



АДМИНИСТРАЦИЯ

Муниципального района
«ЖУКОВСКИЙ РАЙОН»
Калужской области

ПОСТАНОВЛЕНИЕ

г. Жуков

от 13.02.2018

№ 121

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

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

1. Утвердить инструкцию по информационной безопасности при работе муниципальных служащих и работников администрации МР «Жуковский район» (далее - администрация) с информационными системами органов исполнительной власти Калужской области и ресурсами сети Интернет согласно приложению к настоящему постановлению.

2. Заведующему отделом организационно-контрольной работы и взаимодействия с поселениями администрации ознакомить сотрудников администрации муниципального района с инструкцией по информационной безопасности при работе муниципальных служащих и работников администрации МР «Жуковский район» с информационными системами органов исполнительной власти Калужской области и ресурсами сети Интернет.

3. Контроль за исполнением настоящего постановления возложить на зав. главы администрации – управляющего делами Кретову И.И.

Глава администрации

А.В. Суярко

Инструкция
по информационной безопасности при работе муниципальных служащих и
работников администрации МР «Жуковский 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 «Жуковский район» и в информационных системах органов исполнительной власти Калужской области.

2. Обязанности

2.1. **Заместители главы администрации** обязаны:

2.1.1. Организовать контроль исполнения требований настоящей Инструкции муниципальными служащими и работниками подразделений администрации;

2.2. **Заведующие отделами администрации** обязаны:

2.2.1. Организовать выполнение требований настоящей Инструкции муниципальными служащими и работниками подразделений администрации;

2.2.2. Организовать контроль исполнения требований настоящей Инструкции муниципальными служащими и работниками подразделений администрации;

2.2.3. Немедленно сообщать заместителю главы – управляющему делами администрации об имевших место инцидентах информационной безопасности;

2.2.4. При необходимости подключения к персональному компьютеру (далее - ПК) муниципального служащего или работника своего структурного подразделения дополнительного устройства получить документальное подтверждение о возможности такого подключения у начальника отдела информационного обеспечения администрации;

2.3. **Заведующий юридическим отделом администрации** обязан:

2.3.1. Организовать направление информации в отдел организационно-контрольной работы и взаимодействия с поселениями администрации об уволившихся муниципальных служащих и работников администрации в день их увольнения, а также о муниципальных служащих и работниках администрации, перешедших на другую должность в администрации;

2.4. **Муниципальные служащие и работники администрации** обязаны:

2.4.1. Знать и соблюдать требования настоящей Инструкции;

2.4.2. Содействовать исполнению требований настоящей Инструкции другими муниципальными служащими и работниками администрации;

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

2.4.4. Не допускать подключения к своему ПК дополнительных устройств без согласования с руководителем своего структурного подразделения в соответствии с пунктом 2.1.4 настоящей Инструкции;

2.4.5. Контролировать несанкционированные подключения устройств к ПК и в случаях обнаружения таких подключений прекратить работу на ПК, выключить ПК и немедленно сообщить о данном факте руководителю своего структурного подразделения и начальнику отдела информационного обеспечения администрации;

2.4.6. Выполнять следующие требования по антивирусному контролю:

2.4.6.1. Контролировать наличие значка средства антивирусной защиты на панели задач. При отсутствии значка сообщить руководителю своего структурного подразделения и начальнику отдела информационного обеспечения администрации;

2.4.6.2. При обнаружении сообщений средств антивирусной защиты о сбоях в работе, истечении срока действия лицензии и об устаревших базах описания вирусов сообщить руководителю своего структурного подразделения и начальнику отдела информационного обеспечения администрации;

2.4.6.3. 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 руководителю своего структурного подразделения и начальнику отдела информационного обеспечения администрации для принятия мер по проверке и устранению возможного «заражения»;

2.4.7. При работе с электронной почтой:

2.4.7.1. Удалять сомнительные сообщения, не открывая их.

2.4.7.2. 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;

2.4.7.3. Использовать внешние сервисы электронной почты исключительно по согласованию с начальником отдела информационного обеспечения администрации (в настоящей Инструкции под внешними сервисами электронной почты понимаются сервисы, предоставляющие муниципальному служащему или работнику администрации возможность использования персонального почтового ящика, адрес которого заканчивается не на @adm.kaluga.ru, @gmail.com);

2.4.8. При работе в сети Интернет:

2.4.8.1. Согласовывать с руководителем своего структурного подразделения ввод служебной информации (пароль, номер телефона и т.п.) на ресурсах сети Интернет;

2.4.8.2. При возникновении подозрений в том, что открытая страница является поддельной, никаких действий не предпринимать и обратиться за разрешением для дальнейшей работы к руководителю своего структурного подразделения и начальнику отдела информационного обеспечения администрации;

2.4.8.3. 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.

2.4.9. 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 2.3.4 настоящей Инструкции.

3. Запреты

3.1. Муниципальным служащим и работникам администрации ЗАПРЕЩАЕТСЯ:

3.1.1. Использовать компоненты программного и 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 начальником отдела информационного обеспечения администрации;

3.1.3. Самостоятельно вносить какие-либо изменения в конфигурацию средств защиты информации без согласования с начальником отдела информационного обеспечения администрации;

3.1.4. Самостоятельно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ПК или устанавливать дополнительно любые программные или аппаратные средства без согласования с руководителем своего структурного подразделения и начальником отдела информационного обеспечения администрации;

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. Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты. Об обнаружении такого рода свойств и ошибок немедленно ставить в известность руководителя своего структурного подразделения и начальника отдела информационного обеспечения администрации;

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

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

3.1.13. Соглашаться с запуском на ПК и 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. Муниципальные служащие и работники администрации 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 своего структурного подразделения с предложением прекращения работы муниципальных служащих или работников подразделения на ПК при несоблюдении ими требований настоящей Инструкции;

4.2. **Руководители структурных подразделений администрации** 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 заместителю главы – управляющему делами администрации предложения по совершенствованию мер информационной безопасности.

5. Ответственность

5.1. **Муниципальные служащие и работники администрации** несут персональную ответственность в соответствии с действующим законодательством за обеспечение информационной безопасности при использовании ПК и за соблюдение требований настоящей Инструкции.