МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ
КАЛУЖСКОЙ ОБЛАСТИ

ПРИКАЗ

от 22 февраля **2018 г** **№** 164

Об утверждении инструкции по информационной безопасности при работе государственных гражданских служащих и работников министерства здравоохранения Калужской области с информационными системами органов исполнительной власти Калужской области

В целях обеспечения информационной безопасности при работе государственных гражданских служащих и работников министерства здравоохранения Калужской области с информационными системами органов исполнительной власти Калужской области и ресурсами сети Интернет **ПРИКАЗЫВАЮ:**

1. Утвердить инструкцию по информационной безопасности при работе государственных гражданских служащих и работников министерства здравоохранения Калужской области с информационными системами органов исполнительной власти Калужской области (далее – Инструкция) согласно приложению к настоящему приказу.
2. Начальнику отдела кадров ознакомить государственных гражданских служащих и работников министерства здравоохранения Калужской области с Инструкцией.

Министр **К.Н. Баранов**

Приложение к приказу
от «22» 02 2018 № 164

Инструкция
по информационной безопасности при работе государственных гражданских служащих и работников министерства здравоохранения Калужской области 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 министерства здравоохранения Калужской области (далее – министерство) и в информационных системах органов исполнительной власти Калужской области.

2. Обязанности

2.1. **Руководитель структурного подразделения министерства** обязан:

2.1.1. Организовать выполнение требований Инструкции государственными гражданскими служащими и работниками подразделений министерства;

2.1.2. Организовать контроль исполнения требований Инструкции государственными гражданскими служащими и работниками подразделений министерства;

2.1.3. Немедленно сообщать начальнику отдела информатизации министерства об имевших место в подразделении министерства инцидентах информационной безопасности;

2.1.4. При необходимости подключения к персональному компьютеру (далее – ПК) государственного гражданского служащего или работника своего структурного подразделения дополнительного устройства получить документальное подтверждение о возможности такого подключения у начальника отдела информатизации министерства.

2.2. **Начальник отдела кадров министерства** обязан:

2.2.1. Организовать направление информации в отдел инфраструктуры и связи управления информатизации и связи министерства экономического развития Калужской области об уволившихся государственных гражданских служащих и работниках министерства в день их увольнения, а также о государственных гражданских служащих и работниках министерства, перешедших на другую должность в министерстве.

2.3. **Государственные гражданские служащие и работники министерства** обязаны:

2.3.1. Знать и соблюдать требования Инструкции;

2.3.2. Содействовать исполнению требований Инструкции другими государственными гражданскими служащими и работниками министерства;

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

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

2.3.5. 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 информатизации министерства;

2.3.6. Выполнять следующие требования по антивирусному контролю:

2.3.6.1. Контролировать наличие значка средства антивирусной защиты на панели задач. При отсутствии значка сообщить руководителю своего структурного подразделения и начальнику отдела информатизации министерства;

2.3.6.2. 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 информатизации;

2.3.6.3. 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 информатизации министерства для организации проверки и устранения возможного «заражения»;

2.3.7. При работе с электронной почтой:

2.3.7.1. Удалять сомнительные сообщения, не открывая их;

2.3.7.2. 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;

2.3.7.3. Использовать внешние сервисы электронной почты исключительно по согласованию с заместителем министра – начальником управления информатизации в сфере здравоохранения и организационно-контрольной работы министерства (в Инструкции под внешними сервисами электронной почты понимаются сервисы, предоставляющие государственному гражданскому служащему или работнику министерства возможность использования персонального почтового ящика, адрес которого заканчивается не на @adm.kaluga.ru, @admoblkaluga.ru);

2.3.8. При работе в сети Интернет:

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

2.3.8.2. 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 информатизации министерства;

2.3.8.3. 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, закрыть браузер и попытаться найти необходимую информацию на другом сайте;

2.3.9. При обнаружении недокументированных свойств и ошибок в программном обеспечении или в настройках средств защиты немедленно ставить в известность руководителя своего структурного подразделения и начальника отдела информатизации министерства;

2.3.10. 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 Инструкции.

2.4. **Начальник отдела информатизации министерства** обязан:

2.4.1. В случае возникновения инцидентов информационной безопасности сообщить о них в управление информатизации и связи министерства экономического развития Калужской области и принять меры по организации их устранения.

3. Запреты

3.1. Государственным гражданским служащим и работникам министерства **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, без согласования с руководителем своего структурного подразделения и начальником отдела информатизации министерства;

3.1.3. Самостоятельно вносить какие-либо изменения в конфигурацию средств защиты информации без согласования с руководителем своего структурного подразделения и начальником отдела информатизации министерства;

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 информатизации министерства;

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;

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. **Государственные гражданские служащие и работники министерства имеют** право:

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

4.2. **Руководители структурных подразделений министерства** 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 министра – начальнику управления информатизации в сфере здравоохранения и организационно-контрольной работы министерства предложения по совершенствованию мер информационной безопасности.

5. Ответственность

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