Токар О. А.,
Федченко С. І.
Харківський національний університет
Повітряних Сил імені Івана Кожедуба

КІБЕРЗАХИСТ В СУЧАСНОМУ ІНФОРМАЦІЙНОМУ СЕРЕДОВИЩІ ТА ШЛЯХИ ПРОТИДІЇ КІБЕРАТАКАМ

Кібератака, на разі може статись в будь-який час , і на будь – якій інфраструктурі. Питання кібербезпеки просто неможливо ігнорувати, особливо під час війни.

За статистикою, від витоку інформації потерпають, всі інфраструктури, а особливо критичні. В будь – якій організації, підприємстві, тощо, повинен бути фахівець з кібербезпеки. У разі надзвичайної ситуації, який повинен, захистити дані та конфіденційну інформацію установи, оперативно налаштувати внутрішні процеси.

З початку війни розрізнені команди працюють по всій Україні, люди можуть підключатися до слабо захищених мереж, тим самим передавати дані зловмисникам. За кілька секунд хакери-злочинці можуть отримати інформацію з ваших пристроїв. Краще використовувати мобільний інтернет, який, за необхідності, можна роздати для підключення ноутбуків. Також можна використовувати VPN, що дасть змогу анонімізувати трафік. Не передавайте, не зберігайте особливо важливу інформацію в загальних папках на комп'ютері, будь-яких месенджерах, не передавайте її через електронну пошту, використовуйте захищені канали зв’язку. Коли надсилаєте якісь документи через соціальні мережі, подумайте про те, що копія цього файлу залишиться в листуванні та до неї зможуть отримати доступ треті особи. Використовуйте функцію автовидалення листування, вона доступна як в загальних чатах, так і в секретних чатах. Встановіть надійні паролі на корпоративні пошти, та на всі месенджери. Паролі мають бути різними для різних ресурсів, щоб у разі злому одного сервісу зловмисники не могли отримати доступ до іншого. Зазвичай найслабші місця – це не системи, а люди, які працюють. Треба проводити лекції тренінги з кібербезпеки співробітникам.

Загрозу безпеки інфраструктур становлять не лише прямі дії хакерів-злочинців, а й зараження техніки вірусами. Тому до безпеки та захисту інформації необхідно підходити комплексно. Є базовий рівень захисту інформації – це встановлення ліцензійного програмного забезпечення, антивірусів. Усі додаткові способи захисту краще довірити фахівцям. Якщо на підприємстві є неліцензійне програмне забезпечення, його треба негайно замінити.

Питання безпеки повинно бути під контролем. У разі кібератаки необхідно відключити пристрій від мережі. За можливості, з іншого пристрою через іншу мережу спробувати змінити пароль доступу до корпоративної пошти та інших ресурсів.

Обов’язково потрібно виконувати рекомендації спеціалістів з кібербезпеки. У разі витоку інформації фахівець зможе відстежувати, коли, ким, кому передавалася та чи інша інформація.

Вимоги для максимального захисту автоматизованих систем управління:

- систематично оновлювати і сканувати ПК;
- застосовувати тільки ліцензійні версії програм для роботи;
- антивірусний захист;
- здійснювати перевірку змінних носіїв, перед їх використанням в систему;
- відстежувати видалені робочі місця;
- стежити за безпекою мереж;
- регулярно змінювати паролі для користувачів системи;
- користуватися шифрованими з'єднаннями;
- блокувати шкідливі вебресурси;
- зберігання електронних архівів, архівів особливо важливих даних;
- зберігання програмних засобів, необхідних для відновлення змісту баз даних;
- термін зберігання даних;
- можливості переміщення носіїв до спеціально обладнаних місць зберігання.

При виникненні надзвичайних ситуацій необхідно оперативно визначити, оцінити і обробити загрозу, настання якої впливає на діяльність всієї інфраструктури в цілому. По можливості швидко забезпечити відновлення діяльності роботи системи. Здійснити резервне копіювання баз даних та інших особливо важливих даних.

Отже, кібератака і кібербезпека сьогодні стає невід’ємним трендом у нашій країні. Але найголовніше – всім варто розуміти, що кібербезпека починається з дотримання прописаних правил і персональної відповідальності кожного. Тренінги і навчання не дадуть можливості забути про важливість кібербезпеки, що дозволить мінімізувати ймовірність того, що саме необізнаність персоналу спричинить пролом у системі безпеки.