

Министерство цифрового развития государственного управления, информационных технологий и связи Республики Татарстан (далее – Министерство) информирует об обнаружении в марте 2020 года ряда критических уязвимостей в операционных системах семейства Windows, позволяющих потенциальным злоумышленникам осуществлять удаленное управление компьютерами и информационными системами. В частности, по информации от компании Microsoft, серьезные уязвимости обнаружены в службах удаленного доступа к файлам (CVE-2020-0796) и отображения экранных шрифтов (atmfd.dll).

По мнению Федеральной службы безопасности Российской Федерации, сложившаяся ситуация может вызвать очередную волну киберпреступлений, в том числе, направленных против информационных систем органов государственной власти и местного самоуправления, а также против объектов критической информационной инфраструктуры Российской Федерации с целью дестабилизации их работы.

С учетом изложенного, в целях предотвращения компьютерных атак на информационные системы органов государственной власти и местного самоуправления Республики Татарстан и минимизации их возможных негативных последствий руководителям министерств и ведомств Республики Татарстан, главам муниципальных образований предлагается:

- инициировать процесс обновления общесистемного и прикладного программного обеспечения, установленного на рабочих компьютерах и серверном оборудовании всех подчиненных подразделений и подведомственных организаций;

- проинструктировать специалистов подразделений, отвечающих за информатизацию и информационную безопасность, всех остальных сотрудников, включая сотрудников подведомственных организаций, о необходимости усиления мер безопасности при межсетевом взаимодействии с подразделениями и партнерами, находящимися за пределами защищенного периметра ГИСТ РТ. Обратить особое внимание на соблюдение сотрудниками

мер безопасности при получении подозрительных писем по электронной почте от неизвестных отправителей;

- организовать работу по проверке наличия актуальных резервных копий баз данных и иной компьютерной информации, необходимой для стабильной работы органа государственной власти или органа местного самоуправления;

- поручить техническим специалистам подразделений, отвечающих за информатизацию и информационную безопасность, принять меры противодействия вышеназванным уязвимостям операционных систем семейства Windows на компьютерном оборудовании под управлением данных операционных систем: отключить функцию «сжатия» в протоколе SMB v3 и ограничить функционал PREVIEW PANE, WEB CLIENT и ATMFD.DLL.