

*Секція 1. СУЧАСНІ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ
ТЕХНОЛОГІЇ В ЖИТТІ ЛЮДИНИ ТА СУСПІЛЬСТВА*

**АНАЛІЗ АКТИВНОСТІ КОРИСТУВАЧА ЗА ПРОФІЛЕМ
ОПЕРАЦІЙНОЇ СИСТЕМИ iOS**

Апанасенко А.С.

*студент 4-го курсу факультету кібербезпеки та інформаційних технологій
Національного університету «Одеська юридична академія»*

У наш час інформаційні технології все міцніше входять у повсякденне життя, і комп'ютер став уже звичною її частиною. Для більшості людей, що мали досвід спілкування з комп'ютером, слова «іконка», «вікно», «робочий стіл», «меню Пуск» стали звичними й зрозумілими, а логотип чотириколірного прапорця, що розвивається, не викликає подиву.

У звичних нам мобільних комп'ютерних пристроях також є операційна система, яка допомагає нам більш зручніше й оперативніше управляти нашим мобільним пристроєм. Питання, пов'язані з кишеньковими комп'ютерами, смартфонами й комунікаторами, сьогодні стають актуальними, особливо у зв'язку з активним розвитком цього сегмента ринку й стрімким зростанням популярності різноманітних портативних пристроїв.

Будь-яка операційна система оперує деякими сутностями, які разом зі способами управління ними багато в чому характеризують її властивості. До таких сутностей можуть ставитися поняття процесу, об'єкта, файлу та ін. Кожна ОС має свій набір таких сутностей, і вже через управління цією сутністю надаються всі можливі функції. Однією з найпопулярнішою операційною системою в світі є iOS – мобільна операційна система для смартфонів, електронних планшетів, програвачів і деяких інших пристроїв, що розробляються і випускаються американською компанією Apple [1].

Мобільні операційні системи, такі як iOS, відрізняються від більшості інших операційних систем, оскільки вони поставляють кожен додаток у власну захисну оболонку, що заважає іншим застосункам порушувати їх. Це робить неможливим зараження вірусом застосунків у мобільній операційній системі, хоча існують і інші форми шкідливого програмного забезпечення. Захисна оболонка навколо застосунків також становить обмеження, оскільки вона не дозволяє безпосередньо спілкуватися між собою програмами. iOS оминула це, використовуючи розширюваність – функцію, яка дозволяє застосунку схвалювати для зв'язку з іншим застосунком.

Експерти стверджують, що мобільна платформа iOS набагато захищена операційна система перед більшістю видів існуючих атак. Пов'язано це в чималому ступені із суворим цензуруванням App Store.

В будь-якій роботі на першому місці завжди стоїть безпека, пише сайт Anonymus. Під безпекою мається на увазі захист від шкоди і інших небажаних наслідків. Всім потрібна безпека. Навіть смартфонам. Експертами з безпеки в мережі рCloud було проведено дослідження в ході якого було здійснено аналіз даних конфіденційності. З'ясувалося, які програми можуть передавати стороннім сервісам інформацію про користувача.

Є міф про те, що iOS забезпечує повну захищеність інформації, але це не зовсім так. Компанія Apple велику увагу приділяє захисту смартфона від шкідливих програм. Тому, не пропускає їх в App Store. Але, навіть не зважаючи на це найпростішим способом отримати особисті дані користувача є соціальна інженерія. Особливо добре вона спрацьовує на айфон, якщо користувач нехтує простими правилами [2]. Частою причиною є неухважність самого користувача. Але, існує й інша загроза крадіжки особистих даних, а саме з боку уряду, спецслужб і хакерів. Так, наприклад, останні можуть продавати інформацію внаслідок чого спецслужби можуть отримувати дані зі смартфона користувача. І навіть якщо це звучить досить нереально, насправді все так і відбувається навіть на iOS.

Слід брати до уваги, що не зважаючи, на заявлену безпеку системи iOS, існує загроза використання зібраних даних сторонніми особами. Починаючи, задля таргетованої реклами, закінчуючи кібершахраями. На наш погляд, доцільно використовувати Моніторинг активності користувачів – User Activity Monitoring (UAM). UAM фіксує дії користувача, у тому числі використання програм, відкриття вікон, виконання системних команд, натискання прапорців, введення/редагування тексту, відвідані URL-адреси та майже всі інші події на екрані для захисту даних, гарантуючи, що співробітники та підрядники залишаються в межах призначених їм завдань і не становить ризику для організації.

Програмне забезпечення для моніторингу активності користувачів може відтворювати дії користувача як відео та обробляти відео в журналах активності користувачів, які ведуть покрокові записи дій користувача, які можна шукати та аналізувати для розслідування будь-яких невідповідностей.

Список використаних джерел:

1. Compare iPhone models/ iPhone - Apple Official Site [https URL: //www.apple.com/](https://www.apple.com/)
2. Apple Introduces New iPod touch. Apple Press Release URL: <https://www.apple.com/newsroom/2010/09/01Apple-Introduces-New-iPod-touch/>

Науковий керівник: Виходець О.О.