Приложение 5
к политике информационной
безопасности ГБУ ДО СК «Комплексная
спортивная школа»

ПОЛОЖЕНИЕ
по организации парольной защиты информационных ресурсов

1. Общие сведения

1.1 Положение по организации парольной защиты информационных ресурсов государственного бюджетного учреждения дополнительного образования Ставропольского края «Комплексная спортивная школа» (далее – Положение) разработано в целях выполнения требований информационной безопасности, включая требования 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» и регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) во всех информационных ресурсах (далее – ИР) государственного бюджетного учреждения дополнительного образования Ставропольского края «Комплексная спортивная школа» (далее – учреждение), а также контроль за действиями пользователей и администраторов ИР при работе с паролями.

1.2 Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех ИР и контроль действий при работе с паролями возлагается на администратора информационной безопасности учреждения (далее – администратор ИБ).

1.3 Требования настоящего Положения распространяются на всех сотрудников учреждения.

1.4 Бесконтрольность в определении и использовании паролей может повлечь риск несанкционированного доступа к ИР учреждения, повлечь мошеннические и другие действия с ИР, которые могут нанести материальный вред и ущерб репутации учреждения.

2. Требования к паролям

2.1 Пароли в учреждении должны выбираться сотрудниками самостоятельно с учетом следующих требований:

– длина пароля должна быть не менее 8 символов;

– пароль должен содержать символы в различных регистрах, а также цифры и/или специальные символы (!@#$%^&*()-_+=~[]{}|\:;'"<>,.?/);

– пароль не должен нести никакой смысловой нагрузки;

– пароль не должен содержать полностью или частично имени пользователя, текущего года, названия или номера месяца, фамилий, имён, отчеств и других персональных данных, надписей с техники на рабочем месте и т.п.;

– в случае подозрения на то, что пароль стал кому-либо известен, поменять пароль и сообщить о факте компрометации администратору ИБ;

– немедленно сообщить администратору ИБ в случае получения от кого-либо просьбы сообщить пароль;

– менять пароль, каждые 30 дней;

– не сообщать личный пароль никому.

2.2 Использование паролей в ИР должно удовлетворять требованиям политики информационной безопасности учреждения, утвержденной приказом директора учреждения.

3. Смена паролей

3.1 Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в месяц.

3.2 Внеплановая смена личного пароля или удаление учетной записи пользователя в случае прекращения его полномочий (увольнение, переход на другую работу внутри организации и т.п.) должна производиться администраторами ИР немедленно после окончания последнего сеанса работы данного пользователя с ИР.

3.3 Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри организации и другие обстоятельства) администраторов ИР и других сотрудников, которым по роду работы были предоставлены полномочия по управлению парольной защитой.

4. Хранение и контроль

4.1 Хранение сотрудником значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у администратора ИБ или у руководителя подразделения в опечатанном личной печатью пенале.

4.2 Повседневный контроль за действиями при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на руководителей подразделений, периодический контроль – возлагается на администратора ИБ.

4.3 В случае компрометации личного пароля пользователя должны быть немедленно предприняты меры по изменению пароля и выявлению последствий компрометации.

Приложение 6
к политике информационной
безопасности ГБУ ДО СК
«Комплексная спортивная школа»

ПОЛОЖЕНИЕ
об использовании программного обеспечения

1. Назначение и область действия

1.1. Настоящее Положение об использовании программного обеспечения (далее – Положение) разработано во исполнение Федерального закона от 27 июля 2006 г. № 149 «Об информации, информационных технологиях и о защите информации» определяет основные правила и требования по обеспечению информационной безопасности государственного бюджетного учреждения дополнительного образования Ставропольского края «Комплексная спортивная школа» (далее – учреждение) от угроз, связанных с использованием программного обеспечения (далее – ПО).

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

2. Основные требования

2.1. В учреждении разрешается использовать следующие виды ПО:

– ПО, разработанное в учреждении для обеспечения его деятельности;

– ПО, законно приобретенное или полученное учреждением на основании договорных или лицензионных соглашений с разработчиком либо правообладателем;

– «свободное» ПО, распространяемое с открытым исходным кодом (Open Source) либо под свободными лицензиями: GPL, LGPL, BSD, Apache и аналогичными;

– «бесплатное» ПО, лицензия на которое явно допускает его безвозмездное использование в корпоративной среде (в коммерческих целях, на служебных компьютерах, для выполнения должностных обязанностей и т.п.). При этом обязательно наличие текста такой лицензии на русском языке.

2.2. Доступ пользователей к системному и прикладному ПО должен быть санкционирован и разрешен непосредственным руководителем только для выполнения служебных обязанностей.

2.3. Пользователям запрещено:

– получать (приносить, скачивать), хранить, устанавливать и использовать нелицензионное программное обеспечение;

– использовать программное и аппаратное обеспечение учреждения в неслужебных (личных) целях;

– устанавливать и использовать программное обеспечение, которое не требуется им для выполнения должностных обязанностей.

2.4. Пользователи могут самостоятельно в пределах своих прав доступа устанавливать и обновлять необходимое для работы ПО на своих рабочих местах после согласования с руководством. При этом каждый пользователь несет персональную ответственность за ПО, установленное на его рабочей станции.

2.5. Оставлять бездействующие сеансы работы. Пользователь должен самостоятельно блокировать свой сеанс, отходя от компьютера.

2.6. Критичные обновления безопасности ПО подлежат обязательному распространению во всех информационных системах учреждения.

2.7. ПО, установленное или используемое в учреждении в нарушение настоящего Положения, может быть заблокировано или удалено ответственными лицами (см. пункт 3.2).

3. Роли и ответственность

3.1. Ответственность за соблюдение требований пунктов 2.1-2.5 данного Положения возлагается на всех сотрудников учреждения и третьих лиц, использующих в своей деятельности в учреждении программное обеспечение.

3.2. Ответственность за реализацию данного Положения возлагается на руководителей подразделений учреждения. Ответственность за обеспечение технической возможности выполнения требований разделов 2.1-2.5 и за соблюдение требований разделов 2.1-2.7 возлагается на: работников, ответственных за администрирование сегментов информационной телекоммуникационной системы учреждения; работников, выполняющих следующие функции: администраторов информационных систем, администраторов локальной вычислительной сети, администраторов по обеспечению безопасности информации.

Приложение №7
к политике информационной
безопасности ГБУ ДО СК
«Комплексная спортивная
школа»

ПОЛОЖЕНИЕ
о защите от вредоносного программного обеспечения

1. Общие положения

1.1.Положение о защите от вредоносного программного обеспечения (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 ФСТЭК от 11 февраля 2013 № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и определяет порядок применения средств подсистемы антивирусной защиты в ГБУ ДО СК «Комплексная спортивная школа» (далее – Учреждение), задачи, обязанности и права пользователей подсистемы антивирусной защиты, а также порядок ликвидации последствий воздействия программных вирусов.

1.2.Целью создания подсистемы антивирусной защиты в Учреждении является обеспечение защищенности информационных ресурсов от воздействия различного рода вредоносных программ и несанкционированных массовых почтовых рассылок, для обнаружения программных вирусов и восстановления/удаления заражённых (модифицированных) такими вирусами файлов, а также для предотвращения заражения (модификации) информационных ресурсов вредоносным кодом.

1.3.Настоящее Положение разработано в соответствии с действующим законодательством Российской Федерации в области защиты информации и направлена на нейтрализацию угроз безопасности информации, связанных с вирусной активностью в Учреждении.

1.4.Требования настоящего Положения являются неотъемлемой частью комплекса мер безопасности и защиты информации в Учреждении и распространяются на всех сотрудников Учреждения.

2. Основные термины, сокращения и определения

2.1.Автоматизированное рабочее место (далее – АРМ) – персональный компьютер с периферийным оборудованием и предустановленным программным обеспечением.

2.2.Антивирусная защита (далее АВЗ) – комплекс профилактических и диагностических мер, применяемых для защиты информационных систем от заражения вирусами.

2.3.Администратор антивирусной защиты информации (далее – администратор АВЗ) – должностное лицо, назначенное ответственным за эксплуатацию средств АВЗ в Учреждении и обеспечивающее организацию и эффективное использование системы антивирусной защиты информации.

2.4.Вредоносное программное обеспечение (далее – программный вирус) – вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи с целью нарушения работы программно-аппаратных комплексов, удаления файлов, приведения в негодность структур размещения данных, блокирования работы пользователей или же приведения в негодность аппаратных комплексов компьютера.

2.5.Исполняемый файл – файл, содержащий программу в виде, в котором она может быть исполнена компьютером.

2.6.Облачное хранилище – модель онлайн-хранилища, в котором данные хранятся на многочисленных распределённых в сети серверах, предоставляемых в пользование клиентам, в основном, третьей стороной.

2.7.Оперативная память – энергозависимая часть системы компьютерной памяти, в которой во время работы компьютера хранится выполняемый машинный код (программы), а также входные, выходные и промежуточные данные, обрабатываемые процессором.

2.8.Подсистема антивирусной защиты – это совокупность управленческих и правовых действий, программно-аппаратных средств, объединяемых в единый комплекс для создания надежной антивирусной защиты информационной базы, находящейся в локальной сети.

2.9.Пользователь автоматизированного рабочего места (далее – Пользователь) – сотрудник Учреждения, использующий данный персональный компьютер с периферийным оборудованием и предустановленным программным обеспечением для выполнения своих служебных обязанностей.

2.10. Программное обеспечение (далее – ПО) – программа или множество программ, используемых для управления компьютером.

2.11. Спам – массовая рассылка коммерческой и иной рекламы или подобных коммерческих видов сообщений лицам, не выражавшим желания их получать.

2.12. Средства антивирусной защиты информации (далее – средства АВЗ) – специализированные программные средства для обнаружения программных вирусов, а также нежелательных (считающихся вредоносными) программ вообще и восстановления заражённых (модифицированных) такими программами файлов, а также для профилактики – предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

2.13. Локальная вычислительная сеть (далее – ЛВС) — компьютерная вычислительная сеть, охватывающая небольшую территорию и

использующая ориентированные на эту территорию средства и методы передачи данных.

2.14. Съемные носители информации – любой материальный объект или среда передачи, способный достаточно длительное время сохранять (нести) в своей структуре занесённую в/на него информацию.

2.15. Центральный процессор (далее – ЦП) – электронный блок либо интегральная схема (микропроцессор), исполняющая машинные инструкции (код программ), главная часть аппаратного обеспечения компьютера или программируемого логического контроллера.

3. Права и обязанности пользователей подсистемы антивирусной защиты информации

3.1.При загрузке/включении компьютера удостовериться, что запущены средства АВЗ. В случае если средства АВЗ не запустились либо неактивны, немедленно сообщить об этом администратору АВЗ.

3.2.При использовании съемных носителей информации, осуществлять их проверку средствами АВЗ на предмет наличия вредоносного программного обеспечения. При выявлении зараженных файлов произвести их самостоятельное лечение средствами АВЗ, если же лечение невозможно, то удалить/поместить в карантин зараженные файлы. Немедленно сообщить администратору АВЗ о случившемся инциденте.

3.3.При обнаружении зараженных файлов на АРМ выполнить действия, предлагаемые средствами АВЗ (лечение/удаление/помещение в карантин) и немедленно сообщить администратору АВЗ о случившемся инциденте.

3.4.Пользователь не имеет права самостоятельно изменять политики средств АВЗ или отключать средства АВЗ, при возникновении такой необходимости, связанной с профессиональной деятельностью сотрудника, необходимо обратиться к администратору АВЗ.

3.5.При использовании корпоративной почты открывать письма и скачивать вложения разрешается только от заранее известных и/или доверенных адресатов. Запрещается:

3.6.скачивать и запускать исполняемые файлы с любых электронных адресов (при необходимости приема/передачи исполняемых файлов использовать другие средства обмена данными, к примеру, облачные хранилища, съемные носители информации и т.д.);

3.7.переходить по ссылкам, отправленным с неизвестных электронных адресов;

3.8.открывать любые вложения, отправленные с неизвестных электронных адресов.

3.9.Запрещено переходить по ссылкам, которые содержатся в электронных письмах, особенно если они длинные или наоборот, используют сервисы сокращения ссылок (bit.ly, tinyurl.com и т. д.).

3.10. Запрещено открывать вложения, особенно если в них содержатся документы с макросами, архивы с паролями, а также файлы с расширениями RTF, LNK, CHM, VHD.

3.11. Необходимо внимательно проверять адрес отправителя, даже в случае совпадения имени с уже известным контактом.

3.12. При использовании сети Интернет не переходить на сайты, не связанные с профессиональной деятельностью.

3.13. Администратор локальной сети назначается приказом руководителя организации. Запрещено устанавливать на АРМ права локального администратора сотрудникам Учреждения, которые не являются администраторами локальной сети.

3.14. Если на АРМ требуется переустановка ПО, то Пользователь обязан заранее сообщить об этом администратору АВЗ и администратору локальной сети.

3.15. Запрещается самостоятельно скачивать и устанавливать ПО из сети Интернет (либо расширения для имеющегося ПО), для этого обращайтесь к администратору локальной сети. Любое устанавливаемое ПО, издателя которого определить не представляется возможным, должно быть проверено средствами АВЗ на наличие программных вирусов.

3.16. Если же произошло заражение АРМ и не представляется возможным своевременное лечение/удаление/добавление в карантин зараженных файлов средствами АВЗ, то пользователь обязан:

3.17. отключить АРМ от ЛВС;

3.18. немедленно сообщить о заражении администратору АВЗ.

3.19. Если Пользователь заметил подозрительное поведение АРМ (необоснованно высокий уровень загрузки ЦП и/или оперативной памяти, сомнительный трафик, отправляемый АРМ в сеть, изменение расширений файлов, их недоступность либо исчезновение, длительное время отклика АРМ и т.д.), необходимо сообщить об этом администратору АВЗ.

3.20. В Учреждении используются только разрешенные съемные носители информации. Перечень разрешенных носителей информации составляется администратором АВЗ. В данный перечень могут быть внесены все съемные носители информации, которые используются для работы внутри Учреждения, без выноса данных носителей за пределы Учреждения. Каждый съемный носитель регистрируется специалистом по информационной безопасности и маркируется установленным порядком.

3.21. Информацию о всех фактах заражение АРМ Учреждения еженедельно представляется для ознакомления руководству Учреждения.

3.22. Администратор АВЗ и специалист по информационной безопасности Учреждения оставляют за собой право, обновлять и дополнять Инструкцию, заранее оповестив сотрудников Учреждения.