Додаток 1
до наказу «Про порядок дій відповідних структурних підрозділів КПІ ім. Ігоря Сікорського у разі виявлення кіберінцидентів та/або кібератак та затвердження рекомендацій адміністраторам телекомунікаційної системи та автоматизованих інформаційних систем КПІ ім. Ігоря Сікорського щодо превентивних заходів задля упередження руйнівних наслідків кіберінцидентів та/або кібератак»

РЕКОМЕНДАЦІЇ АДМІНІСТРАТОРАМ ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ ТА АВТОМАТИЗОВАНИХ ІНФОРМАЦІЙНИХ СИСТЕМ КПІ ІМ. ІГОРЯ СІКОРСЬКОГО ЩОДО ПРЕВЕНТИВНИХ ЗАХОДІВ ЗАДЛЯ УПЕРЕДЖЕННЯ РУЙНІВНИХ НАСЛІДКІВ КІБЕРІНЦИДЕНТІВ ТА/АБО КІБЕРАТАК

КИЇВ 2022

1. Використовувати програмний або апаратний міжмережевий екран (брандмауер), за можливості – поштовий шлюз і штатні засоби захисту операційних систем (далі – ОС) від шкідливого програмного забезпечення та кіберзагроз.

2. Забезпечити регулярне резервне копіювання даних до захищених банків даних (накопичувачів), які мають можливість здійснювати аутентифікацію користувача.

3. Розробляти в підрозділах плани реагування на кіберінциденти, визначити відповідальну особу.

4. Зменшити ймовірність розповсюдження шкідливого програмного забезпечення у мережі шляхом:

– створення політик, що дозволяють завантажувати файли лише тих типів, які мають надходити (наприклад, заборонити отримання чи передання EXE-файлів);

– блокування вебсайтів, які є шкідливими;

– перевірки антивірусними програмами файлів, що викликають підозру;

– обов'язкової перевірки EXE-файлів, у разі сумнівів у легальності роботи програмного забезпечення (далі – ПЗ), за допомогою програмних комплексів антивірусного забезпечення, наприклад: https://www.virustotal.com/gui/home/upload.

5. Під час використання віддаленого доступу дозволити підключення лише визначеним користувачам за допомогою «білого списку», додати можливість автентифікації користувачів у системі, налаштувати контроль та політику доступу того чи іншого користувача.

6. Нагадувати користувачам автоматизованих інформаційних систем та телекомунікаційних систем підрозділів щодо необхідності:

– запуску ПЗ з надійних джерел або таке ПЗ, що має відповідні сертифікати розробників, і лише після його FAST-сканування антивірусним ПЗ. У разі потреби запуску несертифікованого ПЗ – використовувати віртуальні машини;

– використання антивірусного ПЗ із технологією евристичного аналізу та своєчасним оновленням його бази сигнатур;

– вимкнення або обмеження використання макросів у Microsoft Office;

– вмикання автоматичного оновлення для операційних систем і ПЗ (своєчасного встановлення);

– використання двофакторної автентифікації;

– періодичної (раз на місяць) примусової зміни паролів особистих і робочих облікових записів (зокрема паролів від поштових скриньок);

– уникнення введення паролів облікових записів у формах підозрілих вебсайтів або додатків, що приходять на пошту або іншими засобами зв'язку;

– уникнення відкриття файлів й додатків у поштових повідомленнях від підозрілих відправників (обов'язково попередньо перевіряти адресу відправника);

– уникнення використання робочих адрес електронної пошти та номерів телефону для реєстрації в соціальних мережах або для розміщення особистих оголошень;

– обов’язкової попередньої перевірки вмісту зовнішніх носіїв інформації (USB-флеш) засобами антивірусного захисту з оновленими сигнатурами;

– уникнення збереження даних для автентифікації в легкодоступних місцях (наприклад, на робочому столі). Паролі мають складатися зі стійких парольних фраз, що містять великі / маленькі літери, службові символи, цифри. Для зберігання паролів необхідно використовувати менеджери паролів (наприклад, KeePass). Менеджер паролів і кредити доступу до нього не можуть зберігатись на робочому столі.

7. Встановити сертифіковане програмне забезпечення моніторингу мережевого трафіку та іншого програмного забезпечення, яке може викликати підозру щодо наявності шкідливого програмного коду тощо (Cisco Umbrella, мережеві фільтри).