители информации должны быть проверены на предмет полного уничтожения содержащейся на них важной (конфиденциальной) информации и программного обеспечения с целью предотвращения возможности восстановления этой информации.

3. Реализация требований по физической защите информационных ресурсов.

Данные требования выполняются благодаря использованию следующих программно-технических средств и организационных мероприятий:

3.1. Порядок доступа в помещения, где разрешена обработка конфиденциальной информации, определен приложением к приказу директора ГБУ ДО СК «Комплексная спортивная школа» от «О некоторых мерах по регламентации организации обработки и защиты персональных данных»;

3.2. Порядок видеонаблюдения в учреждении определен положением о системе видеонаблюдения в ГБУ ДО СК «Комплексная спортивная школа», утвержденным приказом директора ГБУ ДО СК «Комплексная спортивная школа» от «О дополнительных мерах по организации работы системы безопасности в учреждении, в том числе – видеонаблюдения»;

3.3. Система контроля и управления доступом (далее – СКУД) представляет собой совокупность программно-аппаратных технических средств безопасности, имеющих целью ограничение и регистрацию входа-выхода

объектов (людей, транспорта) на заданной территории через «точки прохода»: двери, ворота и т.д.

3.4. СКУД включает в себя электронные считыватели информации с электронных карт и электромеханические замки.

3.5. В помещениях Учреждения в качестве средства по предотвращению несанкционированного доступа применяют опечатывание дверей. Флажковое устройство для опечатывания представляет собой чашку с двумя крепежными отверстиями и откидным цилиндрическим стержнем. Внутренняя часть чашки заполняется пластилином, на котором оставляется оттиск печати - пломбира. При попытке вскрытия объекта флажок откидывается, и оттиск печати нарушается, фиксируя о несанкционированном вскрытии объекта.

3.6. Система охранно-пожарной сигнализации (далее - ОПС) представляет собой технический комплекс для обнаружения тревожного события и формирования соответствующих оповещений.

3.7. Алгоритм работы ОПС содержит несколько этапов:

– обнаружение фактора, сопутствующего несанкционированному проникновению на объект (охранная составляющая системы – ОС) или возгоранию (пожарная составляющая – ПС);

– передача информации на управляющий прибор;

– включение светозвуковых оповещателей, передача информации на пульт.

Объект не принимается под охрану, если на нем имеется нарушение целостности окон, дверных запоров, системы сигнализации и другие нарушения, ведущие к ослаблению надежной охраны.

4. Права и обязанности

4.1. Сотрудник обязан:

– использовать только свой электронный считыватель при входе в помещения, оборудованные СКУД;

– бережно относиться к оборудованию СКУД и электронному считывателю;

– немедленно сообщить администратору информационной безопасности в случае утери электронного считывателя;

– соблюдать правила по использованию СКУД.

4.2. Сотруднику запрещается:

– передавать личный электронный считыватель в пользование другим лицам;

– пользоваться электронным считывателем другого лица;

– скрывать факт утраты электронного считывателя;

– оставлять объект с неисправной сигнализацией, а также, не убедившись в том, что объект под охрану сдан;

– заставлять или закрывать извещатели объемного обнаружения;

– допускать к ремонту и профилактическому осмотру средств ОПС лиц, не уполномоченных на это;

– принимать средства ОПС от монтажной организации без участия представителей службы охраны и обслуживающей организации;

– в случае утери ключей от входных дверей и т. п. срочно поставить в известность охрану и принять меры по смене замков.

– разбирать или ломать личный электронный считыватель.

Лица, ответственные за сдачу под охрану и снятие с охраны системы сигнализации, должны соблюдать при сдаче объекта следующий порядок:

– закрыть все окна, форточки, двери и т. д. на шпингалеты, засовы и др.;

– проверить целостность шлейфа сигнализации в местах, доступных для посторонних лиц, убедиться, что все извещатели объемного, звукового, оптико-электронного действия не закрыты какими-либо предметами в зоне его действия;

– закрыть дверь кабинета и опечатать ее;

– расписаться в журнале вскрытия и сдачи помещений под охрану.

Ответственные за внутриобъектовый и пропускной режим, пожарную безопасность должны быть назначены приказом директора Учреждения.

Сотрудники Учреждения обязаны в случае выявления каких-либо неисправностей или изменений охранно-пожарной, тревожной сигнализации немедленно сообщить об этом службе охраны или руководству Учреждения.

Учреждение имеет право принимать меры дисциплинарного характера к сотрудникам, нарушающим положения настоящей политики.

5. Роли и ответственность

5.1. Ответственность за соблюдение данного Положения возлагается на всех работников Учреждения и третьих лиц, использующих информационные ресурсы и системы Учреждения.

5.2. Ответственность за реализацию и контроль исполнения данного Положения возлагается на администратора информационной безопасности; руководителей подразделений Учреждения; работников, участвующих в реализации пропускного режима; работников, ответственных за администрирование сегментов информационно - телекоммуникационной системы Учреждения; работников, выполняющих функции: администраторов информационных систем, администраторов локальной вычислительной сети, администраторов по обеспечению безопасности информации.

Приложение 10
к политике информационной
безопасности ГБУ ДО СК
«Комплексная спортивная школа»

ПОЛОЖЕНИЕ
по действиям пользователей информационных систем в нештатных ситуациях.

1. Общие положения

1.1. Данное положение определяет порядок действий пользователя при возникновении нештатной ситуации при работе с информационной системой (далее – ИС) разработано во исполнение Федерального закона от 27 июля 2006 года № 149 «Об информации, информационных технологиях и о защите информации», приказа Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащиеся в государственных информационных системах» и по реагированию на нештатные ситуации, связанные с работой в ИС. Пользователем ИС (далее – Пользователь) является сотрудник учреждения, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИС для выполнения своих должностных обязанностей. Пользователь в своей работе руководствуется, кроме должностных и технологических инструкций, действующими нормативными, организационно-распорядительными документами по вопросам информационной безопасности.

1.2. Положения инструкции обязательны для исполнения всеми пользователями и доводятся до сотрудников под подпись.

1.3. В настоящем документе под аварийной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИС, предоставляемых пользователям ИС. Аварийная ситуация становится возможной в результате реализации одной из угроз:

– технологические угрозы: пожар в здании; повреждение водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения); взрыв (бытовой газ, теракт, взрывчатые вещества или приборы, работающие под давлением); химический выброс в атмосферу;

– внешние угрозы: массовые беспорядки; сбои общественного транспорта; эпидемия; массовое отравление персонала; стихийные бедствия; удар молнии; сильный снегопад; сильные морозы; просадка грунта (подмыв грунтовых вод, подземные работы) с частичным обрушением здания; затопление водой в период паводка; наводнение, вызванное проливным дождем; торнадо; подтопление здания (воздействие подпочвенных вод,

вызванное внезапным и непредвиденным повышением уровня грунтовых вод);

– телекоммуникационные и ИТ угрозы: сбой системы кондиционирования; сбой ИТ – систем; угроза, связанная с человеческим фактором; ошибка персонала, имеющего доступ к серверной; нарушение конфиденциальности, целостности и доступности конфиденциальной информации;

– угрозы, связанные с внешними поставщиками: отключение электроэнергии; сбой в работе интернет-провайдера; физически разрыв внешних каналов связи.

2. Общий порядок действий при возникновении нештатных ситуаций

2.1. К нештатным ситуациям относятся следующие ситуации:

– сбой в работе программного обеспечения («зависание» компьютера, медленная скорость работы программы, ошибки в работе программы и т. п.);

– отключение электричества;

– сбой в локальной вычислительной сети (отсутствие доступа в локальную сеть, отсутствие доступа в интернет, отсутствие связи с сервером и т. п.);

– выход из строя сервера;

– потеря данных (отсутствие возможности сохранить внесенные данные, отсутствие связи с сервером, повреждение файлов и т. п.);

– обнаружен вирус;

– обнаружена утечка информации (взлом учетной записи пользователя, обнаружение посторонних устройств в системном блоке, обнаружена попытка распечатывания или сканирования документов на принтере и т. п.);

– взлом системы (web-сервера, файл-сервера и др.) или несанкционированный доступ;

– попытка несанкционированного доступа (обнаружены попытки подбора пароля, доступ постороннего лица в помещение и т. п.);

– компрометация ключей (утеря носителя ключевой информации (Rutoken, E-token и т. п.),

– несанкционированный доступ постороннего лица в помещение физического хранения носителя информации, к устройству хранения информации; визуальный осмотр носителя информации посторонним лицом или подозрение, что данные факты имели место; взлом учётной записи пользователя);

– компрометация пароля (взлом учетной записи пользователя, визуальный осмотр посторонним лицом клавиатуры при вводе пароля пользователем и т. п.);

– физическое повреждение ЛВС или ПЭВМ (не включается ПК, при попытке включения отображается синий или черный экраны, повреждены провода и т. п.);

– стихийное бедствие;

– иные нештатные ситуации, не включенные в данный список, но влекущие за собой повреждение элементов ИС и возможность потери защищаемой информации, и названные таковыми пользователем ИС или администратором безопасности ИС.

2.2. При возникновении любой нештатной ситуации во время работы сотрудник, обнаруживший нештатную ситуацию, немедленно ставит в известность специалиста по защите информации. Администратор безопасности проводит предварительный анализ ситуации и, в случае невозможности исправить положение, действует в соответствии с приложением к положению о реагировании на инциденты информационной безопасности; при необходимости, проводится служебное расследование по факту возникновения нештатной ситуации и выяснению ее причин.

2.3. При обнаружении вируса производится локализация вируса с целью предотвращения его дальнейшего распространения, для чего следует физически отсоединить «зараженный» компьютер от ЛВС и провести анализ состояния компьютера. Анализ проводится компетентным в этой области сотрудником. Результатом анализа может быть попытка сохранения (спасения данных), так как после перезагрузки ЭВМ данные могут быть уже потеряны. После успешной ликвидации вируса, сохраненные данные также необходимо подвергнуть проверке на наличие вируса. При обнаружении вируса следует руководствоваться «Инструкцией по организации антивирусной защиты», инструкцией по эксплуатации применяемого антивирусного ПО. После ликвидации вируса необходимо провести внеочередную антивирусную проверку на всех ЭВМ учреждения с применением обновленных антивирусных баз. При необходимости производится восстановление ПО и данных из резервных копий. Проводится служебное расследование по факту появления вируса в ЭВМ (ЛВС).

2.4. При обнаружении утечки информации проводится служебное расследование. Если утечка информации произошла по техническим причинам, проводится внеочередной анализ защищенности системы и, если необходимо, принимаются меры по устранению уязвимостей и предотвращению их возникновения.

2.5. При попытке НСД проводится анализ ситуации на основе информации журналов регистрации попыток НСД и предыдущих попыток НСД (данный журнал ведется автоматизированным способом средствами защиты информации от несанкционированного доступа). По результатам анализа, в случае необходимости, принимаются меры по предотвращению НСД, если есть реальная угроза НСД. Так же проводится внеплановую смену паролей. В случае появления обновлений ПО, устраняющих уязвимости системы безопасности, следует применить такие обновления.

2.6. При компрометации ключей следует руководствоваться инструкциями к применяемой системе криптозащиты.

2.7. При компрометации пароля необходимо немедленно сменить пароль, проанализировать ситуацию на наличие последствий компрометации и принять необходимые меры по минимизации возможного (или нанесенного) ущерба (блокирование счетов пользователей и т. д.). При необходимости, проводится служебное расследование.

2.8. Физическое повреждение ЛВС или ПЭВМ. Определяется причина повреждения ЛВС или ПЭВМ и возможные угрозы безопасности информации. В случае возникновения подозрения на целенаправленный вывод оборудования из строя проводится служебное расследование. Проводится проверка ПО на наличие вредоносных программ-закладок, целостность ПО и данных. Проводится анализ электронных журналов. При необходимости проводятся меры по восстановлению ПО и данных из резервных копий.

2.9. При возникновении стихийных бедствий следует руководствоваться документами, регламентирующими поведение в чрезвычайных ситуациях, принятых в учреждении.

Приложение № 11
к политике информационной безопасности
ГБУ ДО СК «Комплексная спортивная школа»

Перечень
сведений конфиденциального характера
ГБУ ДО СК «Комплексная спортивная школа»

1. Общие положения.

1.1. Перечень сведений конфиденциального характера ГБУ ДО СК «Комплексная спортивная школа» (далее – Перечень) разработан в соответствии с Федеральным законом «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ и Указом Президента РФ от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера» с целью регламентирования работы и определения степени ограничения при использовании информации конфиденциального характера в ГБУ ДО СК «Комплексная спортивная школа» (далее – учреждение).

1.2. Перечень устанавливает ограничения при передаче и распространении сведений, содержащихся в документах, массивах документов, независимо от носителя информации, в целом по учреждению и является руководящим документом при определении исполнителями, допущенными к работе со сведениями конфиденциального характера, грифа ограничения при передаче и распространении разрабатываемых документов.

1.3. Перечень содержит сведения, распространение которых может нанести ущерб интересам учреждения или сторонним организациям, осуществляющим с ним взаимодействие, поэтому они:

- не подлежат передаче по открытым каналам передачи данных и в открытой переписке без принятия мер защиты;
- не сообщаются в личных и деловых переговорах по открытым каналам связи;
- не публикуются в средствах массовой информации до принятия решения об ее опубликовании.

1.4. Категории сведений и сведения, включенные в настоящий Перечень, относятся к сведениям конфиденциального характера и делятся на:

- сведения, содержащие персональные данные;
- служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна);

- сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее).

- сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).

- сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

1.5. Перечень может дополняться и изменяться решением директора учреждения по представлению ходатайств начальников структурных подразделений и заместителей директора.

1.6. Должностные лица, виновные в нарушении установленных правил обращения с информацией конфиденциального характера несут административную, гражданско-правовую или дисциплинарную ответственность в соответствии с действующим законодательством.

2. Сведения конфиденциального характера учреждения

2.1. К категории «служебные сведения» в учреждении относятся:

2.1.1. Сведения о физической и информационной безопасности:

- сведения о порядке и состоянии организации охраны, пропускном режиме, системе сигнализации;
- сведения о целях, результатах, фактах проведения аудиторских и иных проверок;
- сведения о персонале учреждения, в т. ч. о его моральных и деловых качествах;
- сведения о средствах, способах защиты информации конфиденциального характера и методах контроля ее эффективности;
- документация, содержащая сведения по защите информации конфиденциального характера;
- сведения, раскрывающие организацию системы защиты информации конфиденциального характера (общее описание, структура и режимы функционирования), в том числе в части применяемых средств защиты информации при передаче информации конфиденциального характера по отрытым телекоммуникационным каналам связи;

- сведения, содержащие описание структуры локальных вычислительных сетей, полномочий пользователей, обрабатывающих информацию конфиденциального характера;

- сведения по средствам криптографической защиты информации;

- идентификационные и аутентификационные данные пользователей (системные и пользовательские логины и пароли);

- сведения, полученные при выполнении совместных работ с другими организациями, содержащие информацию конфиденциального характера этих организаций;

- сведения о порядке передачи информации конфиденциального характера другим организациям;

- сведения о закрытых ключах шифрования и электронной подписи;

- сведения о фактах ведения переговоров, предметах и целях совещаний и заседаний по защите конфиденциальной информации и сторонних участников, итоговые протоколы (решения).

2.1.2. Сведения сторонних организаций, которые стали известны учреждению в рамках достижения целей и исполнения функций учреждения, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами.

2.1.3. Сведения о финансовой деятельности:

- сведения о бухгалтерском учете (за исключением годового баланса);

- сведения о финансовых операциях;

- сведения о величине доходов и расходов (за исключением годового баланса).

2.1.4. Сведения о проведении открытых конкурсов в электронном виде либо электронных аукционов:

- сведения об участниках, подавших заявки на участие в открытых конкурсах в электронном виде, либо в электронных аукционах;

- сведения, содержащиеся в заявках на участие в открытых конкурсах в электронном виде, либо в электронных аукционах.

2.2. К категории «персональные данные» в учреждении относятся сведения, необходимые для выполнения цели заключения и регулирования трудовых отношений, Учреждением обрабатываются ПДн работников Учреждения и их ближайших родственников:

фамилия, имя, отчество, пол, возраст, дата и место рождения, паспортные данные, адрес регистрации по месту жительства и адрес фактического проживания, номер телефона (домашний, мобильный), данные документов об образовании, квалификации, профессиональной подготовке, сведения о повышении квалификации, семейное положение, сведения о составе семьи, которые могут понадобиться работодателю для предоставления работнику льгот, предусмотренных трудовым и налоговым законодательством, отношение к воинской обязанности, сведения о трудовом

стаже, предыдущих местах работы, доходах с предыдущих мест работы, СНИЛС, ИНН, информация о приеме, переводе, увольнении и иных событиях, относящихся к трудовой деятельности в ГБУ ДО СК «Комплексная спортивная школа», сведения о доходах в ГБУ ДО СК «Комплексная спортивная школа», сведения о деловых и иных личных качествах, носящих оценочный характер.