Муниципальное бюджетное учреждение дополнительного образования «Спортивная школа по киокусинкай»

140404, МО, Г.о. Коломна, ул. Девичье поле д.1, пом.1Б
8-496-618-32-36 Scool-Kyokushin@yandex.ru

27.04.2023 г **№ 49/2**

ПРИКАЗ

«Об утверждении средств защиты вычислительных средств, на которых осуществляется работа по обработке персональных данных спортсменов»

ПРИКАЗЫВАЮ:

1. Утвердить средства защиты вычислительных средств, на которых осуществляется работа с персональными данными спортсменов и законных представителей спортсменов (Приложение 1)
2. Контроль за исполнением настоящего приказа оставляю за собой.

Директор МБУ ДО
«СШ по киокусинкай» В.В. Фоменко

Приложение 1
К приказу от 27.04.2023г. №49/2

Введение

Данный документ содержит перечень требований по обеспечению информационной безопасности автоматизированных рабочих мест пользователей Системы. К рабочим местам пользователей системы относятся следующие автоматизированные рабочие места (далее – АРМ): АРМ сотрудника Организации.

Меры по обеспечению информационной безопасности сегментов Системы должны определяться Политикой информационной безопасности, разработанной в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и Постановления Правительства РФ от 01.11.2012 г. № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных".

Требования по организации работ по защите от НСД

Защита информации от НСД должна обеспечиваться на всех технологических этапах обработки информации, в том числе при проведении ремонтных и регламентных работ. Защита информации от НСД должна предусматривать контроль эффективности средств защиты от НСД. Этот контроль может быть либо периодическим, либо инициироваться по мере необходимости пользователем или администратором информационной безопасности. В организации, эксплуатирующей АРМ, должен быть назначен администратор информационной безопасности, на которого возлагаются задачи организации работ по использованию АРМ пользователя, выработки соответствующих инструкций для пользователей, а также контроль за соблюдением описанных ниже требований.

Требования по размещению технических средств

При размещении технических средств с установленным АРМ пользователей:

- должны быть приняты меры по исключению НСД в помещения, в которых размещены технические средства с установленным АРМ пользователя, посторонних лиц, по роду своей деятельности не являющихся персоналом, допущенным к работе в этих помещениях;

внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать исполнителям работ сохранность доверенных им персональных и статистических данных.

Требования по установке общесистемного и специального ПО

При установке ПО на АРМ пользователя необходимо соблюдать следующие требования:

1. На технических средствах, предназначенных для работы с АРМ пользователя, использовать только лицензионное ПО фирм-изготовителей.
2. Установку ПО АРМ пользователей необходимо производить только с зарегистрированного, защищенного от записи носителя.
3. На АРМ пользователя не должны устанавливаться средства разработки ПО и отладчики.
4. Предусмотреть меры, исключающие возможность несанкционированного необнаруживаемого изменения аппаратной части технических средств, на которых установлено ПО АРМ пользователя (например, путем опечатывания системного блока и разъемов АРМ пользователя).
5. Должны использоваться только сертифицированные СЗИ для защиты от НСД.
6. После завершения процесса установки должны быть выполнены действия, необходимые для осуществления периодического контроля целостности установленного ПО на АРМ пользователей.
7. ПО, устанавливаемое на АРМ пользователей, не должно содержать возможностей, позволяющих:

- модифицировать содержимое произвольных областей памяти;
- модифицировать собственный код и код других подпрограмм;
- модифицировать память, выделенную для других подпрограмм;
- передавать управление в область собственных данных и данных других подпрограмм;
- несанкционированно модифицировать файлы, содержащие исполняемые коды при их хранении на жестком диске;
- повышать предоставленные привилегии;
- модифицировать настройки ОС;
- использовать недокументированные фирмой-разработчиком функции ОС.

Требования по защите от НСД при эксплуатации АРМ

Для обеспечения защиты от НСД при эксплуатации АРМ пользователя необходимо учитывать следующие требования:

1. Должна быть предусмотрена система подтверждения легитимности пользователя при работе с АРМ:
   - аутентификацию – сопоставление предъявленных пользователем уникального идентификатора (логина) и соответствующего ему пароля с учетными записями зарегистрированных пользователей на АРМ;
   - авторизацию – сравнение набора прав, присвоенных учетной записи аутентифицированного пользователя с требуемыми для доступа к запрошенному ресурсу, функции, интерфейсу, информационному объекту.
2. Должны использоваться сертифицированные ФСТЭк СЗИ для защиты от НСД.
3. Должен быть предусмотрен механизм смены пароля для пользователей, при смене пароля в обязательном порядке должно запрашиваться его предыдущее значение.
4. При использовании механизма отсылки по электронной почте забытого пароля должна осуществляться проверка на соответствие учетной записи и электронного адреса.
5. Для снижения ошибочных действий пользователей должно быть разработано полное и доступное руководство пользователя.

Для обеспечения защиты АРМ от вредоносного кода должна использоваться сертифицированная программа для защиты от вирусов.

Требования к защите от вредоносного кода

Вредоносный код – любой программный код (компьютерный вирус, троян, сетевой червь), приводящий к нарушению функционирования средств вычислительной техники и/или предназначенный для искажения, модификации, уничтожения, блокирования или несанкционированного копирования информации.

Возможен следующий характер проявлений действий ВК:

- искажение изображения на экране монитора;
- искажение символов, вводимых с клавиатуры;
- блокирование клавиатуры, звуковые эффекты;
- стирание или порча отдельных частей диска или файлов;
- повреждение загрузочных секторов жесткого диска ПЭВМ;
- остановка загрузки или зависание компьютера, значительное замедление его работы;
- уничтожение или искажение информации о системной конфигурации АРМ пользователя.

ВК может попасть на компьютер со сменного носителя (CD-ROM, USB флэш-накопителей и других носителей, даже если эти носители не содержат файлов), при загрузке файлов из сети, с сообщением, полученным по электронной почте, а также через уязвимости операционных систем просто при наличии сетевого подключения компьютера к локальной вычислительной сети. Для защиты АРМ пользователя необходимо использовать сертифицированные антивирусные продукты. При наличии технической возможности, обновление средств защиты и сигнатурных баз должно производится централизованно, с рабочего места администратора программных средств.

В целях обеспечения защиты от воздействий вредоносного кода пользователю АРМ запрещается:

- самостоятельно устанавливать программное обеспечение, в том числе командные файлы;
- использовать при работе «зараженный» вредоносным кодом либо с подозрением на «заражение» носитель и/или файл;
- использовать личные носители на АРМ пользователя;
- самостоятельно проводить “лечение” носителя и/или файла;
- самостоятельно отключать, удалять и изменять настройки установленных средств защиты.

Пользователь АРМ обязан:

- проводить контроль на отсутствие ВК любых сменных и подключаемых носителей (CD-дисков, DVD-дисков, USB флэш-накопителей и т.п.) и файлов;
- входной контроль на отсутствие ВК компакт-дисков и DVD-дисков, предназначенных для одноразовой записи информации, проводит получатель (владелец) диска однократно с момента приобретения (получения) диска перед использованием его на компьютерах;

обращаться в службу поддержки пользователей системы или непосредственно к администратору.