прикордонної служби України. Серія : Юридичні науки. 2018. Вип. 2. URL: http://nbuv.gov.ua/UJRN/vnadpcurn_2018_2_6.

УДК 621.34
ОЛЕКСАНДР СЕРГІЙОВИЧ ТКАЧЕНКО
студент 3 курсу факультету №6 Харківського національного університету внутрішніх справ
ВОЛОДИМИР ВОЛОДИМИРОВИЧ ТУЛУПОВ
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій факультету № 4 Харківського національного університету внутрішніх справ

ПИТАННЯ БЕЗПЕКИ ПРИ ВИКОРИСТАННІ СУЧАСНОГО СТАНДАРТУ LTE

У розвинених країнах світу продовжується перехід до інформаційної сервісно-технологічної економіки. На теперішній час в Україні використовується стандарт зв'язку четвертого покоління LTE (Long Term Evolution), який вважається перспективним. За даними компанії HUAWEI, LTE забезпечує швидкість до 326,4 Мбіт/с від базової станції до користувача і до 172,8 Мбіт/с у зворотному напрямку.

Метою створення стандарту LTE є збільшення можливостей високошвидкісних систем мобільного зв'язку, зменшення вартості передачі даних, можливість надання широкого спектру недорогих послуг.

Мобільний зв'язок четвертого покоління передбачає використання цілого спектру технологій, які раніше розвивалися паралельно. Всі вони внесли свій внесок у специфікацію LTE реалізованої в двох основних варіантах технологій: з дуплексним частотним поділом LTE-FDD (Frequency Division Duplex) і часовим поділом LTE-TDD (Time Division Duplex).

З точки зору безпеки таких LTE мереж враховуючи різні технології ускладнює пошук її вразливостей. В мережах 4G весь трафік проходить через єдину архітектуру EPC (Evolved Packet Core) за протоколом IP.

З фізичної точки зору в мережах LTE використовуються великі смуги частот, високорівнева модуляція сигналу, технологія MIMO (Multiple Input Multiple Output) яка дозволяє збільшити смугу пропускання каналу, при якому для передачі даних використовуються дві і більше антени і така ж кількість антен для прийому. Разом вони забезпечують адекватну завадостійкість, високі швидкості передачі даних і ємність мережі. Важливою особливістю мережі 4G є те, що з її архітектури зникло поняття контролера радіомережі (RNC), який в 3G виконував основну функцію з управління комунікаційними ресурсами. Тому базові станції в LTE стали більш інтелектуальними і самостійними – вони отримали можливість маршрутизувати трафік, що дозволило організовувати з'єднання між абонентами безпосередньо, минаючи ядро мережі. Щоб звести до мінімуму атаки на конфіденційну інформацію, базова станція повинна забезпечити

виконання таких важливих операцій, як кодування та розшифрування користувачів даних, а також зберігання ключів.

Стандарт LTE виділяє п'ять основних груп безпеки це, насамперед:

– архітектура безпеки мережі повинна забезпечити користувачів надійним доступом до сервісів і захист від атак на інтерфейси;

– мережевий рівень повинен дозволяти вузлам мережі безпечно обмінюватися як даними користувачів, так і керуючими даними і забезпечувати захист від атак на провідні лінії;

– користувальницький рівень повинен забезпечувати безпечний доступ до мобільного пристрою; рівень додатків повинен гарантувати безпечний обмін повідомленнями;

– видимість і можливість зміни налаштувань безпеки повинна дозволяти користувачеві дізнаватися, чи забезпечується безпека і включати різні режими для її забезпечення.

Є також проблеми і з самим стандартом. По-перше, дуже гостро стоїть завдання взаємодії з не LTE мережами. Якщо трафік між користувальницьким обладнанням і базовою станцією шифрується (це вимога стандарту) і загроза порушення конфіденційності стає неактуальною, то взаємодія базової станції з радіоконтролером мережі 3G по умовчанню ніяк не захищене а, отже, це пролом для можливих атак з боку зловмисників. По-друге, відсутність обов'язкової аутентифікації між ядром мережі і базовою станцією. Цю опцію оператор зв'язку для зниження своїх витрат щодо розгортання мережі LTE може і не задіяти зовсім. Не можна забувати і про обмеження LTE. Наприклад, збільшення швидкості підключення зазвичай обертається зменшенням радіусу дії базової станції, який в середньому для 4G становить близько 5 км і залежить від використовуваного частотного діапазону . Тому базових станцій в мережі стає більше, і вони розташовуються ближче одна до одної.

Ще одна особливість LTE в тому, що ця технологія орієнтована на підключення інтелектуальних пристроїв, з поширенням яких число потенційно небезпечних сервісів буде тільки зростати, що дозволить зловмисникам отримати доступ до конфіденційної інформації провайдера і побудувати нові витончені схеми інформаційних злочинів.

Всі функції захисту в LTE об'єднані стандартом і передбачають захист на декількох рівнях: на рівні доступу до мережі, на рівнях мережевого і користувальницького доменів, на рівні додатків та на рівні відображення і конфігурацій.

Кожен з цих рівнів передбачає аутентифікацію і авторизацію всіх пристроїв, чого немає в Інтернеті. Технологія LTE передбачає використання не тільки IP-адреси, але і системи розповсюдження ключів шифрування для всіх пристроїв, підключених до мережі з можливістю переходу зі 128 до 256-бітові ключі і введення нових алгоритмів, зберігаючи зворотну сумісність. Крім алгоритмів шифрування і забезпечення комплексної безпеки в мережах 4G використовуються додаткові алгоритми, які навіть за умови того, що один з них буде зламаний, решта забезпечать безпеку мережі LTE. Крім того, в

LTE зберігаються і методи аутентифікації користувачів по прив'язці до SIM карти, як в традиційному мобільному зв'язку. Користувач може заблокувати доступ до телефону з PIN-кодом.

Таким чином, виходячи з вище сказаного, головною особливістю з точки зору захисту абонента розглянутого стандарту четвертого покоління рухомого зв'язку LTE, процес обслуговування приховується тимчасовими ідентифікаторами.

УДК 378.091
МАРИНА ОЛЕГІВНА БУЧКО
АНАСТАСІЯ ОЛЕКСІЇВНА ЗАБЛОЦЬКА
здобувачі вищої освіти ІІ курсу факультету економіко-правової безпеки
Дніпропетровський державний університет внутрішніх справ
ОЛЬГА ГЕННАДІЇВНА КОСТЕНКО
старший викладач кафедри українознавства та іноземних мов
Дніпропетровський державний університет внутрішніх справ

ПЕРСПЕКТИВИ ЗАПРОВАДЖЕННЯ МЕДІА В ОСВІТНІЙ ПРОЦЕС

В нашому житті великий вплив на різні сфери життя людини мають інноваційні технології, які зростають з кожним днем. Від людини вимагається не лише знання сучасних технічних пристроїв та уміння з ними працювати, а й певний рівень критичного мислення (здатності інтерпретувати інформацію, яку було отримано із різноманітних засобів масової інформації, розуміння різноманітних медіа текстів тощо), навичок самостійної роботи, пов'язаної з обробкою та пошуком, презентацією інформаційного матеріалу тощо.

Сучасні учні, студенти (курсанти) є активними споживачами інформації різноманітних медіа. Уже в середині ХХ сторіччя у зарубіжних країнах світу в педагогічній науці був сформований спеціальний напрям під назвою – медіа освіта, покликаний допомогти їм, краще адаптуватися в умовах медіа культури. Цілі та задачі медіа освіти зарубіжних вчених трактуються по-різному, але в педагогічному аспекті даний напрям вивчає взаємодію медіа з процесами виховання та навчання. Тому за мету для нашої праці є саме дослідження інтеграції медіа в навчальний процес.

Розвиток засобів масової інформації комунікації і залучення їх до навчально-виховного процесу, значно активізували творчі уроки педагогів у багатьох країнах світу. Існуючий процес комп'ютеризації та інформатизації сучасного суспільства визначив напрями вітчизняних і зарубіжних досліджень, які аналізують різні аспекти проблеми інтеграції сучасних медіа в освітній процес. В. Робак зазначає, що у Німеччині було відкрито багато науководослідних інституту які проводять дослідження цієї галузі. Видатний німецький вчений Б. Щерб став першим професором медіа педагогіки. Він вважає,що медіа педагогіка, застосовується у позаурочній роботі і саме там має найкращі перспективи.