



СЛУЖБА БЕЗПЕКИ УКРАЇНИ

вул. Володимирська, 33, м. Київ, 01601, тел./факс: (044) 226-34-31, тел. 256-99-05
www.sbu.gov.ua, e-mail: sbu_cu@ssu.gov.ua Код ЄДРПОУ 00034074

19.09.18 № *99/664*

На № _____ від _____

Прим. № 1

**Прем'єр-Міністру України
Гройсману В.Б.**

*Щодо порушень порядку використання
державних інформаційних ресурсів*

Шановний Володимире Борисовичу!

Службою безпеки України у ході реалізації заходів з контррозвідувального захисту інтересів держави у сфері кібернетичної безпеки отримано дані про передумови до несанкціонованого доступу і зміни інформації, що є власністю держави, яка розміщується на офіційних веб-ресурсах та поштових сервісах органів державної влади України.

За результатами аналізу інформації оприлюдненої на загальнодоступних ресурсах мережі Інтернет було виявлено реквізити доступу користувачів до акантів у соціальних мережах "ВКонтакте" та "LinkedIn", месенджера миттєвих повідомлень "Qip", реєстрація на яких відбувалась з використанням службових електронних поштових скриньок в доменній зоні "@.gov.ua". посадовими особами органів державної влади та місцевого самоврядування України.

У соціальній мережі "ВКонтакте" 257 записів створено з використанням поштових адрес у домені "@bank.gov.ua" (Національний банк України), 117- "@rada.gov.ua" (Верховна Рада України), 52 – "@kmu.gov.ua" (Кабінет Міністрів України), 26 - "@moz.gov.ua" (Міністерство охорони здоров'я).

Зазначене створює умови для проведення спецслужбами РФ комп'ютерної розвідки, з використанням інформації російських соціальних мереж та несанкціонованого отримання доступу до державних електронних інформаційних ресурсів України.

Оприлюднена у 2018 році база клієнтів безкоштовного хостингу "000webhost" (РФ) за 2015 рік містить 20 облікових записів, створених за допомогою поштових адрес в доменній зоні gov.ua (Міністерства оборони, Національного банку, Державної міграційної служби, ГУ ДКСУ у Волинській обл., ДП "Укренерго").

За результатами моніторингу веб-ресурсів в доменній зоні "gov.ua" встановлено, що українському діапазону IP - адрес відповідає 2363 із 2659, закордонним провайдерам – 265 (РФ - 19, США – 76, ФРН – 89, Велика Британія – 45, Нідерланди – 17), що свідчить про розміщення програмно-

ДЕПАРТАМЕНТ ДОКУМЕНТООБІГУ ТА КОНТРОЛЮ
СЕКРЕТАРІАТУ КАБІНЕТУ МІНІСТРІВ УКРАЇНИ
№ 37838/0/1-18 від 24.09.2018



21

15:50:15

21-0609

технічних засобів, на яких розміщуються зазначені державні електронні інформаційні ресурси поза межами України.

Державні органи, веб-ресурси яких обслуговуються іноземними провайдерами телекомунікацій: РФ - Національна комісія, що здійснює державне регулювання у сфері комунальних послуг (<http://nkr.gov.ua>), ГУ Держтехногенбезпеки в АР Крим (<http://arkditb.gov.ua>), Головне управління юстиції Міністерства юстиції України в АР Крим (<http://minjust-crimea.gov.ua>), Пенсійний фонд України в Новоайдарському районі (<http://naydar-pfu.gov.ua>), Асоціація міжнародних автомобільних перевізників України (<http://smar.gov.ua>), Управління Укртрансінспекції у Львівській області (<http://uti-lviv.gov.ua>); ФРН - Державний архів Закарпатської області (<http://dazo.gov.ua>), Департамент сім'ї, молоді та спорту Донецької ОДА (<http://donsportmolod.gov.ua>), Київська міська рада (<http://kmr.gov.ua>), Головне територіальне управління юстиції у Львівській області (<http://obljustlviv.gov.ua>), Відділ безпеки дорожнього руху Управління превентивної діяльності ГУ НП в Чернігівській області (<http://saichn.gov.ua>); Велика Британія - Департамент агропромислового розвитку Херсонської ОДА (<http://apk-kherson.gov.ua>), Прокуратура Рівненської області (<http://pro.gov.ua>), Державне агентство резерву України (<http://rezerv.gov.ua>), Департамент молоді та спорту виконавчого органу Київської міської ради (<http://sms.gov.ua>); Нідерланди - Департамент економічного розвитку і торгівлі Тернопільської ОДА (<http://economy-te.gov.ua>), Департамент освіти та науки Одеської міської ради (<http://osvita-omr.gov.ua>).

Крім того встановлено, що 29 органів державної влади та місцевого самоврядування, використовують для службового листування серверне обладнання компанії Yandex.Ru (обладнання територіально знаходиться в РФ, а компанія перебуває під санкціями України), при цьому електронні поштові скриньки посадових осіб зареєстровані у доменній зоні "@.gov.ua".

Державні органи, що використовують для службового листування поштовий сервіс Yandex.Ru: Інвестиційний портал Київської обл. (<http://invest-koda.gov.ua>), Харківський апеляційний адміністративний суд (<http://khaas.gov.ua>), Державна бюджетна установа "Київський обласний центр з інвестицій та розвитку" (<http://kosz.gov.ua>), Виконавча дирекція Київського обласного відділення Фонду соціального страхування з тимчасової втрати працездатності (<http://krfse.gov.ua>), ГУ юстиції Міністерства юстиції України в АР Крим (<http://minjust-crimea.gov.ua>), Асоціація міжнародних автомобільних перевізників України (<http://smar.gov.ua>), Головне територіальне управління юстиції у Сумській області (<http://sumyjust.gov.ua>), Український державний фонд підтримки фермерських господарств (<http://udf.gov.ua>), Український фонд підтримки підприємництва (<http://ufpp.gov.ua>), Управління Укртрансінспекції у Львівській обл. (<http://uti-lviv.gov.ua>).

Також слід зазначити, що 123 поштові сервери органів державної влади та місцевого самоврядування, які зареєстровані у доменній зоні "gov.ua", розміщені за межами України (РФ – 6, ФРН – 42, США – 34, Нідерланди – 13, Франція – 6, Велика Британія – 8).

Державні органи, поштові сервери яких розміщено поза межами України: РФ - Козелецька районна рада Чернігівської обл. (kozrada.gov.ua); ФРН - Державна екологічна інспекція в Івано-франківській обл. (ifdei.gov.ua), Донецька ОДА (mail.dn.gov.ua), Головне територіальне управління юстиції у Львівській обл. (obljustlviv.gov.ua); США – Департамент культури, туризму та курортів Херсонської ОДА (visitkherson.gov.ua), Головне територіальне управління юстиції у Тернопільській обл. (terjust.gov.ua), Нідерланди – Департамент економічного розвитку і торгівлі Тернопільської ОДА (economy-te.gov.ua), Управління адміністративних послуг Полтавської міської ради (snpa-pl.gov.ua), Департамент освіти і науки Луганської ОДА (oblosvita-lg.gov.ua); Франція – Відділ освіти Краснокутської РДА

Харківської обл. (osvita-krk.gov.ua); Велика Британія - Уманська РДА Черкаської обл. (umanrda.gov.ua), Управління соціального захисту населення Охтирської РДА Сумської обл. (ruszn-okhtyrka.gov.ua), Каланчацька РДА Херсонської обл. (mail.rda-kalanchak.gov.ua).

Окреме занепокоєння викликає наявність на 92 сайтах доменної зони "gov.ua" програмних модулів виробництва "Яндекс.Метрики" та 11 – "Rambler. Топ 100". Зазначене окрім широкого функціоналу зі збору інформації про відвідувачів сайту надає можливість здійснювати вибіркове "оновлення", що створює умови для виконання шкідливого програмного коду на комп'ютерах користувачів сайтів українських державних органів та установ та компрометації ресурсу шляхом перехоплення сесій адміністраторів.

Таким чином, проведений аналіз вказує на порушення посадовими особами державних органів вимог постанови Кабінету Міністрів України від 21.10.15 № 851 "Деякі питання використання доменних імен державними органами в українському сегменті Інтернету", а також про неправомірне використання наданих їм у службове користування засобів комунікацій, що створює сприятливі умови для компрометації їх облікових записів, несанкціонованого доступу третіх осіб до державних електронних інформаційних ресурсів та проведення спецслужбами держави-агресора акцій деструктивного кібернетичного та інформаційного впливу на Україну.

З метою усунення вказаних загроз кібернетичній безпеці держави та унеможливлення проведення заходів комп'ютерної розвідки, пропонуємо надати доручення:

- Державній службі спеціального зв'язку та захисту інформації України опрацювати питання щодо запровадження системи норм та правил використання службовими особами мережі Інтернет (службової електронної пошти), а також контролю доступу до неї для протидії несанкціонованим втручанням та ураженням шкідливим програмним забезпеченням інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем державних установ;

- міністерствам та іншим органам виконавчої влади, місцевого самоврядування привести у відповідність до вимог постанови Кабінету Міністрів України від 21.10.15 № 851 функціонування офіційних веб-сайтів та поштових сервісів.

З повагою

Голова Служби



В. Грицак