

УТВЕРЖДАЮ

Директор МБОУДО

МУК шт. Кильмезь

Фазулов М.М.



Приказ № 54 от 29.06. 2017 г.

**Правила
безопасной работы
в сети «Интернет» и с входящей
электронной корреспонденцией**

Содержание

| | |
|---|---|
| 1. Введение..... | 2 |
| 2. Назначение..... | 2 |
| 3. Область действия..... | 2 |
| 4. Основные положения..... | 2 |
| 4.1. При работе в сети «Интернет»..... | 2 |
| 4.2. При работе с электронной почтой..... | 3 |
| 5. Ответственность..... | 4 |

1. Введение

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

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.

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

2. Назначение настоящего документа

Настоящие Правила разработаны для работников муниципального бюджетного образовательного учреждения дополнительного образования межшкольного учебного комбината пг.Кильмезь Кильмезского района Кировской области далее – МБОУДО МУК пгт.Кильмезь), автоматизированное рабочее место (далее – АРМ) которых имеет подключение к информационно-телекоммуникационной сети «Интернет».

Целью разработки данных Правил являются:

- регламентация действий сотрудников управления образования 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 министерства.

3. Область действия настоящего документа

Правила обязательны для исполнения всеми работниками министерства, 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 МБОУДО МУК пгт.Кильмезь 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 скачивать файлы с официальных интернет-сайтов органов исполнительной власти субъектов Российской Федерации, территориальных органов федеральных органов исполнительной власти, государственных порталов.

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

4.1.7. Использовать при работе в сети «Интернет» отечественные браузеры «Yandex.Браузер» или «Спутник» и отечественные поисковые системы (Яндекс, Майл, Спутник). Использование иностранных интернет-браузеров допускается при наличии необходимости работы с информационными системами, которые некорректно работают или несовместимы с отечественными браузерами (например, ГАСУ, Единая информационная система в сфере закупок (ЕИС), АИС Сбербанк-АСТ и другие). При этом в случае наличия возможности использования для работы с такими системами свободно распространяемых браузеров (например, Mozilla Firefox) рекомендуется сделать выбор в их пользу. Для другой работы в сети «Интернет», не связанной с информационной системой, необходимо использовать отечественный интернет-браузер.

4.2. При работе с электронной почтой

4.2.1. Электронная почта предоставляется работникам МБОУДО МУКпгт.Кильмезь 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 отправки сообщения, вызывающего подозрения о 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:

1. Изменение стандартной стартовой страницы поиска интернет-браузера без вашего одобрения.

2. Несанкционированное открытие новых окон, появление на экране монитора сообщений о том, что на компьютере обнаружены вредоносные или рекламные программы.

3. Сообщения антивируса о невозможности обновиться.

Некоторые вредоносные программы нейтрализуют возможность обновления антивирусных средств, что делает систему защиты неэффективной.

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.