МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Державний вищий навчальний заклад
«КРИВОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ»

РОЗПОРЯДЖЕННЯ

03 листопада 2017 року м.Кривий Ріг № 43

Щодо протидії загрозам функціонуванню інформаційно-телекомунікаційних систем

Відповідно до листів Міністерства освіти і науки України від 28.09.2017 р. № 1/9-408 та Департаменту освіти і науки Дніпропетровської обласної державної адміністрації від 17.10.2017 №5536/0/211-17 з метою уникнення кіберзагроз в інформаційно-телекомунікаційній системі ДВНЗ «Криворізький національний університет» вважається за доцільне:

1. Деканам факультетів, завідувачам кафедр, керівникам структурних підрозділів, працівникам університету взяти до відома вищезазначені листи, використовувати рекомендації під час роботи на офіційному веб-сайті університету та з корпоративною поштою.

2. Керівникам структурних підрозділів, начальнику ІОЦ:

- заборонити використання особистих технічних засобів у складі виробничих автоматизованих систем (USB-флеш накопичувачі);

- заборонити підключення до комп'ютерів університету технічних засобів із модулями передачі даних (Bluetooth, GSM тощо), призначених для створення каналів зв'язку з мережами загального користування та іншими електронними пристроями;

- заборонити використання студентами та співробітниками мережі університету для доступу до особової електронної пошти, загальнодоступних та соціально-орієнтованих ресурсів мережі Інтернет;

- забезпечити неприпустимість відкриття вкладень у підозрілих повідомленнях (у листах від адресатів, щодо яких виникають сумніви; наприклад: автор з невідомих причин змінив мову спілкування; тема листа є нетиповою для автора, спосіб, у який звертається автор до адресата, є нетиповим, тощо; а також у повідомленнях із нестандартним текстом, що спонукають до переходу на підозрілі посилання або до відкриття підозрілих файлів – архівів, виконуваних файлів та ін.);

- користувачам в разі інфікування персонального комп'ютера не перезавантажувати систему;

- заборонити запуск виконуваних файлів (*.exe) на комп'ютерах з директорій %TEMP%, %APPDATA%.

3. Системним адміністраторам, начальнику ІОЦ:

- забезпечити фільтрування вхідних/вихідних інформаційних потоків, зокрема поштового та веб-трафіку;

- контактні електронні поштові скриньки, які зазначені на офіційному веб-сайті університету перевести з символьного типу до графічного, для ускладнення процедури автоматичного збору та аналізу відомостей потенційними зловмисниками в майбутньому;

- підвищити захищеність інформаційно-телекомунікаційних систем за допомогою актуальних версій антивірусного програмного забезпечення;

- встановити офіційний патч Microsoft Security Bulletin MS17-010-Critical;

- на мережевому обладнанні та груповими політиками заблокувати на системах та серверах порти 135, 445, 1024-1035 TCP.

- для можливості відновлення зашифрованих файлів користатися програмами ShadowExplorer або PhotoRec.

Ректор М.І. Ступнік