Приложение № 17
к Приказу от 06.02.2018 г. № 19

ила подключения и взаимодействия с сетями общего пользования в вом сегменте «Информационной системы, содержащей сведения о возможностях дополнительного образования на территории Московской области»

1. Общие положения

1.1 Настоящие правила подключения и взаимодействия с сетями общего вания в типовом сегменте «Информационной системы, содержащей ия о возможностях дополнительного образования на территории вской области» (далее – информационная система или ЕИСДОП) няют порядок подключения и организации доступа к ресурсам и ам, к сетям общего пользования типа Интернет (далее – Сеть), а также правила взаимодействия и безопасного использования общедоступных мационных ресурсов сети.

1.2 Требования настоящих правил распространяются на всех ователей типового сегмента ЕИСДОП, использующих сети общего вания.

1.3 Доступ к ресурсам Сети предоставляется пользователям нительно в целях исполнения ими служебных обязанностей, включая информации, сбор данных, повышение квалификации и т.п.

1.4 Доступ к ресурсам Сети может быть заблокирован без варительного уведомления при возникновении нештатных ситуаций.

1.5 Установка и изменение конфигурации программного обеспечения, азначенного для взаимодействия с Сетью, должны выполняться по сованию с администратором информационной безопасности.

1.6 При обнаружении фактов использования, не рекомендованного аммного обеспечения, администратор информационной безопасности ен отключить рабочее место сотрудника от Сети, поставить об этом в ность непосредственного руководителя данного сотрудника.

2. Правила подключения к Сети

2.1. Подключение типового сегмента ЕИСДОП к Сети осуществляется по ению администратора информационной безопасности, на основании ветствующего обоснования.

2.2. Право подключения информационной системы к Сети, без льзования межсетевого экрана – запрещено.

2.3. Устанавливаемые межсетевые экраны должны соответствовать бованиям к межсетевым экранам, утверждённым приказом ФСТЭК России от

...раля 2016 г. № 9, по меньшей мере по 6 классу защиты межсетевых ...ов.

2.4 При подключении информационной системы к Сети рекомендуется:
- при предоставлении пользователям доступа к Сети исходить из принципа ...альной достаточности;
- использовать операционные системы со встроенными функциями ...ы информации от несанкционированного доступа или использовать ...ициированные решения;
- эффективно использовать имеющиеся в маршрутизаторах средства ...ничения доступа (фильтрацию), включающие контроль по списку доступа, ...ификацию пользователей, взаимную аутентификацию маршрутизаторов;
- осуществлять анализ принимаемой из Сети и передаваемой в Сеть ...мации на наличие "вирусов".

2.5 К работе в Сети допускаются пользователи, ознакомленные с ...щими правилами.

2.6 Контроль за выполнением мероприятий по обеспечению безопасности ...мации при подключении типового сегмента ЕИСДОП к Сети возлагается на ...нистратора информационной безопасности.

3. Правила взаимодействия с Сетью

3.1. Взаимодействие типового сегмента ЕИСДОП с Сетью осуществляется ...менением средств межсетевого экранирования. Любые подключения к ...в обход системы межсетевого экранирования не допускаются. Средства ...етевого экранирования должны быть сертифицированы по требованиям ...асности информации.

3.2. Пользователи типового сегмента ЕИСДОП не имеют права ...водить самостоятельную установку и модификацию указанного ...раммного обеспечения. Вся ответственность за использование не ...ендованного к использованию программного обеспечения ложится на ...ователя типового сегмента ЕИСДОП.

3.3. Пользователю типового сегмента ЕИСДОП запрещается:
- загружать файлы с неизвестных web или FTP сайтов;
- подключать служебный компьютер к внешним сетевым ресурсам с ...льзованием неслужебного канала связи в обход либо дополнительно к ...ствующему подключению;
- использовать публичные интернет-сервисы для хранения служебной ...рмации;
- использовать информационные ресурсы и сервисы международной сети ...рнет, находящиеся под запретом действующего законодательства и иных ...мативных актов Российской Федерации или запрещенных внутренними ...мативно-распорядительными документами;
- самостоятельно устанавливать и запускать загруженные из сети Интернет ...ые программы и исполняемые файлы;

-самостоятельно изменять любые системные и сетевые настройки и ройки установленных систем безопасности;

-допускать к работе на своем служебном компьютере посторонних лиц ступа в сеть Интернет;

-предпринимать в сети Интернет какие-либо действия и размещать либо информацию, способную ущемлять имущественные и щественные права третьих лиц, а также носящую оскорбительный тер или противоречащую действующему законодательству Российской рации;

-проводить сканирование и иные нештатные действия в отношении в информационной безопасности.

4. Ответственность

4.1. Ответственность за все действия в Сети, произведенные с ютера пользователя, им самим или другими лицами с использованием его ей записи, несет данный пользователь.

4.2. Ответственность за осуществление общего контроля выполнения ваний к защите информации при взаимодействии с сетью Интернет гается на администратора информационной безопасности ЕИСДОП.