УТВЕРЖДЕНА
приказом ГПОУ «УМК»
от 28.09.2016 № 62/а

ИНСТРУКЦИЯ

по информационной безопасности в сфере информационного обмена

Оглавление

1. Общие положения

1.1. Назначение документа

1.1.1. Инструкция по информационной безопасности в сфере информационного обмена определяет основные требования по организации работы с использованием сетей связи общего пользования и сетей международного информационного обмена, в том числе сети Интернет (далее – общедоступные сети) в информационных системах персональных данных (ИСПДн) ГПОУ «УМК» (далее – Учреждение).

1.1.2. Настоящая инструкция разработана в соответствии с Федеральным законом от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и защите информации», «Доктриной информационной безопасности Российской Федерации», утвержденной Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895, указом Президента от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» и других нормативных правовых актов в области защиты информации.

1.2. Область действия документа

1.2.1. Настоящая инструкция является руководящим документом по обеспечению безопасности межсетевого взаимодействия.

1.2.2. Настоящая инструкция предназначена для:

- лиц, назначенных приказом директора Учреждения в состав комиссии по защите персональных данных (далее – Комиссия);
- лица, ответственного за обеспечение функционирования ИСПДн (далее – администратор ИСПДн);
- лиц, допущенных к автоматизированной обработке персональных данных (ПДн) в ИСПДн (далее – пользователи ИСПДн).

1.2.3. Лица, указанные в п. 1.2.2 настоящей Инструкции должны быть с ней ознакомлены под подпись в Журнале учета ознакомлений с локальными нормативными актами, и предупреждены об ответственности за нарушение ее требований.

1.3. Вступление в силу документа

1.3.1. Настоящая инструкция вступает в силу с момента ее утверждения директором Учреждения.

1.3.2. Изменения в настоящую инструкцию вносятся приказом директора Учреждения.

2. Интернет

2.1. Интернет – всемирная компьютерная сеть, которая использует для взаимодействия стек протоколов TCP/IP (протокол управления передачи сообщений / Интернет протокол). Работа в Интернет осуществляется в режиме реального времени (online). Существует ряд

протоколов и служб, связанных с TCP/IP и Интернетом. Наиболее распространенными из них являются:

- SMTP – протокол приема-передачи электронной почты.
- TELNET – протокол для подключения к удаленным системам, присоединенным к общедоступным сетям в режиме удаленного терминала.
- FTP – протокол, предназначенный для передачи файлов с одного компьютера на другой в вычислительной сети.
- DNS – служба сетевых имен, используемых для протоколов TELNET, FTP и т. д.
- WWW – служба (всемирная паутина), использующая гипертекстовый формат HTML (язык разметки гипертекста), предназначенная для передачи тестовой, графической, аудио и видео информации, а также ссылок на другие документы (гипертекстовые ссылки – выделенные области документа, позволяющие переходить к другому документу, содержащему связанную информацию).

2.2. Помимо перечисленных, существует ряд служб и протоколов для удаленной печати, предоставления удаленного доступа к файлам и дискам, работы с распределенными базами данных и т.д.

2.3. Основная цель обеспечения информационной безопасности – предотвращение несанкционированного доступа, уничтожения, искажения, копирования, блокирования информации в компьютерных и телекоммуникационных системах.

3. Условия работы в общедоступных сетях

3.1. Подключение к общедоступным сетям

3.1.1. Подключение АРМ ИСПДн к общедоступным сетям должно быть реализовано только при служебной необходимости. В остальных случаях подключать АРМ ИСПДн к общедоступным сетям не рекомендуется.

3.1.2. Для защиты от нежелательного входящего трафика, а также для контроля исходящего, доступ АРМ ИСПДн к общедоступным сетям должен осуществляться через межсетевой экран (МЭ). Допускается использование персональных МЭ.

3.1.3. К использованию в ИСПДн допускаются только сертифицированные ФСТЭК России МЭ не ниже 5 класса.

3.2. Правила работы в общедоступных сетях

3.2.1. Передача ПДн через общедоступные сети (e-mail, ftp и др.) допускается только в зашифрованном с помощью средств криптографической защиты информации (СКЗИ) виде.

3.2.2. Содержание ресурсов общедоступных сетей, а также файлы, загружаемые из них, подлежат обязательному антивирусному контролю.

3.2.3. Информация о посещаемых пользователями ИСПДн ресурсах общедоступных сетей может протоколироваться для последующего анализа и, при необходимости, может быть представлена директору Учреждения для контроля.

4. Права и обязанности в сфере информационного обмена

4.1. Обязанности председателя Комиссии

4.1.1. Разработка структуры информационного обмена в локальной вычислительной сети (ЛВС) Учреждения и организация безопасного ее подключения к общедоступным сетям.

4.1.2. Разработка правил фильтрации пакетов, передаваемых (принимаемых) в (из) общедоступные(х) сети(ей).

4.1.3. Разработка списков доступных и запрещенных ресурсов общедоступных сетей.

4.1.4. Организация безопасных подключений к удаленным ресурсам (SSL, VPN и др.).

4.2. Обязанности администратора ИСПДн

4.2.1. Обеспечение безопасного доступа пользователей ИСПДн в общедоступные сети (настройка МЭ в соответствии с требованиями руководящих и нормативных документов ФСТЭК России, руководств по безопасной настройке от производителей МЭ, настоящей инструкции).

4.2.2. Организация маршрутизации в ЛВС и доступности TCP/UDP портов АРМ.

4.2.3. Поддержание актуальности баз антивирусных средств (АВС) на АРМ ИСПДн.

4.2.4. Настройка обозревателей пользователей ИСПДн и другого программного обеспечения (ПО) для работы в ЛВС и общедоступных сетях.

4.3. Обязанности пользователей ИСПДн

4.3.1. Пользователи ИСПДн обязаны знать и соблюдать требования настоящей инструкции и правила работы со средствами защиты информации (СЗИ), установленными в ИСПДн.

4.3.2. При наличии подозрительной активности в сети (предупреждения СЗИ, появление не закрываемых всплывающих окон, высоком трафике и т.д.) или при необычном поведении программных средств АРМ (проигрывании различных звуков, произвольной перезагрузке АРМ и т.д.) пользователи ИСПДн обязаны обращаться к администратору ИСПДн.

4.3.3. Пользователям ИСПДн запрещается:

- работать в общедоступных сетях при отключенных средствах защиты (АВС, МЭ);
- передавать ПДн субъектов ПДн через общедоступные сети (электронная почта, ftp, www, icq и др.), без использования СКЗИ;
- посещать сайты сомнительной репутации;
- использовать общедоступные сети в личных (просмотр, прослушивание, скачивание медиа и других файлов, посещение социальных сетей и т. д.) или коммерческих (игра на forex, в покер-online и т.д.) целях;
- открывать письма, пришедшие по электронной почте, с вложениями файлов с расширениями .exe, .pif, .corn, .scr, например: договор.exe, а также файлы, в именах которых присутствует второе расширение, например: договор.doc.pif. Данные письма необходимо удалять не читая;

- преднамеренно рассылать спам или компьютерные вирусы;
- распространять (публиковать) ПДн в общий доступ;
- распространять информацию, запрещенную действующим законодательством РФ, нарушающую права и интересы третьих лиц, не соответствующую морально-этическим нормам ее получателей, а также рассылать обманные, беспокоящие или угрожающие сообщения;
- копировать или распространять информацию с нарушением авторских прав или условий лицензионных соглашений;
- фальсифицировать свой IP-адрес и иную техническую (служебную) информацию.

4.4. Права пользователей ИСПДн

4.4.1. Пользователи ИСПДн, подключенные к общедоступным сетям, имеют право использовать их только в целях выполнения своих должностных обязанностей.

5. Ответственность

5.1. Председатель Комиссии несет персональную ответственность за организацию безопасного информационного обмена в ЛВС и общедоступных сетях.

5.2. Администратор ИСПДн несет персональную ответственность за настройку ПО, операционных систем и технических средств, обеспечивающих работу пользователей ИСПДн в ЛВС и общедоступных сетях.

5.3. Пользователи ИСПДн несут персональную ответственность за соблюдение требований настоящей инструкции, в части их касающейся.

5.4. За нарушение требований настоящей инструкции к пользователям ИСПДн могут быть применены следующие санкции:

1) ограничение доступа к ресурсам общедоступных сетей;
2) лишение доступа к общедоступным сетям;
3) принятие административных мер воздействия;
4) применение иных санкций и мер, предусмотренных законодательством РФ.