УПРАВЛЕНИЕ
ОБРАЗОВАНИЯ И НАУКИ
ТАМБОВСКОЙ ОБЛАСТИ

ул. Советская, 108, г. Тамбов, 392000
Тел. 72-37-38, факс 72-30-04
E-mail: post@obraz.tambov.gov.ru
ОГРН 1066829047064
ИНН 6829021123 КПП682901001
09.03.2022 № 1.01-28/867
На № _____ от _____

Руководителям органов местного самоуправления, осуществляющих управление в сфере образования

Руководителям образовательных организаций, находящихся на областном бюджете

О мерах по повышению защищенности информационной инфраструктуры системы образования

Уважаемые коллеги!

Согласно письмам ФСТЭК России от 28 февраля 2022 г. № 240/22/952, № 240/22/953 и № 240/22/960 (В. Лютиков) о подготовке к проведению компьютерных атак на информационную инфраструктуру Российской Федерации, направленных на получение конфиденциальной информации, а также на нарушение функционирования и вывод из строя информационной инфраструктуры органов государственной власти, в том числе через компрометацию и нарушения функционирования зарубежными хакерскими группировками официальных сайтов органов государственной власти и организаций Российской Федерации управление образования и науки области сообщает следующее.

Предполагается, что проведение компьютерных атак планируется осуществлять через внедрение в обновления иностранного программного обеспечения вредоносного программного обеспечения. При этом распространение обновлений с вредоносными вложениями может осуществляться через центры обновлений (официальные сайты) разработчиков иностранного программного обеспечения, размещаемые в сети «Интернет».

Учитывая изложенное, обращаем внимание на необходимость (при наличии возможности) приостановить работы по обновлению применяемого в информационных системах иностранного программного обеспечения и программно-аппаратных средств, страной происхождения которых является США и страны Европейского союза, а также исключить их автоматическое централизованное обновление посредством сети «Интернет».

Также в целях повышения защищенности информационных систем и ресурсов, включая официальные сайты органов местного самоуправления, осуществляющих управление в сфере образования, а также образовательных организаций (далее – ИСР), рекомендуем:

провести инвентаризацию служб и веб-сервисов, используемых для функционирования ИСР и размещенных на периметре информационной инфраструктуры (далее – службы и веб-сервисы);

отключить неиспользуемые службы, веб-сервисы, сайты;

усилить требования к парольной политике администраторов и пользователей ИСР, исключив при этом использование паролей, заданных по умолчанию, отключить сервисные и неиспользуемые учетные записи;

обеспечить сетевое взаимодействие с применением защищенных актуальных версий протоколов сетевого взаимодействия (HTTPS, SSH и других протоколов); исключить применение в ИСР подсчета и сбора данных о посетителях, сервисов предоставления информации о 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, интерфейсов взаимодействия API, «виджетов» и других ресурсов, загружаемых со сторонних сайтов, заменив их при необходимости гиперссылкой на такие ресурсы.

Таким образом, в целях повышения устойчивости ИСР к распределенным атакам, направленным на отказ в обслуживании (DdoS-атакам), просим:

обеспечить настройку правил средств межсетевого экранирования, направленных на блокировку неразрешенного входящего трафика;

обеспечить фильтрацию трафика прикладного уровня с применением средств межсетевого экранирования уровня приложений (web application firewall (WAF)), установленных в режим противодействия атакам;

активировать функции защиты от атак отказа в обслуживании (DDoS-атак) на средствах межсетевого экранирования и других средствах защиты информации;

ограничить количество подключений с каждого IP-адреса (например, установить на веб-сервере параметр rate-limit);

блокировать входящий трафик, поступающий с IP-адресов, страной происхождения которых являются США, страны Европейского союза или иной страной, являющейся источником компьютерных атак;

блокировать трафик, поступающий из «теневого Интернета» через Tor-браузер (список узлов, которые необходимо заблокировать содержится по адресу https://www.dan.me.uk/tornodes).

Вместе с тем, сообщаем, что анализ угроз безопасности информации, проводимый специалистами ФСТЭК России в условиях сложившейся политической обстановки, показывает, что зарубежными хакерскими группировками, в частности хакерской группировкой ANONYMOUS, в социальных сетях и мессенджерах размещается информация о призывах к администраторам информационных систем раскрыть сведения об особенностях функционирования информационных систем, предоставлении аутентификационной информации и наличии уязвимостей с целью

проникновения в информационные системы и размещения противоправной информации.

С целью предотвращения получения зарубежными хакерскими группировками информации об особенностях функционирования информационных систем просим принять дополнительные меры по следующим направлениям работ:

проинформировать администраторов и пользователей информационных систем о недопущении распространения информации о функционировании информационной системы, передаче сторонним лицам своей аутентификационной информации;

проинформировать администраторов и пользователей информационных систем об ответственности за нарушение требований в области информационной безопасности;

усилить контроль над действиями в информационной системе администраторов и пользователей;

провести внеплановую смену паролей администраторов и пользователей, используемых для доступа в информационные системы;

исключить (при возможности) удаленный доступ посредством сети «Интернет» к информационным системам для администраторов и пользователей;

обеспечить (при возможности) двухфакторную аутентификацию администраторов информационных систем.

Вышеизложенные рекомендации просим довести до сотрудников и работников местного самоуправления, осуществляющих управление в сфере образования и образовательных организаций.

Информацию о выполнении указанных мер и рекомендаций необходимо направить в ТОГБУ «Компьютерный центр» на адрес электронной почты: compcentr@obraz.tambov.gov.ru в срок до 10 марта 2022 года в соответствии с приложением.

Органам местного самоуправления, осуществляющих управление в сфере образования необходимо предоставить сводную информацию по всем образовательным организациям муниципального образования, а также по органу местного самоуправления, осуществляющего управление в сфере образования и информационно-методическому центру.

По вопросам можете обращаться в ТОГБУ «Компьютерный центр» по телефонам: 53-01-48; 47-60-05.

Приложение: архивный файл: zip (9 Кб).

Заместитель начальника управления С.И. Сусоров

С.Н. Маковеев
8 (4752) 53-01-48