1432019/2022-8507(1)

ПРАВИТЕЛЬСТВО САНКТ-ПЕТЕРБУРГА

КОМИТЕТ ПО ОБРАЗОВАНИЮ

пер. Антоненко, дом 8, лит. А, Санкт-Петербург, 190031
Тел.(812) 417-34-54, Факс (812) 417-34-56
E-mail: kobr@gov.spb.ru
www.k-obr.spb.ru

Штамп регистрации № _____

На № _____ от _____

О мерах по повышению защищенности информационной инфраструктуры системы образования

Заместителям глав администраций районов Санкт-Петербурга

Руководителям организаций, находящихся в ведении Комитета по образованию

Уважаемые руководители!

В связи с введением в Санкт-Петербурге с 25.02.2022 режима повышенной готовности, связанного с возможностью деструктивного воздействия на информационно-коммуникационную инфраструктуру, Комитет по образованию просит принять дополнительные меры по обеспечению информационной безопасности в образовательных организациях и учреждениях, функционирующих в системе образования Санкт-Петербурга, находящихся в вашем ведении (далее – организации), с учетом информации, содержащейся в письме Министерства просвещения Российской Федерации от 03.03.2022 № 04-147 «О мерах по повышению защищенности информационной инфраструктуры системы образования» и письме Рособрнадзора от 04.03.2022 № 04-45 согласно приложению и сообщает следующее.

Комитет по образованию считает целесообразным проведение внеплановых инструктажей пользователей информационных систем и баз данных в организациях (далее – ИС), включая ИС и базы данных, содержащие персональные данные, по вопросам выполнения мер информационной защиты. В ходе проведения указанных инструктажей необходимо довести следующую информацию.

Ответственность за обеспечение защиты информации на рабочем месте пользователя возлагается непосредственно на пользователя (потребителя информации).

Необходимо регулярно создавать резервные копии всех важных документов на внешних носителях.

Недопустимо открывать почтовые вложения от неизвестных отправителей. При получении сообщения электронной почты в обязательном порядке необходимо оценивать адрес отправителя на предмет его легитимности. Недопустимо переходить по указанной в тексте письма интернет-ссылке с неизвестным адресом, если у пользователя нет уверенности в безопасности этой интернет-ссылки. В случае возникновения подозрений в небезопасности интернет-ссылки рекомендовано воспользоваться сервисом «Онлайн сканер» (https://vms.drweb.ru/online/?1ng=ru)

Руководителям организаций необходимо проинформировать сотрудников организаций:

о недопущении распространения информации о функционировании ИС и передачи администраторами и пользователями ИС своей аутентификационной информации сторонним лицам;

об ответственности за нарушение требований в области защиты информации.

Руководителям организаций необходимо:

усилить контроль над действиями администраторов и пользователей ИС;

усилить контроль за передачей информации с использованием официальной электронной почты, мессенджеров и другими способами через информационно-коммуникационную сеть Интернет;

исключить применение иностранных систем видеоконференцсвязи, в том числе Zoom, Skype, а также систем удаленного доступа (RAdmin, TeamViewer);

обеспечить контроль невозможности подключения неучтенных съемных машинных носителей информации и мобильных устройств;

обеспечить ограниченное и безопасное использование в организациях личных средств вычислительной техники (ноутбуков, планшетов, смартфонов), модемов и съемных машинных носителей информации.

Руководителям организаций в целях повышения защищенности сайтов организаций рекомендуется:

провести инвентаризацию служб и веб-сервисов, используемых для функционирования сайтов и отключить неиспользуемые службы и веб-сервисы.

усилить требования к парольной политике администраторов и пользователей сайтов, исключив при этом использование паролей, заданных по умолчанию. Отключить неиспользуемые учетные записи;

исключить применение на сайтах сервисов для подсчета и сбора данных о посетителях, их местоположении и иных сервисов, разработанных иностранными организациями (например, сервисов onthe.io, ReCAPTCHA, YouTube, Google Analytics, Google Maps, Google Translate, Google Analytics);

исключить возможность использования встроенных видео- и аудио-файлов, «виджетов» и других ресурсов, загружаемых со сторонних сайтов, заменив их при необходимости гиперссылкой на такие ресурсы.

Руководителям организаций обеспечить проведение должностными лицами, ответственными за защиту информации, на постоянной основе следующих мероприятий:

проверка наличия на автоматизированных рабочих местах и серверах активированных и настроенных сертифицированных средств антивирусной защиты;

смена административных паролей на средствах управления локальной вычислительной сети, обеспечив (при возможности) двухфакторную аутентификацию администраторов информационных систем;

проверка прав доступа пользователей к локальным и общим сетевым информационным ресурсам с автоматизированных рабочих мест;

внеплановая смена паролей пользователей, используемых для доступа к локальным и общим сетевым информационным ресурсам;

установление политики принудительного logoff в операционных системах на автоматизированных рабочих местах и серверах

приостановление установки обновлений системного программного обеспечения иностранного происхождения;

проведение аудита на наличие несанкционированных подключений к сети Интернет, и, в случае наличия, принятие мер по их закрытию;

исключение возможности удаленного управления прикладным и системным программным обеспечением, телекоммуникационным оборудованием через сеть Интернет с использованием несертифицированных средств защиты информации.

Руководителям образовательных организаций-ППЭ:

изолировать от сети Интернет все персональные компьютеры, используемые для подготовки, проведения ГИА и обработки экзаменационных работ ГИА (кроме Станции авторизации в ППЭ);

отключить автоматическое обновление операционных систем MSWindows всех серверов и персональных компьютеров, не обновлять операционные системы в ручном режиме.

Приложение: на 6 л. в 1 экз.

Заместитель председателя Комитета **М.Ю.Пучков**

Место для подписи

Губкова Н.В., 576-18-22