



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

25 июня 2022 г. № 2/1785

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!

Согласно поступившей в ФСТЭК России информации одним из векторов проведения компьютерных атак в отношении информационной инфраструктуры Российской Федерации является внедрение вредоносного программного обеспечения через почтовые вложения. Нарушители используют методы социальной инженерии, отправляя пользователям фишинговые электронные письма с вредоносным вложением.

Указанные электронные письма содержат вложения в виде электронных документов, содержащих списки участников совещания, протоколов (например, электронные документы с наименованиями «Список участников.doc» и «17.06.2022_Протокол_МРГ_Подгруппа_ИБ.doc»). Фишинговые письма направляются с адресов электронных почт, содержащий домен gmx[.]ru.

В целях предотвращения реализации указанных угроз безопасности информации считаем необходимым принять следующие дополнительные меры по защите информации:

заблокировать доставку писем от домена-отправителя gmx[.]ru;

обновить базы антивирусных средств защиты до актуальных версий;

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.

Проинформировать пользователей информационной системы о необходимости безопасной работы с электронной почтой, а именно:

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

не открывать письма от неизвестных адресатов;

не открывать вложения, особенно если в них содержатся документы с макросами, архивы с паролями, исполняемые файлы.

Руководителя Управления

С. У. [подпись], *[подпись]*

В.Цалко