Администрация муниципального района «Сухиничский район»

КАЛУЖСКАЯ ОБЛАСТЬ

ПОСТАНОВЛЕНИЕ

от 20.02.2018 № 113

Об утверждении Инструкции по информационной безопасности при работе муниципальных служащих и сотрудников администрации МР «Сухиничский район» с информационными системами органов исполнительной власти Калужской области и ресурсами сети Интернет

В целях обеспечения информационной безопасности при работе муниципальных служащих и сотрудников администрации МР «Сухиничский район» с информационными системами органов исполнительной власти Калужской области и ресурсами сети Интернет, администрация МР «Сухиничский район»

ПОСТАНОВЛЯЕТ:

1. Утвердить Инструкцию по информационной безопасности при работе муниципальных служащих и сотрудников администрации МР «Сухиничский район» с информационными системами органов исполнительной власти Калужской области и ресурсами сети Интернет (прилагается).
2. Заведующему отделом информационных технологий и автоматизации администрации МР «Сухиничский район» (М.А.Жортушев) ознакомить муниципальных служащих и сотрудников администрации МР «Сухиничский район» с Инструкцией по информационной безопасности при работе муниципальных служащих и сотрудников администрации МР «Сухиничский район» с информационными системами органов исполнительной власти Калужской области и ресурсами сети Интернет.
3. Настоящее постановление вступает в силу с момента его подписания и подлежит размещению на официальном сайте администрации МР «Сухиничский район».

Глава администрации
МР «Сухиничский район» **А.С. Колесников**

Приложение к постановлению
администрации МР «Сухиничский
район»
от 20.02.2018 № 113.

Инструкция
по информационной безопасности при работе муниципальных служащих и сотрудников администрации МР «Сухиничский район» с информационными системами органов исполнительной власти Калужской области и ресурсами сети Интернет

1. Общие положения

1.1. Основная цель настоящей Инструкции — предотвращение несанкционированного уничтожения, искажения, копирования, блокирования информации, обрабатываемой на компьютерах администрации МР «Сухиничский район» в информационных системах органов исполнительной власти Калужской области.

2. Обязанности

2.1. Руководители отделов администрации МР «Сухиничский район» обязаны:

2.1.1. Организовать выполнение требований настоящей Инструкции муниципальными служащими и сотрудниками отделов администрации МР «Сухиничский район»;

2.1.2. Организовать контроль исполнения требований настоящей Инструкции муниципальными служащими и сотрудниками отделов администрации МР «Сухиничский район»;

2.1.3. Немедленно сообщать ответственному за информационную безопасность об имевших место в отделе администрации инцидентах информационной безопасности;

2.2. Муниципальные служащие и сотрудники отделов администрации МР «Сухиничский район» обязаны:

2.2.1. Знать и соблюдать требования настоящей Инструкции;

2.2.2. Хранить свои пароли и идентификаторы втайне, способом, исключающим возможность доступа к ним посторонних лиц;

2.2.3. Не допускать подключения к своему ПК дополнительных устройств без согласования с ответственным за информационную безопасность;

2.2.4. Контролировать несанкционированные подключения устройств к ПК и в случаях обнаружения таких подключений прекратить работу па ПК, выключить ПК и немедленно сообщить о данном факте руководителю отдела и ответственному за информационную безопасность;

2.2.5. Выполнять следующие требования по антивирусному контролю:

2.2.5.1. Контролировать наличие значка средства антивирусной защиты на панели задач. При отсутствии значка сообщить руководителю своего отдела и ответственному за информационную безопасность;

2.2.5.2. При обнаружении сообщений средств антивирусной защиты о сбоях в работе, истечении срока действия лицензии и об устаревших базах описания вирусов сообщить руководителю своего отдела и ответственному за информационную безопасность;

2.2.5.3. При возникновении подозрения на «заражение» ПК вредоносным

программным обеспечением (нетипичная работа программ, появление графических и звуковых эффектов, искажение данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) прекратить работу на ПК, выключить ПК и сообщить о данном факте ответственному за информационную безоапасность для принятия мер по проверке и устранению возможного «заражения»;

2.2.6. При работе с электронной почтой:

2.2.6.1. Удалять сомнительные сообщения, не открывая их.

2.2.6.2. В случае, если сообщение получено от известного адресата, но содержит сомнительное содержание текста и/или темы, то, прежде, чем продолжить обработку письма, уточнить у адресата факт отправки данного сообщения;

2.2.7. При работе в сети Интернет:

2.2.7.1. При возникновении подозрений в том, что открытая страница является поддельной, никаких действий не предпринимать и обратиться за разрешением для дальнейшей работы к ответственному за информационную безопасность;

2.2.7.2. При возникновении на экране ПК «всплывающих» сообщений в виде окон, закрывающих обзор страницы и требующих для своего закрытия нажатия кнопок (обычно «Да», «Нет»), не имеющих при этом «крестика» для закрытия окна, закрыть браузер (internet explorer, firefox, chrome, opera, яндекс браузер и т.д.). В случае присутствия «крестика» попытаться закрыть окно, «кликнув» по нему. Если результат не достигнут, то закрыть браузер и попытаться найти необходимую информацию на другом сайте.

2.2.8. Регулярно делать резервные копии своих файлов (документов) на внешний носитель информации (флэш-накопитель, внешний жесткий диск), отключаемый от ПК после записи резервной копии, с периодичностью не реже одного раза в неделю в соответствии с требованиями пункта 2.2.3 настоящей Инструкции.

3. Запреты

3.1. Муниципальным служащим и сотрудникам администрации МР «Сухиничский район» **ЗАПРЕЩАЕТСЯ:**

3.1.1. Использовать компоненты программного н аппаратного обеспечения ПК в неслужебных целях;

3.1.2. Отключать средства защиты информации, в том числе: средства защиты от несанкционированного доступа, средства доверенной загрузки, средства антивирусной защиты, средства криптографической защиты информации, без согласования с руководителем отдела и ответственным за информационную безопасность;

3.1.3. Самостоятельно вносить какие-либо изменения в конфигурацию средств защиты информации;

3.1.4. Самостоятельно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ПК или устанавливать дополнительно любые программные или аппаратные средства;

3.1.5. Осуществлять обработку информации ограниченного доступа на ПК, не предназначенных для этих целей;

3.1.6. Оставлять включенными без контроля свои ПК, не активировав средства защиты от несанкционированного доступа (временную блокировку экрана и клавиатуры и т.п.);

3.1.7. Оставлять без контроля носители, содержащие ключи электронной подписи и конфиденциальную информацию;

3.1.8. Передавать на любых носителях ключи электронной подписи и конфиденциальную информацию лицам, не допущенным к работе с ними;

3.1.9. Предпринимать умышленные попытки несанкционированного доступа

к информационным ресурсам и информационно-коммуникационным сетям, доступ к которым не предусмотрен исполнением служебных обязанностей;

3.1.10. Размещать пароли на окружающих предметах, в файлах, электронных записных книжках, мобильных устройствах, других носителях информации без применения средств шифрования;

3.1.11. Сообщать другим пользователям реквизиты своей учетной записи, а также регистрироваться для работы на ПК под чужой учетной записью;

3.1.12. Соглашаться с запуском на ПК п установкой на ПК сторонних приложений, предлагаемых ресурсами сети Интернет (бесплатная проверка компьютера на вирусы, скачивание обновлений, установка «полезных» приложений и т.д.).

4. Права

4.1. Муниципальным служащим и сотрудникам администрации МР «Сухиничский район» имеют право:

4.1.1. Получать необходимую техническую и методологическую помощь по вопросам работы ПК и обеспечения информационной безопасности.

4.1.2. Обращаться к руководителю отдела с предложением прекращения работы муниципальных служащих и сотрудников администрации МР «Сухиничский район» на ПК при несоблюдении ими требований настоящей Инструкции;

4.2. Руководители отделов администрации МР «Сухиничский район» имеют право:

4.2.1. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи информации и технических средств;

4.2.2. Направлять главе администрации МР «Сухиничский район» предложения по совершенствованию мер информационной безопасности.

5. Ответственность

5.1. Муниципальные служащие и сотрудники администрации МР «Сухиничский район» несут персональную ответственность в соответствии с действующим законодательством за обеспечение информационной безопасности при использовании ПК и за соблюдение требований настоящей Инструкции.