

ПРИНЯТО
решением Совета Центра МБУ ДО «ЦВР
«Крылатый» г.о Самара
протокол № 2
от 09.01.2020 г.

УТВЕРЖДАЮ
Директор МБУ ДО
«ЦВР «Крылатый» г.о. Самара

О.В.Шумских
Введено в действие приказом
от «09» января 2020 года 09/11 - ОД

ПОЛОЖЕНИЕ
по безопасной работе сотрудников муниципального бюджетного учреждения
дополнительного образования «Центр внешкольной работы «Крылатый» городского округа
Самара при использовании сети Интернет.

1. Общие положения

1.1. Настоящее Положение по безопасной работе сотрудников муниципального бюджетного учреждения дополнительного образования «Центр внешкольной работы «Крылатый» городского округа Самара при использовании сети Интернет, осуществлении информационного взаимодействия с сервисами государственных информационных систем (далее - Положение) разработан в соответствии рекомендациями решения Координационного Совета по защите информации при полномочном представителе Президента Российской Федерации в Приволжском федеральном округе от 27.04.2016.

1.2. Положение основано на требованиях Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», нормативных правовых актах Российской Федерации, регулирующих отношения в области защиты информации.

1.3. Целями Положения являются:

- регулирование работы пользователей при использовании сети Интернет и осуществлении информационного взаимодействия с сервисами государственных информационных систем;
- обеспечение целостности, конфиденциальности и доступности хранящейся и передаваемой информации, находящейся на автоматизированных рабочих местах (далее - АРМ) или локальной вычислительной сети (далее - ЛВС);
- соблюдение требований, предусмотренных законодательством Российской Федерации и нормативными правовыми актами в области защиты информации.

1.4. При работе в сети Интернет и информационных системах пользователи руководствуются законодательством Российской Федерации, нормативными правовыми актами, иными документами в области информационных технологий и безопасности информации, а также настоящим положением.

2. Общие правила пользования на АРМ

2.1. Пользователь отвечает за правильность включения (выключения) АРМ, вход в систему и все действия при работе на нем.

2.2. АРМ разрешается использовать исключительно в служебных целях.

2.3. Пользователь обязан исключить возможность неосторожного причинения вреда техническим и информационным ресурсам.

2.4. Систематически осуществлять резервное копирование важной информации, хранящейся на АРМ пользователя.

2.5. Систематически проверять обновление антивирусной базы (как правило, в настройках антивируса, установлено их автоматическое обновление).

2.6. Во время работы экран монитора компьютера располагать в помещении таким образом, чтобы исключить возможность несанкционированного ознакомления с отображаемой на

нем информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

2.7. При временном отсутствии пользователя на рабочем месте экран монитора должен быть потушен или использована экранная заставка.

2.8. Обо всех выявленных нарушениях, связанных с информационной безопасностью, а так же для получения консультаций по вопросам информационной безопасности, необходимо обращаться к системному администратору МБУ ДО «ЦВР «Крылатый» г.о. Самара.

Пользователям запрещается:

2.9. Открывать на АРМ файлы и запускать программы, полученные из непроверенных источников.

2.10. Передавать свои идентификационные данные (пароли, логины), атрибуты доступа к ресурсам информационной системы посторонним лицам.

2.11. Отключать (блокировать) средства защиты информации.

2.12. Привлекать посторонних лиц для производства ремонта или настройки АРМ.

2.13. Разглашать обрабатываемую информацию третьим лицам.

2.14. Копировать служебную информацию на внешние носители без разрешения руководства.

2.15. Самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств.

2.16. Несанкционированно открывать общий доступ к папкам на АРМ.

2.17. Осуществлять подключение к АРМ и ЛВС посторонних и личных устройств (например: смартфоны, телефоны, считыватели информации, излучающие устройства (Wi-Fi, Bluetooth, радиомодемы) и т.п.).

3. Правила пользования в сети Интернет

»

3.1. Ресурсы сети Интернет предоставляются пользователям для получения информации необходимой для выполнения служебных обязанностей.

3.2. Пользователь обязан не предпринимать попыток несанкционированного доступа к информационным ресурсам, доступ к которым ему ограничен.

3.3. Пользователь может посещать только те ресурсы, содержание которых не противоречит законодательству Российской Федерации, а цель посещения должна быть связана с его служебной деятельностью.

3.4. Внимательно набирать имена сайтов. Поддельные сайты могут иметь отличие даже одного знака или тот же вид, что и оригинальные. Такие сайты могут содержать невидимые области, нажатие на которые может привести к заражению АРМ вредоносными программами или перенаправление на зараженные сайты. Более безопасно не набирать вручную наименование сайта, а пользоваться заранее сделанными закладками.

3.5. В настоящее время киберпреступники создают поддельные сайты. На не проверенных сайтах ввод конфиденциальных данных не рекомендуется!

3.6. Категорически запрещено использование для служебной деятельности иностранных Интернет-сервисов систем обмена мгновенными сообщениями, голосовой и видеoinформацией (ICQ, QIP, Jabber, Viber, Whatsap, Skype и т.д.), облачных сервисов хранения информации (iCloud, Google Drive, Dropbox и т.д.).

3.7. Пользователям запрещается:

- использовать доступ к сети Интернет в личных целях;

- посещать досугово-развлекательные сайты;

- использовать доступ к сети Интернет для распространения и тиражирования информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность.

4. Правила работы с электронной почтой

4.1. Категорически запрещено использование иностранных почтовых сервисов электронной почты (Gmail, Yahoo и т.д.) для служебной деятельности.

4.2. При получении электронного письма с вложением необходимо внимательно посмотреть адрес отправителя. В случае, если этот адрес неизвестен, или отличается от реального хотя бы одним знаком, открытие вложений таких писем не безопасно, поскольку могут содержать вредоносные программы.

4.3. В последнее время зафиксирована рассылка на электронные адреса пользователей, а также на официальные почтовые ящики органов исполнительной власти Самарской области и органов местного самоуправления муниципальных образований в Самарской области, во вложении к которым содержатся вредоносные файлы типа «Акты сверки^p», «Коммерческое предложение^p», «Судебное производство^p», с различными графическими изображениями. Такие вложения, как правило, содержат вирусы-шифровальщики (Trojan.Encoder), которые имитируют зависание операционной системы Windows компьютера и шифруют документы пользователей с расширениями *.doc, *.xls, *.pdf, *.txt, *.jpg, *.tif, *.rar, *.zip и другими, некоторые передают (воруют) информацию на сторонние сервера.

Вирусы-шифровальщики не определяются антивирусными программами в момент заражения АРМ.

4.4. При получении письма от неизвестного адресата, необходимо связаться с исполнителем и уточнить происхождение файлов. В случае невозможности установить происхождение письма, необходимо его удалить, не сохраняя и не запуская приложенные файлы.

4.5. Запрещается передавать информацию ограниченного доступа через сеть Интернет (в том числе посредством электронной почты) без использования средств защиты информации.

4.6. Запрещается осуществлять массовые рассылки электронной почты неслужебного характера (СПАМа).

4.7. Необходимо своевременно очищать свой почтовый ящик.

5. Правила антивирусной защиты

5.1. Для обеспечения антивирусной защиты должно использоваться сертифицированное лицензионное антивирусное программное обеспечение.

5.2. Ярлык антивирусной программы, как правило, находится в области уведомления или на вкладке «отображать скрытые значки» (нижний правый угол экрана).

5.3. Пользователи при работе с внешними носителями информации обязаны перед началом работы осуществить их проверку на предмет отсутствия компьютерных вирусов.

5.4. Обновление антивирусной программы, как правило, производится автоматически, в противном случае необходимо обратиться к администратору ЛВС.

5.5. Периодическое тестирование всего установленного программного обеспечения на предмет компьютерных вирусов производится автоматически. Полную проверку АРМ необходимо проводить при установке антивирусной программы, в случаях подозрения заражением, периодически 1 - 2 раза в год.

5.6. В случае обнаружения подозрительных программ срабатывает антивирус и необходимо прекратить какие-либо действия на АРМ и обратиться к системному администратору МБУ ДО «ЦВР «Крылатый» г.о. Самара.

5.7. В случае обнаружения вируса, не поддающегося лечению, системный администратор МБУ ДО «ЦВР «Крылатый» г.о. Самара, ответственный за обеспечение безопасности информации, принимает меры по восстановлению работы системы.

5.8. Вирусы-шифровальщики не определяются антивирусными программами в момент заражения АРМ.

5.9. В тех случаях, когда заражение вирусом АРМ все-таки произошло, необходимо:

- немедленно отключить компьютер для остановки действий вредоносной программы и не включать компьютер с зашифрованными данными, т.к. во время включений и перезагрузок происходят изменения файловой системы компьютера;

- не пытаться самостоятельно изменять расширения зараженных файлов, а также удалять любые файлы с рабочего компьютера и электронные сообщения;
 - обратиться к системному администратору МБУ ДО «ЦВР «Крылатый» г.о. Самара, отвечающему за установку антивирусных программ, обеспечение безопасности информации в своем структурном подразделении; с
 - обратиться к техническим специалистам по информационным технологиям, обслуживающим Вашу вычислительную технику;
 - обратиться в службу технической поддержки установленной у Вас антивирусной программы и совместно с ними попытаться восстановить утраченную информацию.
- 5.10. По информации производителей антивирусных программ возможность восстановления информации - минимальна, т.к. каждое вредоносное сообщение содержит индивидуальный файл-шифровальщик.

6. Ответственность Пользователя

6.1. Пользователи несут персональную ответственность за свои действия в период осуществления информационного взаимодействия с использованием АРМ;

6.2. За нарушение настоящего Положения, повлекшее неправомерное уничтожение, блокирование, модификацию либо копирование охраняемой законом информации, нарушение работы государственных информационных систем и ресурсов, АРМ пользователя может быть отключен от ЛВС до выяснения обстоятельств нарушения.

6.3. Нарушение требований законодательства Российской Федерации об информации, информационных технологиях и о защите информации влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.