|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ  УЧРЕЖДЕНИЕ ЗДРАВООХРАНЕНИЯ «СТАНЦИЯ СКОРОЙ  МЕДИЦИНСКОЙ ПОМОЩИ» г.КАЗАНИ | |  | ДӘҮЛӘТ СӘЛАМӘТЛЕК САКЛАУ  АВТОНОМ УЧРЕЖДЕНИЯСЕ  КАЗАН ШӘҺӘРЕ  «АШЫГЫЧ МЕДИЦИНА ЯРДӘМЕ CТАНЦИЯСЕ» | |
|  | | | | |
| **ПРИКАЗ**  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | г. **Казань** | | | **БОЕРЫК**  №\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

*О дополнительных мерах по повышению защищенности*

*информационной инфраструктуры в ГАУЗ «ССМП»*

В целях исполнения рекомендаций Федеральной службы по техническому и экспортному контролю (далее ФСТЭК РФ) о дополнительных мерах по повышению защищенности информационной инфраструктуры, изложенных в письме Министерства здравоохранения Республики Татарстан № 09-01/4446 от 06.04.2022 (далее письмо),

ПРИКАЗЫВАЮ:

Принять к исполнению рекомендации ФСТЭК РФ и организовать следующие мероприятия:

1. Запретить использование личных средств вычислительной техники (ноутбуков, планшетов, смартфонов) сетевых устройств и дисковых накопителей на автоматизированных рабочих местах информационных систем ГАУЗ «ССМП».
2. Запретить размещения защищаемой информации в облачных сервисах, а также передачи через мессенджеры, Google Docs и другие сервисы.
3. Исключить применение иностранных систем видеоконференции, в том числе Zoom, Skype, а также систем удаленного доступа (RAdmin, Team Viewer).
4. Руководителям структурных подразделений обеспечить:
   1. Периодическую (1 раз в 3 месяца) смену логина / пароля учетных записей сотрудников своих подразделений - пользователей информационных систем ГАУЗ «ССМП».
   2. Контроль:

* соблюдения ограничений на использование личных средств вычислительной техники, подключения неучтенных съемных машинных носителей информации и мобильных устройств;
* подключаемых к автоматизированным рабочим местам съемных машинных носителей информации и анализ записываемой на них информации;
* соблюдения ограничений на использование программного обеспечения, не относящегося к производственной деятельности и не требуемого для выполнения должностных обязанностей работников.

1. Отделу АСУ:
   1. Обеспечить регистрацию событий информационной безопасности информации на сетевом и серверном оборудовании, используемые на объекте, особенно событий, связанных с внешними подключениями, анализом сетевого трафика, превышением количества попыток входа пользователей, с попытками запуска сторонних программ и сервисов, а также с удаленным доступом.
   2. Провести:

* проверку настроек средств межсетевого экранирования и активного сетевого оборудования, включая актуальные обновления прошивок, отключение неиспользуемых портов и ограничение на доступ пользователей в сеть «Интернет»;
* инвентаризацию пользователей, имеющих удаленный доступ к информационным ресурсам ГАУЗ «ССМП»;
* обновление антивирусного программного обеспечения до последней версии и установку актуальных баз данных средств антивирусной защиты;
* анализ представленных, в пунктах 4-10 приложения к письму Минздрава РТ, рекомендаций. Определить рекомендации, которые возможно применить в ИТ инфраструктуре ГАУЗ «ССМП» и использовать их в работе.
  1. Реализовать многофакторную аутентификации для удаленного и локального доступа привилегированных пользователей.
  2. Ограничить возможность удаленного управления прикладным и системным программным обеспечением, телекоммуникационным оборудованием через сеть Интернет.
  3. Настроить автоматическое обновления баз данных средств антивирусной защиты.
  4. Проверять актуальность версий программного обеспечения средств защиты информации, применяемых для обеспечения безопасности узлов локально-вычислительной сети, а также баз данных, не реже, чем раз в 3 дня, при наличии их обновлений – незамедлительное применение этих обновлений.
  5. Информировать подрядные организации в сфере информационных технологий, о необходимости принятия мер по блокированию угроз и о необходимости соблюдения требований по безопасности при предоставлении услуг.

1. Комиссии по защите персональных данных, в срок до 25.04.2022г.,

* Разработать инструкцию по работе с электронной почтой и представить Главному врачу на утверждение.
* Внести в инструкцию по организации парольной защиты изменения в соответствии с рекомендациями, представленными в письме и представить обновленную версию на утверждение Главному врачу.

1. Заведующей канцелярией ознакомить с настоящим Приказом руководителей структурных подразделений и членов комиссии по защите персональных данных в ГАУЗ «ССМП».
2. Контроль за исполнением настоящего Приказа оставляю за собой.

Главный врач Ф.Ш. Галяутдинов

Исп.: Н.С. Хусаинов

т. 9172335654