



ПРАВИТЕЛЬСТВО  
СВЕРДЛОВСКОЙ ОБЛАСТИ  
МИНИСТЕРСТВО ОБРАЗОВАНИЯ  
И МОЛОДЕЖНОЙ ПОЛИТИКИ  
СВЕРДЛОВСКОЙ ОБЛАСТИ

Мальшева ул., д. 33, Екатеринбург, 620075  
тел. (факс) (343) 312-00-04 (многоканальный)  
E-mail: info.minobraz@egov66.ru, http://minobraz.egov66.ru

07.08.2024 № 02-0282/11472

На № \_\_\_\_\_ от \_\_\_\_\_

О реализации мер защиты  
информации

Руководителям органов местного  
самоуправления, осуществляющих  
управление в сфере образования

Руководителям образовательных  
организаций, подведомственных  
Министерству образования и  
молодежной политики Свердловской  
области

Уважаемые руководители!

Министерство образования и молодежной политики Свердловской области (далее – Министерство образования) сообщает, что согласно поступившей в Министерство цифрового развития и связи Свердловской области информации от Управления Федеральной службы по техническому и экспортному контролю России по Уральскому Федеральному округу (далее – ФСТЭК России), анализ сведений об угрозах безопасности информации, проводимый специалистами ФСТЭК России в условиях сложившейся обстановки, показывает, что хакерской группировкой Cyber Anarchy Squad скомпрометирована информационная инфраструктура общества с ограниченной ответственностью «Аванпост» (далее – ООО «Аванпост»), в результате чего, предположительно, нарушителями зашифрована инфраструктура ООО «Аванпост», а также похищено 390 Гб защищаемой информации.

Отмечаем, что ООО «Аванпост» является российской компанией-разработчиком систем авторизации и аутентификации. Указанные решения применяются органами государственной власти.

В целях нейтрализации угроз безопасности информации, связанных с несанкционированным доступом к информационной инфраструктуре органов государственной власти через подрядные организации, считаем необходимым принять следующие дополнительные меры защиты:

1) сменить пароли учетных записей пользователей информационной инфраструктуры органа государственной власти, а также учетных записей пользователей программного обеспечения, разработчиком которого является ООО «Аванпост»;

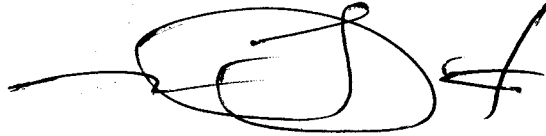
2) ограничить удаленный доступ работников ООО «Аванпост», которые осуществляют техническое сопровождение поставляемого ими программного обеспечения. В случае невозможности ограничения доступа обеспечить мониторинг действий удаленных работников ООО «Аванпост»;

3) провести внеплановое сканирование на наличие уязвимостей в инфраструктуре организации. Принять исчерпывающие меры по устранению критических уязвимостей, выявленных в ходе сканирования;

4) обеспечить резервирование информации, обрабатываемой в программном обеспечении ООО «Аванпост».

Министерство образования просит не допустить публикации указанной информации в информационно-телекоммуникационной сети «Интернет» и средствах массовой информации.

Заместитель Министра



Е.М. Бирюк