УТВЕРЖДАЮ
Директор
КОГОБУ СШ с УИОП пгт Фаленки

С.Г. Шулятников
(приказ № 124/3 от 29.12.2017 года)

ПРАВИЛА БЕЗОПАСНОЙ РАБОТЫ В СЕТИ «ИНТЕРНЕТ» И С ВХОДЯЩЕЙ ЭЛЕКТРОННОЙ КОРРЕСПОНДЕНЦИЕЙ В КОГОБУ СШ с УИОП пгт Фаленки

1. Общие положения

1.1. В настоящее время основным фактором, влияющим на безопасность государственных информационных ресурсов, является угроза их заражения вредоносным программным обеспечением (далее - ВПО).

1.2. Сайты в сети «Интернет», вложения в сообщениях электронной почты могут содержать ВПО, запуск которых может привести к различным негативным последствиям: нарушению функционирования или сбоям в работе программного обеспечения, информационных систем, к уничтожению, изменению, блокированию, неправомерным копированию и распространению документов и файлов пользователя.

1.3. Во избежание указанных последствий необходимо соблюдать правила безопасной работы в сети «Интернет».

2. Назначение настоящего документа

2.1. Настоящие Правила разработаны для работников КОГОБУ СШ с УИОП пгт Фаленки (далее - школа), автоматизированное рабочее место (далее - АРМ) которых имеет подключение к информационно-телекоммуникационной сети «Интернет».

2.2. Целью разработки данных Правил являются:

- регламентация действий сотрудников школы при работе в сети «Интернет» и с входящей корреспонденцией, поступающей на электронные почтовые ящики;
- обеспечение безопасности (целостности, конфиденциальности и доступности) информации, обрабатываемой на АРМ или сетевых ресурсах школы.

3. Область действия настоящего документа

Правила обязательны для исполнения всеми работниками школы, осуществляющими работу в сети «Интернет» и с электронной почтой.

4. Основные положения

4.1. При работе в сети «Интернет»

4.1.1. Запрещается осуществлять выход в сеть «Интернет» при отсутствии (либо отключении) на АРМ установленного антивирусного средства защиты информации.

4.1.2. Доступ к ресурсам сети «Интернет» предоставляется работникам школы только для исполнения должностных обязанностей.

4.1.3 Запрещается осуществлять доступ к ресурсам сети «Интернет» в других целях (развлекательные и игровые ресурсы, социальные сети).

4.1.4. Закрывать страницы сайтов с большим количеством навязчивых рекламных предложений в виде баннеров или всплывающих окон сразу после их открытия.

4.1.5. Запрещается загружать и запускать файлы и программное обеспечение из сети «Интернет», переходить по ссылкам из источников, указанных в пункте 4.1.4.

Разрешено загружать файлы с официальных интернет-сайтов органов исполнительной власти субъектов Российской Федерации, территориальных органов федеральных органов исполнительной власти, государственных порталов.

4.1.6. Запрещается устанавливать на АРМ любое ПО, загруженное из сети «Интернет» и с внешних носителей информации.

4.1.7. Запрещается вносить изменения в настройки интернет-браузера и любого другого ПО АРМ.

4.1.8. Запрещается сохранять пароли на доступ к информационным ресурсам в сети «Интернет» в кэше интернет-браузера.

4.1.9. Использовать при работе в сети «Интернет» СПО браузер Mozilla Firefox и отечественную поисковую систему Яндекс. Использование иностранных интернет-браузеров Google Chrome и Microsoft Internet Explorer допускается при наличии необходимости работы с информационными системами, которые некорректно работают или несовместимы с Mozilla Firefox браузерами (например, ГАСУ, Единая информационная система в сфере закупок (ЕИС), АИС Сбербанк-АСТ и другие). Все указанные браузеры запускать только при помощи ярлыков, находящихся на «Рабочем столе».

4.2. При работе с электронной почтой

4.2.1. Электронная почта предоставляется работникам школы только для исполнения служебных обязанностей.

4.2.2. Запрещается использовать свой рабочий электронный адрес в личных целях или для пересылки личных сообщений, для подписки на рассылки и другие сервисы сети «Интернет», а также при регистрации на любых сайтах сети «Интернет», если это прямо не связано с должностными обязанностями.

4.2.3. Для создания почтовых ящиков в служебных целях использовать только отечественные почтовые серверы mail.ru, yandex.ru, rambler.ru.

4.2.4. Не допускается передача по сети «Интернет» информацию об учетных записях (имена пользователей, пароли) и другой конфиденциальной информации (ограниченного распространения), перечень которой определен Указом Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера».

При необходимости передача такой информации по сети «Интернет» производится только с использованием специально предназначенных для этого шифровальных (криптографических) средств защиты информации, прошедших в установленном законодательством Российской Федерации порядке сертификацию в Федеральной службе безопасности Российской Федерации.

4.2.5. Запрещается работа со служебной электронной почтой как на служебных, так и на личных мобильных устройствах и персональных компьютерах, подключенных к общедоступным точкам доступа к сети «Интернет».

4.2.6. Запрещается переходить по ссылкам и открывать файлы в сообщениях, содержащих:

текст рекламного характера с просьбой перейти по ссылке или открыть вложение;

информацию, файлы или ссылки, не имеющие отношения к служебной деятельности, ранее обсуждаемой теме и не затребованные у отправителя, в том числе в случаях, когда отправителем является официальная организация.

При необходимости следует уточнить у отправителя (по телефону) факт посылки сообщения, вызывающего подозрения в его достоверности.

4.2.7. Удалять сообщения с подозрительными вложениями, не открывая вложения, и очищать корзину, где хранятся удаленные сообщения.

4.2.8. В случае наличия подозрений о присутствии вредоносных программ необходимо информировать об этом администратора информационной безопасности.

Признаки заражения персонального компьютера ВПО:

- ошибки, возникающие при загрузке компьютера;
- блокирование доступа к данным;
- изменение стандартной стартовой страницы поиска интернет-браузера без Вашего одобрения, изменение браузера, используемого по умолчанию;
- появление на «Рабочем столе», в меню «Пуск» ярлыков запуска ПО, которое не входит в состав стандартного ПО АРМ;
- несанкционированное открытие новых окон, появление на экране монитора сообщений о том, что на компьютере обнаружены вредоносные или рекламные программы.

5. Ответственность

Персональную ответственность за несоблюдение настоящих Правил при работе на АРМ в сети «Интернет» и с электронной почтой несет сотрудник, являющийся пользователем указанного АРМ, в соответствии с действующим законодательством Российской Федерации.