ФСТЭК РОССИИ
УПРАВЛЕНИЕ ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ ПО ДАЛЬНЕВОСТОЧНОМУ ФЕДЕРАЛЬНОМУ ОКРУГУ
Ленина, д. 37, г. Хабаровск, 680030
Тел., факс (4212) 35-11-08
E-mail: dfo@fstec.ru

22.06.2022 г. № 2/1748

На № _____

Первому вице-губернатору
Хабаровского края,
председателю Совета по
информационной безопасности
при Губернаторе Хабаровского края
А.А.НИКИТИНУ

main@adm.khv.ru

О мерах по повышению защищенности информационной инфраструктуры Российской Федерации

Уважаемый Александр Александрович!

В соответствии с мерами по повышению защищенности информационной инфраструктуры (исх. Управления от 1 марта 2022 г. № 2/562) в целях повышения устойчивости сайтов органов государственной власти к распределенным атакам, направленным на отказ в обслуживании (DdoS-атакам), рекомендовано блокировать входящий трафик, поступающий с IP-адресов, страной происхождения которых являются США, страны Европейского союза или иные страны, являющиеся источником компьютерных атак.

В случае если для реализации служебных задач необходимо взаимодействие IP-адресами, принадлежащими указанным странам, возможно организовать такое взаимодействие путем реализации следующих дополнительных мер защиты информации:

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);

обеспечить мониторинг информационных ресурсов Национального координационного центра по компьютерным инцидентам (далее - НКЦКИ) на предмет выявления IP-адресов, содержащихся в бюллетенях НКЦКИ, с которых проводятся DdoS-атаки, с целью оперативного принятия мер по их блокировке.

В соответствии с мерами по повышению защищенности информационной инфраструктуры (исх. Управления от 7 марта 2022 г. № 2/601) в целях предотвращения реализации угроз безопасности информации, связанных с фишингом, рекомендовано заблокировать получение электронных писем от доменов-отправителей, страной происхождения которых являются США и страны Европейского союза.

В случае если для реализации служебных задач необходим обмен электронными письмами с организациями из указанных стран, возможно организовать такое взаимодействие путем реализации следующих дополнительных мер защиты информации:

сформировать список доменов-отправителей, страной происхождения которых являются США и страны Европейского союза, от которых предполагается получение электронной почты;

внимательно проверять адрес отправителя, даже в случае совпадения имени с уже известным контактом;

не открывать письма от неизвестных адресатов;

проверять письма, в которых содержатся призывы к действиям (например, «открой», «прочитай», «ознакомься», «вниманию»);

не переходить по ссылкам, которые содержаться в электронных письмах, особенно если они длинные или наоборот, используют сервисы сокращения ссылок (bit.ly, tinyurl.com и т.д.);

проверять ссылки, даже если письмо получено от другого пользователя информационной системы;

не открывать вложения, особенно если в них содержаться документы с макросами, архивы с паролями, исполняемые файлы;

обеспечить мониторинг информационных ресурсов НКЦКИ на предмет выявления фишинговых рассылок в органы (организации) с целью оперативного принятия мер защиты информации на основании индикаторов компрометации, содержащихся в бюллетенях НКЦКИ.

При этом необходимо провести обязательное информирование всех работников органа (организации) о необходимости выполнения мер по защите информации при открытии каждого электронного письма.

С уважением,

Исполняющий обязанности
руководителя Управления Р.Хабибулин