Приложение
к приказу министерства образования
Саратовской области
от 03 10.2016 г. № 3110

# ПРАВИЛА

**безопасной работы служащих министерства образования Саратовской области, работников образовательных организаций, функции и полномочия учредителя, в отношении которых осуществляет министерство образования Саратовской области при осуществлении эксплуатации информационных систем и интернет - сервисов с использованием информационно-телекоммуникационной сети «Интернет»**

## Общие положения

Правила безопасной работы служащих министерства образования Саратовской области, работников образовательных организаций, функции и полномочия учредителя, в отношении которых осуществляет министерство образования Саратовской области при осуществлении эксплуатации информационных систем и интернет - сервисов с использованием информационно - телекоммуникационной сети «Интернет» (далее - Правила) разработаны в соответствии с Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и защите информации» и нормативными правовыми актами Российской Федерации, регулирующими отношения в области защиты информации.

Правила предназначены для служащих министерства образования Саратовской области, работников образовательных организаций, функции и полномочия учредителя, в отношении которых осуществляет министерство образования Саратовской области, которые при выполнении своих должностных регламентов или должностных обязанностей осуществляют эксплуатацию информационных систем и интернет - сервисов с использованием сети «Интернет» (далее - Пользователи).

Целями Правил являются:

обеспечение целостности, конфиденциальности и доступности обрабатываемой информации в информационных системах с использованием сети «Интернет»;

соблюдение Пользователями требований нормативных правовых актов и законодательства Российской Федерации в области защиты информации.

Пользователи в своей работе руководствуются Правилами, а также иными руководящими, нормативными документами в области информационной безопасности.

## Обязанности Пользователей по обеспечению безопасности информации

1. Пользователю разрешается использовать закрепленное за ним

автоматизированное рабочее место (далее – АРМ) только в служебных целях.

2. Необходимо установить и эксплуатировать на АРМ последнюю версию браузера, имеющего встроенные функции предупреждения о сайтах, распространяющих вредоносные программы.

3. Регулярно обновлять на АРМ базы средств антивирусной защиты.

4. Необходимо загружать на АРМ программное обеспечение и драйверы только с сайта компании-разработчика данного программного обеспечения.

5. Если при посещении какого-либо сайта в сети «Интернет», без вашего ведома автоматически открывается новое окно браузера или появляется предложение об установке на АРМ нового программного обеспечения, необходимо сразу закрыть его и не использовать данный сайт.

6. Не реже одного раза в неделю осуществлять резервное копирование важной служебной информации, хранящейся на АРМ Пользователей.

7. Соблюдать парольную политику (Раздел «Парольная политика» Правил).

8. Использовать разные пароли для доступа к разным информационным системам.

9. Производить блокировку АРМ (блокировку экрана монитора) при отсутствии Пользователя на рабочем месте.

10. При получении электронного письма от неизвестного адресата, необходимо попытаться установить автора письма и уточнить у него происхождение файлов. В случае невозможности установить происхождение электронного письма, необходимо его удалить, не запуская выполнение полученных программ, не сохраняя и не открывая приложенные файлы.

11. Перед открытием любого полученного или загруженного из сети «Интернет» файла необходимо проверить отсутствие вредоносных программ средствами антивирусной защиты. Зараженные и подозрительные файлы необходимо незамедлительно удалить, в том числе из «корзины».

12. При утрате ключа электронной подписи или подозрении о его возможной компрометации, о данном факте необходимо незамедлительно сообщить непосредственному руководителю, а так же лицу, ответственному за обеспечение информационной безопасности или администратору информационной безопасности (далее - АИБ) для отзыва сертификата данного электронного ключа.

13. Пользователь обязан исключить возможность причинения умышленного или по неосторожности вреда техническим, программным средствам, информационным ресурсам министерства образования Саратовской области и образовательных организаций, функции и полномочия учредителя, в отношении которых осуществляет министерство образования Саратовской области (далее – организации), а также нарушения конфиденциальности, целостности и доступности обрабатываемой информации на АРМ.

14. Обо всех выявленных нарушениях, связанных с информационной безопасностью, а так же для получений консультаций по вопросам информационной безопасности, необходимо обратиться к АИБ организации.

15. Запрещается открывать файлы и запускать программы, полученные из неизвестных, непроверенных источников в сети «Интернет».

16. Запрещается передавать свои идентификационные данные другим лицам (пароли, логины).

17. Запрещается оставлять без присмотра в доступном месте или передавать другим лицам свой ключ электронной подписи.

18. Запрещается предпринимать попытки несанкционированного доступа к информационным ресурсам организации, доступ к которым ограничен политикой информационной безопасности.

19. Запрещается использовать доступ к сети «Интернет» для распространения и тиражирования информации ограниченного пользования, сведений, направленных на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность.

20. Запрещается использовать программные и аппаратные средства, позволяющие получить доступ к ресурсам сети «Интернет», содержание которых не имеет отношения к деятельности организации, а также к ресурсам, содержание и направленность которых запрещены международным и Российским законодательством включая материалы, носящие вредоносную, угрожающую, клеветническую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения оружия, взрывчатых, сильно действующих, ядовитых, наркотических веществ.

21. Запрещается отключать или изменять настройки установленных на АРМ средств защиты информации.

22. Запрещается привлекать посторонних лиц для производства ремонта, технического обслуживания или настройки АРМ, установки программного обеспечения на АРМ без согласования с АИБ.

23. Запрещается загружать на АРМ файлы через файлообменные сети (например, BitTorrent, DirectConnect и другие) в связи с высокой вероятностью загрузки вредоносных программ.

## Парольная политика

1. Пароль для доступа к информационным системам должен состоять не менее, чем из восьми символов.

2. В пароле должны присутствовать символы из числа следующих категорий:

- заглавные буквы английского алфавита от A до Z;
- строчные буквы английского алфавита от a до z;
- цифры (от 0 до 9);
- символы, не принадлежащие алфавитно-цифровому набору (например: !, $, #, %,*, @, &).

3. Пароль не должен содержать имя учетной записи Пользователя или какую-либо его часть.

4. Пароль не должен включать в себя легко вычисляемые сочетания символов, простые комбинации символов «123», «54321», «user» и им подобные, а так же фамилию, имя, отчество и даты рождения Пользователя и родственников Пользователя, клички домашних животных, номерные знаки автомобилей, номера телефонов и другие пароли, которые могут быть подобраны, основываясь на информации о Пользователе.

5. Не использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов (например, «аааааааа», «55555»).

6. Не использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, «12345678»«qwerty» и т.п.).

7. При смене пароля не использовать вновь ранее использованные пароли.

8. При смене пароля новое значение пароля должно отличаться от предыдущего не менее чем в 4 позициях.

9. Во время ввода пароля необходимо убедиться, что клавиатура находится вне видимости посторонних лиц и оптических технических средств (видеокамер, фотоаппаратов).

## Ответственность Пользователя за нарушение Правил

Пользователь несет персональную ответственность:

- за соблюдение требований, установленных настоящими Правилами;
- за свои действия при осуществлении эксплуатации информационных систем и интернет - сервисов с использованием информационно-телекоммуникационной сети «Интернет»;
- за самостоятельную, несанкционированную установку на АРМ программного обеспечения, модификацию или тиражирование установленного на АРМ программного обеспечения, изменение алгоритмов функционирования технических и программных средств, входящих в состав АРМ;
- за самостоятельное, несанкционированное использование на АРМ модемов, смартфонов для подключения к сети «Интернет».

Нарушение настоящих Правил, повлекшее неправомерное уничтожение, блокирование, модификацию либо копирование охраняемой законом информации, нарушение работы информационных систем и сервисов, может повлечь дисциплинарную, административную или уголовную ответственность в соответствии с действующим законодательством.