# Модуль: Безпека мобільних пристроїв



### Практична вправа:

«Налаштування захисних механізмів у мобільному пристрої»



**Навчальна мета заняття:** відповідно до конкретних умов навчитися налаштовувати параметри мобільного пристрою та встановлених на ньому програм для безпечного використання.



Час проведення: 1 год. Міси

Місце проведення: комп'ютерний клас.



### Устаткування:

персональний комп'ютер (ПК) зі встановленою операційною системою Windows 7 або вище та доступом до мережі Інтернет, програма виведення зображення з мобільного пристрою на екран монітора персонального комп'ютера, Telegram, Viber, WhatsApp.

# Порядок проведення заняття

Налаштування безпеки мобільного пристрою слід організовувати за двома головними напрямами:

- 1) налаштування операційної системи мобільного пристрою;
- 2) налаштування прикладних програм.

Що стосується першого напряму, то, передусім, для безпечного користування смартфоном слід встановити надійний механізм його розблокування. Для цього потрібно зайти у налаштування системи та встановити пароль, який буде достатньо довгим та складатиметься з літер, цифр та спеціальних символів (рис. 1).

Проведення Немає безпеки	
Ключ розблокування Середній рівень безпеки	
РІN-код Помірно-високий рівень безпеки	
Пароль Високий рівень безпеки, Поточний тип блокування	
Немає	
Біометричні дані	

Рис. 1. Налаштування паролю для розблокування пристрою

Для виконання розглянутого завдання на iPhone: «Налаштування» > «Touch ID i > код-пароль» > «Запит паролю: одразу» > «Змінити пароль» > «Довільний код (літери + цифри).



У випадку, якщо дозволяють функції пристрою, можна також налаштувати біометричну ідентифікацію.

Крім наведеного, слід переглянути інші налаштування безпеки та встановити їх таким чином, щоб вони відповідали потрібному рівню захисту (рис. 2).



Рис. 2. Налаштування параметрів безпеки та конфіденційності

Після проведення загальних налаштувань операційної системи слід убезпечити себе від витоку інформації із заблокованого пристрою. Для цього, перш за все, потрібно вимкнути повідомлення на заблокованому екрані (рис. 3). Також відповідні налаштування можуть бути встановлені окремо для кожного застосунку («Налаштування» > «Програми»). Виконання описаних дій дозволить стороннім особам бачити приватні повідомлення.



Для виконання розглянутого завдання на iPhone: «Налаштування» > «Пароль» > «Доступ з блокуванням екрану»; «Налаштування» > «Сповіщення» > «Показ мініатюр» > «Без блокування».



Рис. 3. Вимкнення повідомлень

Слід пам'ятати, що окремі налаштування стосуються не тільки самого мобільного пристрою, а й облікового запису. Враховуючи це, потрібно переглянути налаштування безпеки облікового запису та встановити відповідні параметри.

Одним з прикладів такого налаштування є встановлення двофакторної автентифікації (рис. 4).

Вхід в обліковий запис Google		
Пароль	Остання зміна: 29 квіт. 2020 р.	>
Двохетапна перевірка	● Вимк.	>
Способи підтвердження вашої особи Це допоможе підтвердити вашу особу під час входу або зи з вами, якщо ми виявимо підозрілу активність в обліково	з'язатися му записі	
Номер телефону для відновлення	Додайте номер мобільного телефону	>
Резервна електронна адреса	Додайте електронну адресу	>

Рис. 3. Налаштування безпеки облікового запису



Для виконання розглянутого завдання на iPhone: «Сайт Apple ID» > «Двофакторна ідентифікація» > «Увімкнути»; «Безпека» > «Перевірені номери телефонів» > «Змінити» > «Додати номер телефону з можливістю приймання текстових повідомлень».

Для заборони відслідковування своїх дій після авторизації в обліковому записі можна встановити спеціальне розширення (https://tools.google.com/ dlpage/gaoptout?hl=ru).

Залежно від конкретних умов слід правильно налаштувати синхронізацію даних. Якщо ви не бажаєте зберігати відомості на віддаленому ресурсі, потрібно вимкнути автоматичну синхронізацію даних у налаштуваннях відповідного облікового запису в мобільному пристрої (рис. 4).

Goog	@gmail.com e
Контакти	
Натисніть, щоб	виконати синхронізувати
зараз Эстання синхро 17:50	нізація: 7 червня 2019 р.,
Google Play	Фільми
Натисніть, щоб і Вараз	виконати синхронізувати
Синхронізацію в	зимкнено
Google Play	Музика
атисніть, щоб	виконати синхронізувати (5
anaa	M/



Для виконання розглянутого завдання на iPhone: «Налаштування» > «Apple ID, iCloud, медіаматеріали» > «iCloud» > «iCloud Drive» > «Фото». Крім наведеного, слід також вимкнути автоматичне підключення до Wi-Fi мереж (рис. 5). Якщо у вас налаштоване автопідключення до відомих точок доступу Wi-Fi, ви так само автоматично можете бути під'єднаними до підробленої точки доступу. У подальшому весь трафік Інтернет може

бути пропущений через обладнання зловмисника. Це дозволяє порушнику примусово перенаправляти запити з вашого пристрою на свої ресурси. При цьому ви можете навіть нічого не помітити.

< Підключення	Q	< Wi-Fi	Wi-Fi Direct	< Додатково	
Wi-Fi		Увімкнено	Додатково Зв'яжіться з нами	Виявлення підозрілих мереж Останчім часом підозрілих мереж не	К
Bluetootn Підключення до наявних поблизу пристроїв Bluetooth.		Поточна мережа	•	виявлено Показ інформації про якість	4
NFC та оплата Здійснюйте мобільні платежі, надсилайте дані, а також зчитуйте або записуйте теги NFC.	$\bigcirc$	Доступні мережі	-	Режим енергозбереження Wi-Fi Заощаджуйте заряд батарей, аналізуючи	Швидкість мережі 144 Мбіт/с
Режим без зв'язку Вимкнення функцій виклику, обміну повідомленнями, а також мобільних даних.		<u></u>		характер трафиу WiFi. Установки мережі Керування мережами	Безпека wpa2 psk
Мобільні мережі		ିଲ୍ e		Керування збереженими мережами Wi-Fi. Журнал керування Wi-Fi Перегляд останніх програм, що вмикали або вимикали Wi-Fi.	192 Керування маршрутизатором ?
Диспетчер SIM-картки	40.7014	TP	-	? Нотврот 2.0 Автоматичне підключення до мереж WIFFI, що підтримують технологію Нотврот 2.0.	Підключатися автоматично

Рис. 5. Налаштування Wi-Fi



Для виконання розглянутого завдання на iPhone: «Налаштування» > «Wi-Fi» > Обрати відповідну мережу > «Автопідключення» > «Вимкнути».

Що стосується налаштувань окремих застосунків, то тут слід передусім звернути увагу на обмеження їх доступу до чутливих даних: файлів на телефоні, контактів, геолокації тощо (рис. 6).

← д	цозволи додат ९   ?	← Дозволи додат ♀ ⑦ : ← Дозволи додат ♀	9 i
	LinkedIn	Meest Vysor	
	дозволено	дозволено дозволено	
	Немає наданих дозволів	🖸 Камера Немає наданих дозволі	в
	відмовлено	відмовлено відмовлено	
0	Геодані	Геодані           Геодані         Геодані	
	Календар	👗 Контакти 🌷 Мікрофон	
	Камера	Пам'ять	
*	Контакти		
Ļ	Мікрофон		



Для виконання розглянутого завдання на iPhone: «Налаштування» > «Конфіденційність» > «Геолокація», «Відслідковування» > поставити «Вимкнути» у налаштуваннях відповідних застосунків. У використовуваних браузерах також слід налаштувати відповідну безпеку. Наприклад, у Google Chrome це можна зробити як на рис. 7.

û	→ ☆ ≛ (i) C	← Налаштування 🛛	← Паролі ♀ ♀ ;	🔶 Конфіденційність 🛛 🛛		
	Нова вкладка	Вибрати інший обліковий запис	Зберігання паролів Увімкнено	Отримати доступ до способів ?		
	пова анонімна вкладка	Синхронізація та сервіси Google	Автоматичний вхід ?	є збережені способи оплати		
	Історія	Основні	Автоматично входити в облікові записи на веб-сайтах за допомогою збережених даних. Якщо цю функцію	Попередньо завантажувати ?		
Введіть г	Завантаження	Пошукова система	вимкнено, потрібно вводити облікові дані під час кожного входу.	переглядати та шукати Використовує файли cookie, щоб		
	Закладки	Google Перевірити паролі		зберігати налаштування, навіть якщо ви не відвідуєте ці сторінки		
YouTube	Останні вкладки	Паролі	Захистіть свої паролі від порушень безпеки даних та інших проблем із безпекою	"Не відстежувати" Вимк.		
R	Версія для комп'ютера 🛛	Способи оплати	Ніколи не зберігалося	Duran Contraction DNIO		
RST.ua	Налаштування Адреси й інше			використовувати оезпечну систему DNS Автоматично		
Статті для в	Довідка й відгуки	Конфіденційність	-	Очистити історію Очистити історію, файли cookie, дані сайтів, кеш…		

Рис. 7. Налаштування безпеки браузера

Важливоючастиноюзахистумобільногопристроюєправильненалаштування програм для спілкування (месенджерів). Найбільш поширеними такими рішеннями на теперішній час є Telegram (рис. 8), Viber (рис. 9), WhatsApp (рис. 10).

+		۹	:	🔶 Приватність і безпека
Ļ	Сповіщення та звуки			Приватність
ŀ	Приватність і безпека			Заблоковані користувачі 6
$\bigcirc$	Дані та сховище			Номер телефону Ніхто
$\mathcal{O}$	Налаштування чатів			Відвідини та стан у мережі Мої контакти
	Папки			Фото профілю Мої контакти
	Пристрої			Пересилання повідомлень Ніхто
<u> </u>				Виклики Усі
V				Групи Мої контакти
Допо	мога			Змінити, хто може додавати вас до груп і
$\underbrace{\cdots}$	Поставити запитання			каналів.
?	ЧаПи Telegram			Безпека
$\bigcirc$	Політика приватності			Код блокування
Tele	aram для Android v7.4.2 (2227) а	arm64-v8	а	Двоетапна перевірка Увімкнено

Рис. 8. Налаштування безпеки месенджера Telegram



# Рис. 9. Налаштування безпеки месенджера Viber

÷	Налаштування	🔶 Конфіденційність	🔶 Двоетапна перевірка	÷	Резервна копія бесід
9 6	1 Неу there! I am using WhatsA	Хто може бачити мою особисту інформацію Якщо ви приховуєте, коли востанне були в мережі, ви не можете бачити час відвідування інших контактів Востаннє в мережі Ніхто Фото профілю Ніхто	ж * * Для додаткового захисту ввімкніть двоеталну перевірку. Під час повторної ресстрації номера у WhatAon биле залитано PIN-кол	٥	Станне резервне копіовання Створюйте резервні копії повідомлень і видновити і після перестановлення видновити і після перестановлення також буде збережено у внутрішній пом'яті телефона.
٠	Сповіщення Звуки повідомлень, груп і дзвінків	Звістка Ніхто		4	Налаштування Google Диска
0	Пам'ять і дані Використання мережі, автозавантаження	Статус Мої контакти			Резервну копію повідомлень і медіафайлів на Google Диску не захищено наскрізним шифруванням WhatsApp.
0	<b>Довідка</b> Довідковий центр, служба підтримки, Політика конфіденційності	Звіти про прочитання Вимкнувши цю опцію, ви не зможете надсилати та отримувати звіти про прочитання. Звіти про прочитання завжди надсилаються для групових			Резервне копіювання на Google Ніколи Обліковий запис Google
		оесід.			Не вибрано
	Запросити друга	<b>Групи</b> Усі	увімкнути		Резервне копіювання через Тільки Wi-Fi

Рис. 10. Налаштування безпеки месенджера WhatsApp

Щодо налаштувань резервного копіювання даних у різних застосунках, тут рішення користувач має прийняти самостійно з урахуванням існуючих ризиків.

#### Завдання

1. Налаштуйте параметри безпеки для:

- операційної системи свого мобільного пристрою;
- облікових записів, прив'язаних до мобільного пристрою;
- встановлених на мобільному пристрої застосунків.