УКРАЇНА
ЛЬВІВСЬКА ОБЛАСНА ДЕРЖАВНА АДМІНІСТРАЦІЯ
УПРАВЛІННЯ З ПИТАНЬ ЦИФРОВОГО РОЗВИТКУ
вул. В. Винниченка, 18, м. Львів 79008, тел.: (032) 299-92-49
e-mail: thedigital@loda.gov.ua, код ЄДРПОУ 44634695
_____ № _____ На № _____ від _____

Керівнику апарату
облдержадміністрації
Ірині ШУРПЯК

Керівникам структурних
підрозділів
облдержадміністрації

Районним військовим
адміністраціям

Щодо посилення кіберзахисту

Генеральним штабом Збройних Сил України прогнозується висока ймовірність проведення напередодні Дня Незалежності України кібератак, спрямованих на державні інформаційні ресурси, інформаційно-комунікаційні системи органів державної влади та місцевого самоврядування, державних та приватних установ, організацій та підприємств, а також постачальників електронних комунікаційних мереж та послуг.

Враховуючи вимоги статей 3 і 17 Закону України «Про правовий режим воєнного стану» та з метою забезпечення сталого функціонування зазначених вище державних інформаційних ресурсів, інформаційно-комунікаційних систем просимо проінформувати керівників підприємств, установ та організацій у сфері вашого управління щодо:

вжиття невідкладних заходів з посилення кіберзахисту напередодні Дня Незалежності України (додаються);

організації цілодобового чергування осіб, відповідальних за забезпечення захисту інформації та кібербезпеки (кіберзахисту);

заборони висвітлення в засобах масової інформації даних про кіберінциденти (кібератаки);

забезпечення невідкладного інформування про виявлені кіберінциденти (кібератаки), що потенційно можуть становити кібер загрозу національній безпеці держави та передачу телеметричної інформації про кіберінциденти до:

CERT_UA на електронну адресу: cert@cert.gov.ua; за телефоном: (044)-281-88-05/(044)-281-88-25 або за допомогою форми на сайті https://cert.gov.ua.contact-us через офіційну сторінку команди на Facebook: https://www.facebook.com/UACERT;

Департамент кіберполіції Національної поліції України на електронну адресу: incident@cyberpolice.gov.ua;

Ситуаційного центу забезпечення кібербезпеки Служби безпеки України на електронну адресу: incident@dis.gov.ua; за телефоном (093)-34823-34;

Генерального штабу Збройних Сил України на електронну адресу: Cub.doc@post.mil.gov.ua

Додаток: на 4 арк.

Начальник управління **Максим СТОЛЯРЧУК**

Іващенко Юрій 2999249

МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ
ГОЛОВНОКОМАНДУВАЧ ЗБРОЙНИХ СИЛ УКРАЇНИ

Повітрофлотський проспект, 6, м. Київ, 03168, Тел.: (044) 234-71-52 Факс: (044) 226-20-15
E-mail: kabmin_doc@mil.gov.ua Код згідно з СДРПОУ 24966552

від "__" _____20__ р. № _____ На № _____ від "__" _____20__ р.

Прем'єр-міністру України
Денису ШМИГАЛЮ

Шановний пане Прем'єр-міністре!

Відповідно до Закону України "Про основні засади забезпечення кібербезпеки України" Генеральний штаб Збройних Сил України впроваджує в умовах надзвичайного і воєнного стану заходи із забезпечення кіберзахисту критичної інформаційної інфраструктури, важливих об'єктів, які мають загальнодержавне значення, в тому числі шляхом здійснення інформаційно-аналітичної діяльності.

В ході виконання вищезазначеного завдання Генеральним штабом Збройних Сил України прогнозується висока ймовірність проведення напередодні Дня Незалежності України кібератак, спрямованих на державні інформаційні ресурси, інформаційно-комунікаційні системи органів державної влади та місцевого самоврядування, державних та приватних установ, організацій та підприємств, а також постачальників електронних комунікаційних мереж та послуг.

Враховуючи вимоги статей 3 і 17 Закону України "Про правовий режим воєнного стану" та з метою забезпечення сталого функціонування зазначених вище державних інформаційних ресурсів, інформаційно-комунікаційних систем, прошу Вас надати доручення керівникам центральних та місцевих органів виконавчої влади, а також підприємств, установ та організацій, роботу яких спрямовує Кабінет Міністрів України та/або відповідні органи виконавчої влади, щодо:

вжиття невідкладних заходів з посилення кіберзахисту напередодні Дня Незалежності України (додаються);

організації цілодобового чергування осіб, відповідальних за забезпечення захисту інформації та кібербезпеки (кіберзахисту);

заборони висвітлення в засобах масової інформації даних про кіберінциденти (кібератаки);

забезпечення невідкладного інформування про виявлені кіберінциденти (кібератаки), що потенційно можуть становити кібер загрозу національній

безпеці держави, та передачу телеметричної інформації про кіберінциденти (кібератаки) до:

CERT-UA на електронну адресу: cert@cert.gov.ua; за телефоном: (044)-281-88-05/(044)-281-88-25 або за допомогою форми на сайті https://cert.gov.ua/contact-us через офіційну сторінку команди на Facebook: https://www.facebook.com/UACERT;

Департаменту кіберполіції Національної поліції України на електронну адресу: incident@cyberpolice.gov.ua;

Ситуаційного центру забезпечення кібербезпеки Служби безпеки України на електронну адресу: incident@dis.gov.ua; за телефоном: (093)-348-23-34;

Генерального штабу Збройних сил України на електронну адресу: Cub.doc@post.mil.gov.ua.

Додаток: Заходи з посилення кіберзахисту державних інформаційних ресурсів, інформаційно-комунікаційних систем напередодні Дня Незалежності України, на 2 арк..

З повагою

Головнокомандувач Збройних Сил України
генерал Валерій ЗАЛУЖНИЙ

Додаток

ЗАХОДИ
з посилення кіберзахисту державних інформаційних ресурсів,
інформаційно-комунікаційних систем напередодні
Дня Незалежності України

Для попередження та зменшення наслідків від можливих кібервпливів, спрямованих на державні інформаційні ресурси, інформаційні та комунікаційні системи органів державної влади та місцевого самоврядування, державних та приватних установ, організацій та підприємств, а також постачальників електронних комунікаційних мереж та послуг рекомендуємо вжити наступні заходи:

1. Провести роз'яснювальну роботу з працівниками щодо правил використання службових поштових скриньок, дотримання правил кібергігієни, політики використання паролів, заборони використання неліцензійного програмного забезпечення, а також програмного забезпечення країни-агресора.

2. Забезпечити постійний контроль за актуальністю операційних систем, що використовуються як на серверному обладнанні так і у кінцевих користувачів, а саме оновлення, наявність вразливостей (CVE) та подальше усунення недоліків, в тому числі щодо веб-ресурсів.

3. Провести сканування локальних мереж, кінцевих мережевих точок та сервісів що в ній знаходяться на предмет відкритих недокументованих портів та можливих вразливостей.

4. Здійснити перевірку ПЕОМ адміністраторів мережі та критично важливих вузлів системи на наявність підозрілих процесів і програм (наприклад: системних служб, що запускаються не зі стандартного розташування; програм, що не мають цифрового підпису виробника, тощо).

5. Забезпечити проведення аналізу трафіку на предмет підозрілих активностей за допомогою спеціалізованого програмного забезпечення типу snort, Suricata чи іншого аналогічного програмного забезпечення.

6. Забезпечити контроль за обліковими записами адміністраторів мережевого та серверного обладнання, за можливості використовувати ключі (сертифікати) або складні паролі, періодично їх змінюючи.

7. З метою захисту публічних сервісів від DDoS атак провести, за можливості, зміну IP адрес, та забезпечити використання сервісів Cloudflare або аналогічних.

8. Провести перевірку роботи логування та створення резервних копій (за правилом 3-2-1) критично важливих систем (сервісів), здійснити резервне копіювання та забезпечити зберігання резервних копій на окремих носіях.

9. Дотримуватися рекомендацій CERT-UA, які знаходяться за посиланнями https://cert.gov.ua/recommendation/11388,https://cert.gov.ua/article/17580.

10. Обмежити доступ до інформаційно-комунікаційних систем, серверного та комп'ютерного обладнання, які не будуть використовуватися та функціонування яких не є критичним на період свята.

Начальник Центрального управління зв'язку
та кіберборотьби Генерального штабу
Збройних Сил України
бригадний генерал Олексій КОВАЛЕНКО