В Україні польоти БПЛА здійснюються відповідно до законодавства у галузі державної авіації України. Проте законодавча база у цій сфері ще потребує суттєвого удосконалення.

Список використаних джерел:

1. Gettinger D. The Drone Databook. The Center for the Study of the Drone at Bard College, 2019. 320 p.

2. Tal D., Altschuld J. Drone Technology in Architecture, Engineering, and Construction: A Strategic Guide to Unmanned Aerial Vehicle Operation and Implementation. Wiley, 2021. 168 p.

3. Um J.-S. Drones as Cyber-Physical Systems Concepts and Applications for the Fourth Industrial Revolution and Implementation. Springer, 2019. 274 p.

УДК 004.043

БАРАБАШ ВІТАЛІЙ ОЛЕКСАНДРОВИЧ

студент 1 курсу групи Ф6-Кбдср-21-1 факультету № 6

Харківського національного університету внутрішніх справ

ТУЛУПОВ ВОЛОДИМИР ВОЛОДИМИРОВИЧ

кандидат технічних наук, доцент,

доцент кафедри кібербезпеки та DATA-технологій факультету № 6

Харківського національного університету внутрішніх справ

ДЕЯКІ ПИТАННЯ ПРЕВЕНТИВНОГО ЗАХИСТУ ПРИВАТНОСТІ ІНФОРМАЦІЇ

Метою доповіді є питання превентивності захисту приватності інформації в разі втрати або викрадення пристрою на системі Windows 10.

На теперішній час слід констатувати, що ми стали занадто довіряти звичайному паролю на своїх пристроях, завдяки яким ми можемо працювати та досить відверто спілкуватися з іншими людьми.

Як правило у нас на комп’ютері встановлені останні версії антивірусів, налаштовані брандмауери, останні збірки Windows, встановлені паролі на

облікові записи. Звісно, всі ці міри безпеки можуть захистити нас та нашу інформацію від злочинців в мережі, але не при фізичному контакті нашого пристрою з руками зловмисника. У кожного користувача є данні, які можуть нашкодити власнику, але в нашому випадку, витік даних може нашкодити безпеці інших людей.

При фізичному доступі до нашого пристрою, звичайний пароль, код, фізичний ключ або відбиток пальців може обійтися за допомогою сторонніх програм, які потребують завантаження через Dos, що дозволяє редагувати файл SAM, який, при штатній роботі системи, охороняється та контролюється процесом lass.exe від втручання, навіть від адміністратора системи.

Для вирішення цього питання на теперішній час існує два найпопулярніших рішення для таких дій, це Kon-boot та Offline NT password & registry editor. Кожен з них має свої недоліки та привілеї.

Kon-boot використовується для одноразового доступу до системи й не чіпає файлів системи, бо робота системи, при такому завантажені, схожа на Live CD в Linux.

Offline NT password редактує на постійній основі файл SAM, що дозволяє входити в систему без використання flash накопичувача з Bootloader’ром. Всі ці рішення працюють лише при вимкненому в BIOS режимі Secure Boot, його можна перемикати в будь-який час, якщо в BIOS не був встановлений пароль.

Якщо зловмиснику не потрібна робота з нашого облікового запису, а лише данні з диску, тоді можна просто дістати диск та підключити до іншого комп’ютера або використовувати Live CD образ будь-якої збірки Linux.

Таке завантаження досить часто не потребує втручання до налаштувань BIOS, так як більшість Uefi Bios та деякі Legacy, мають окреме меню для одноразового запуску з системного диску або flash носія Linux.

Дізнатися про комбінацію клавіш можна з мережі знаючи виробника ноутбуку або материнської плати ПК.

Так, Linux завантажується без єдиної підозри зі сторони BIOS, тому має доступ до наявних дисків, в тому числі й системного. Досить просто вмонтувати

диск до обраної Live CD системи та безперешкодно копіювати данні з дисків, та в окремому випадку з під root, редагувати їх.

Роблячи підсумки, слід зазначити, що для захисту приватності інформації достатньо встановити пароль до BIOS, не використовувати емуляцію Legacy на Uefi Bios, завжди тримати увімкненим Secure Boot та зашифрувати данні за допомогою BitLocker.

Ці дії не уявляють складнощів та не заважають комфортному використанню пристроїв власником. Захистити данні від монтування або звичайного підключення до іншого комп'ютера диску можна завдяки пропрієтарній Windows програмі BitLocker, що зашифрує наявну інформацію на диску.

Список використаних джерел:

1. Яка різниця між UEFI и Legacy BIOS? /gravitsapa.info: веб-сайт. URL: https://gravitsapa.info/kakie-otlichiya-mezhdu-uefi-i-legacy-biosami/ (дата звернення 12.11.2021)

УДК 339.92

БАРАНЕНКО ЄГОР ОЛЕКСАНДРОВИЧ

курсант 2 курсу факультету №4

Харківського національного університету внутрішніх справ

ОНИЩЕНКО ЮРІЙ МИКОЛАЙОВИЧ

кандидат наук з державного управління, доцент,

заст. декана факультету з навчально-методичної роботи факультету №4

Харківського національного університету внутрішніх справ

БЛОКЧЕЙН, ЯК ВАРІАНТ ЗАХИСТУ ДАНИХ

З кожним днем роль кіберпростору в нашому житті невпинно збільшується. Щороку об'єм інформації в інтернеті зростає в рази, а з ним зростає кількість конфіденційної інформації, яку необхідно захищати.