

УДК 621.34

**РАЧИНСЬКИЙ ОЛЕКСІЙ ОЛЕКСАНДРОВИЧ**

*курсант 2 курсу факультету №1*

*Харківського національного університету внутрішніх справ*

**ЄВТУШОК ВОЛОДИМИР АНАТОЛІЙОВИЧ**

*старший викладач кафедри тактичної та спеціальної підготовки факультету*

*№ 2 Харківського національного університету внутрішніх справ*

**ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ВИКОРИСТАННЯ 5G  
У ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ**

Fifth generation (далі – 5G) – це п'яте покоління мобільної мережі, що в порівнянні з попереднім стандартом - 4G (LTE), дає змогу передавати дані зі значно більшою швидкістю, істотно знижує затримки та реалізує розрізання мережі на окремі простори для віртуалізації єдиної системи, за допомогою широкого спектру нових технічних функцій, яка дасть змогу створити повноцінну екосистему між пристроями.

Ефективність анти кримінальної та охоронної діяльності залежить від ступеня та якості інтеграції інноваційних технологій у роботу правоохоронних органів. 5G є засобом забезпечення найшвидшого зв'язку з майже відсутніми затримками, тому його ефективність застосування у критичних сферах, де необхідна якомога швидка передача даних: організація безпеки дорожнього руху, можливість створення стрімінгових платформ, які у режимі реального часу будуть вести трансляції з нагрудних камер поліцейських тощо. Також однією з головних переваг 5G є Internet of Things (далі – IoT). За допомогою технології розшарування мережі, IoT під'єднає пристрої до інтернету та надасть їм нові функції, після чого взаємопов'язані прилади виключать необхідність участі людини, за рахунок використання відповідного програмного забезпечення та обладнання. Наприклад, оснащення службових автомобілів автокеруванням, у випадках критичних ситуацій, де необхідно направити транспортний засіб з точки А у точку Б, без участі водія; проведення огляду

місця події спеціалістами-вибухотехніками НПУ, за відсутність можливості безпосереднього та фізичного контакту.

Незважаючи на всі позитивні аспекти переходу до 5G є ряд проблемних питань, які пов'язані з використанням систем законного перехоплення телекомунікацій (далі – СПТ) :

1. Неможливість опрацювання збільшеного об'єму даних. Як ми вже зазначили – мережі 5G передають дані зі швидкістю значно переважаючу минулий протокол зв'язку (швидкість LTE – 100 Мб/с, а вдосконалого LTE-Advanced - 1Гб/с, на відміну від 10-20 Гб/с, що надає 5G). Це майже унеможливорює проведення оперативно-розшукових заходів та негласних слідчих (розшукових) дій у телекомунікаційних мережах загального користування за допомогою стандартних методів СПТ, через технічну нездатність мережного комплексу і засобів управління системою перехоплення телекомунікацій (далі – ЗУСП) (сервери, станції, термінали та інші) опрацювати різко збільшений потік даних (збір, обробка, аналіз, зберігання тощо).

2. Хендовер. Це процес передачі сесії зв'язку, що відбувається при переході користувача з однієї зони покриття в іншу. Явище виникає внаслідок неможливості повністю покрити країну однією інфраструктурою – покриттям 5G. Через це системи СПТ повинні опрацьовувати постійну фіксацію та контроль даних під час зміни мереж, які працюють на різних технологіях радіодоступу, що потребує технічного вдосконалення програмного забезпечення ЗУСП та СПТ в цілому.

3. Розгортання головної магістралі 5G Core. Мережа 5G Core дає змогу суміщати одночасну роботу 4G та 5G та має абсолютно нову архітектуру та механізми роботи. Головним нововведенням є підтримка криптографії протоколу захисту транспортного рівня (далі – TLS), яке дає можливість здійснювати зв'язок користувачам мережі, унеможливаючи проведення дешифрування пакетів зв'язку та отримання доступу за допомогою СПТ, що є головною проблемою розгортання 5G.

Отже, з урахуванням вище викладеного матеріала ми можемо зробити такий висновок: мережа 5G має ряд інноваційних переваг над попереднім стандартом 4G(LTE), але через технічну недосконалість СПТ розгортання 5G ставить під загрозу проведення оперативно-розшукових заходів та негласних слідчих (розшукових) дій у телекомунікаційних мережах, що в свою чергу може призвести до погіршення криміногенного положення у країні та здійснення охоронних функцій правоохоронними органами.

УДК 004.056:351.741

### **РУДИЙ ТАРАС ВОЛОДИМИРОВИЧ**

*кандидат технічних наук, доцент,*

*доцент кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів*

*Львівського державного університету внутрішніх справ*

### **ЗАЧЕК ОЛЕГ ІГОРОВИЧ**

*кандидат технічних наук, доцент,*

*доцент кафедри інформаційного та аналітичного забезпечення діяльності правоохоронних органів*

*Львівського державного університету внутрішніх справ*

### **ЗАХАРОВА ОЛЕКСАНДРА ВАСИЛІВНА**

*кандидат юридичних наук, доцент,*

*доцент кафедри кримінального процесу та криміналістики*

*Львівського державного університету внутрішніх справ*

## **ДЕЯКІ АСПЕКТИ ОРГАНІЗАЦІЙНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ДЕРЖАВИ**

Важливим завданням для України в найближчій перспективі є розроблення та негайне реалізування прийнятних організаційно-правових заходів у практиці протидії кіберзлочинності, наповнення уже прийнятих рамкових законів реальним змістом. До того ж, встановлені завдання суб'єктів