РАДА НАЦІОНАЛЬНОЇ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

НАЦІОНАЛЬНИЙ КООРДИНАЦІЙНИЙ ЦЕНТР КІБЕРБЕЗПЕКИ

вул. Петра Болбочана, 8, м. Київ, 01601, телефон: (044) 255-06-50, телефакс: (044) 255-05-85

17.04.20 № 1035/16-04/2-20

Міністерства, інші центральні органи виконавчої влади, обласні державні адміністрації та суб'єкти господарювання України
(за списком)

У зв'язку із протиепідемічними заходами в Україні установами, підприємствами та організаціями застосовується дистанційний режим роботи, в ході якого масово використовуються засоби електронних комунікацій, сервіси відеозв'язку та обміну інформацією в мережі Інтернет, а також віддаленого доступу до службових інформаційних систем.

Указана ситуація активно використовується хакерськими угрупованнями для цілеспрямованих кібератак з метою проникнення до мереж органів державної влади та об'єктів критичної інфраструктури.

Національним координаційним центром кібербезпеки (далі – НКЦК) на цей час фіксується критичне збільшення кіберінцидентів та порушень інформаційної безпеки, пов'язаних з використанням зазначених засобів комунікацій, віддаленим доступом та адмініструванням інформаційних систем.

До такої ситуації, в першу чергу, призводить нехтування вимогами законодавства у сфері захисту інформації при здійсненні передачі даних з використанням мережі Інтернет.

Зокрема, відповідно до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах», постанов Кабінету Міністрів України від 29 березня 2006 року № 373, від 19 червня 2019 року № 518, від 14 травня 2015 року № 303 передача службової і таємної інформації здійснюється у зашифрованому вигляді або захищеними каналами зв'язку, державні органи з метою здійснення захищеного інформаційного обміну використовують ресурси Національної телекомунікаційної мережі. Для інформаційного обміну службовою інформацією державні органи та органи місцевого самоврядування використовують ресурси Національної системи конфіденційного зв'язку.

Ураховуючи викладене, онлайн-сервіси відеоконференцій, офісних додатків загального призначення, зокрема Zoom, Skype, Team, Webex,

Whatsapp, не можуть використовуватися для передачі вказаної інформації з обмеженим доступом.

На сьогодні в сервісі Zoom виявлено вразливості, які надають можливість прихованого віддаленого доступу до комп'ютера користувача, втручання у роботу, несанкціонованого перехоплення та запису відео- та іншої інформації. У результаті витоку інформації на цей час у мережі Інтернет доступна база даних користувачів Zoom, яка містить понад 500 000 записів, у тому числі персональні дані.

Крім того, організація віддаленого доступу до інформаційних та інформаційно-телекомунікаційних систем повинна здійснюватися з використанням засобів мережевого захисту з обов'язковою ідентифікацією та автентифікацією користувачів (щонайменше з використанням унікального імені користувача та пароля). Перелік уповноважених для віддаленого доступу працівників повинен бути затверджений відповідним розпорядженням (наказом).

Використання вбудованих в операційні системи (Microsoft Windows, Apple macOS та ін.) засобів віддаленого доступу (віддалений робочий стіл RDP, VNC, спільний доступ до файлів тощо) із налаштуваннями за замовчанням не забезпечує захисту від кібератак, у тому числі внаслідок підбору паролів та експлуатації відомих вразливостей.

Загальні вимоги до кіберзахисту та правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах встановлені Кабінетом Міністрів України постановами від 29 березня 2006 року № 373, від 19 червня 2019 року № 518.

У разі виявлення кіберінцидентів, кібератак, несанкціонованих дій в інформаційних системах, порушень інформаційної безпеки необхідно невідкладно (протягом доби) інформувати Адміністрацію Держспецзв'язку та НКЦК.

Особи, винні у порушенні вимог законодавства у сферах електронних комунікацій та захисту інформації, кібербезпеки, державної таємниці, несуть відповідальність згідно із законом.

Просимо довести вказану інформацію до співробітників вашої організації та підпорядкованих підрозділів і забезпечити неухильне дотримання вимог законодавства у цих сферах.

Фахівці НКЦК готові надавати консультаційну та технічну допомогу щодо організації безпечного використання інформаційних та інформаційно-комунікаційних систем. Інформацію про кіберінциденти, запити на отримання допомоги необхідно направляти на електронну адресу НКЦК: cyber@rnbo.gov.ua або звертатися за телефоном (044) 255-06-37.

Заступник Секретаря
Ради національної безпеки
і оборони України,
заступник керівника Національного
координаційного центру кібербезпеки **Сергій ДЕМЕДЮК**

Ради національної безпеки і оборони України
СЛУЖБА ОРГАНІЗАЦІЙНОЇ РОБОТИ ТА КОНТРОЛЮ