ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ, УПРАВЛІННЯ ПРОЕКТАМИ І ПРОГРАМАМИ

УДК 004.453.4

В.В. Самотий*, д-р техн. наук, професор*
(Львівський державний університет безпеки життєдіяльності)
У.Ю. Дзелендзяк*, канд. техн. наук, доцент*
(Національний університет «Львівська політехніка»)

ПРОБЛЕМИ БЕЗПЕКИ ТА КОНФІДЕНЦІЙНОСТІ ТЕХНОЛОГІЙ ДОПОВНЕНОЇ РЕАЛЬНОСТІ

Проведено аналіз проблем безпеки та конфіденційності, пов'язаних із додатками та системами доповненої реальності, а також із технологіями, які їх підтримують. Ці проблеми були проаналізовані за двома категоріями: обсяг системи та функціональність. У першій категорії розглянуто системи доповненої реальності (AR-системи) зростаючого масштабу: окремі додатки, кілька додатків на одній AR-платформі та кілька взаємодіючих AR-систем. Для цієї категорії проаналізовано проблеми, пов'язані з входом, виходом та доступом до даних. Виходячи з вище наведених проблем захисту інформації в AR-технологіях, вказані основні напрямки їх вирішення.

Ключові слова: доповнена реальність, віртуальна реальність, AR-додаток, AR-система, контент, відеопотік, шкідливі програми, конфіденційність, безпека, атаки.

V. Samotyy, U. Dzelendzyak

THE SECURITY AND PRIVACY PROBLEMS OF AUGMENTED REALITY TECHNOLOGIES

The analysis of security and confidential problems, connected with augmented reality systems and support technologies have been conducted. These problems have been analyzed using 2 categories: system volume and functionality. In the first category the augmented reality systems (AR-systems) of growing scale: single applications, multiple applications within a single AR platform, and multiple communicating AR-systems have been reviewed. For this category the problems connected with input, output and data access have been analyzed. Based on the described problems of information security in AR-technologies, the main directions of their solutions have been indicated.

Key words: augmented reality, virtual reality, AR application, AR system, content, video stream, malicious application, privacy, security, attacks.

Вступ. Технології доповненої реальності (AR) обіцяють покращити наше сприйняття і взаємодію з реальним світом. На відміну від систем віртуальної реальності, які замінюють реальний світ імітованим, системи доповненої реальності, відчувають властивості фізичного світу та накладають згенеровані комп'ютером візуальні, звукові і тактильні сигнали на реальні зворотні зв'язки в режимі реального часу. Контентом для накладення можуть бути навігаційні дані для водія автомобіля, схеми для ремонту електронних приладів і навіть дистанційне проектування рук хірурга під час складної операції. Щодо майбутнього доповненої реальності прогнози експертів різняться. Співзасновниця Geoloqi Ембер Кейс стверджує, що доповнена реальність перейде на новий рівень тільки тоді, коли користувачі зможуть самі створювати різні об’єкти, анімацію та програми [1]. Технологія доповненої реальності найближчим часом повинна стати доступною не тільки для розробників, але і для звичайних користувачів. Це означає, що цей контент буде дуже швидко поширюватися по мережі. Але, як і будь-яка інша технологія, доповнена реальність поряд з новими можливостями несе в собі і нові ризики з точки зору безпеки та конфіденційності [1].

Аналіз досліджень та публікацій

Найбільш поширеними ризиками з точки зору безпеки та конфіденційності при розробленні та використанні мобільних додатків з доповненою реальністю є фішинг (сукупність прийомів, призначених для отримання доступу до такої секретної інформації, як логіни і паролі) та використання різноманітних шкідливих додатків [2]. У додатках AR можливості для шкідливих програм є практично безмежними. Це і кейлогери для захоплення облікових даних користувача, і мобільні троянські програми віддаленого доступу (mobile remote access Virus – mRAT), які можуть заразити пристрій та таємно перехоплювати дані та комунікації, або агент, який через мобільний пристрій завантажує шкідливе програмне забезпечення в мережу [1].

Швидке зростання ринку доповненої реальності робить проблему усунення ризиків ще більш актуальною. На теперішній час розроблено багато корисних і доступних користувачеві додатків AR, таких як браузер доповненої рельності Wikitude (пошук інформації, прив'язаної до місцевості), Zappar (відображення на екрані зображень, фотографій, музики і відео, які пов'язані з обраним об'єктом), Layar, Spectrek, Junaio, Historypin, LocalScope та інші. Ще однією новинкою у сфері доповненої реальності є контактні лінзи iOptik, що показують своєму власникові доповнену реальність і відео високої чіткості, які прийдуть на зміну телебаченню і мобільній електроніці. За допомогою системи iOptik користувач може бачити цифрову інформацію, що проектується, наприклад, схему руху або відеодзвінки. Відзначимо, що система може повноцінно працювати у режимі доповненої реальності або відображати інформацію з екрана смартфона і портативного ігрового пристрою [3]. У звіті 2016 Emerging Technology Domains Risk Survey доповнена реальність названа однією з десяти технологічних областей, які в разі злому можуть привести до серйозних збоїв (у сфері безпеки, конфіденційності, фінансової або операційної) [4].

Виклад основного матеріалу. Додатки та технології доповненої реальності можуть мати будь-які або всі з нижче перелічених характеристик [5]:

- комплексний набір завжди увімкнених вхідних пристроїв і датчиків (мікрофон, камера, GPS);
- кілька вихідних пристроїв (дисплей, динамік);
- платформа, яка може запускати кілька програм одночасно;
- можливість бездротового зв'язку з іншими системами доповненої реальності.

Комплекс проблем безпеки та конфіденційності, який виникає з появою нових технологій та їх застосуванням, необхідно розглядати за двома категоріями: обсяг системи та функціональність. У першій категорії розглядаються системи доповненої реальності (AR-системи) зростаючого масштабу: окремі додатки, кілька додатків на одній AR-платформі та кілька взаємодіючих AR-систем. Для цієї категорії потрібно вирішувати проблеми, пов'язані з входом, виходом та доступом до даних. На рис. 1 показано комплекс проблем безпеки та конфіденційності, пов'язаних з технологіями доповненої реальності та їх додатками.

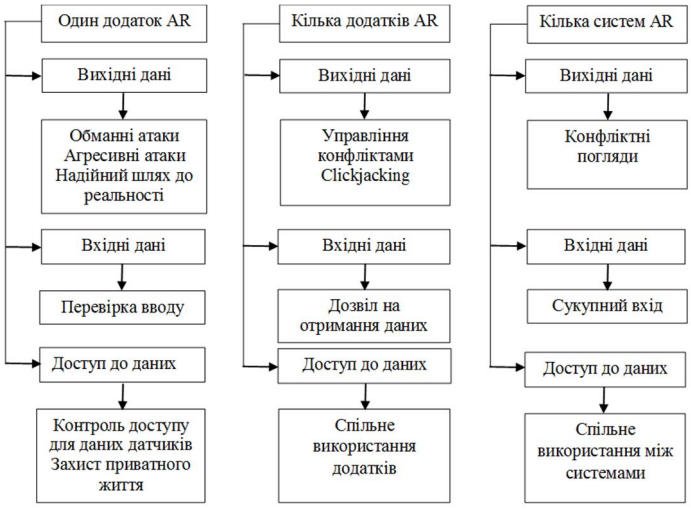

Рисунок 1 – *Проблеми безпеки та конфіденційності технологій AR*

Проблеми безпеки та конфіденційності в окремих додатках AR. Розглянемо загрози безпеці та конфіденційності в рамках одного додатка AR.

Вихідні дані. Користувачі повинні повністю довіряти програмам AR, які накладають візуальні, слухові або тактильні відчуття реального світу з віртуальними зворотними зв'язками. Пристрої, що забезпечують зворотній зв'язок із одночасним впливом на людину через декілька каналів сприйняття (зір, слух, дотик), можуть використовуватися шкідливими програмами для надання користувачам неправдивої інформації про реальний світ. Наприклад, шкідлива програма може накладати невірний файл обмеження швидкості поверх фактичного знака обмеження швидкості (або розмістити підроблений знак там, де його немає), або навмисно забезпечити неправильний переклад тексту реального світу іноземною мовою. У більш загальному сенсі, така програма може змусити користувачів хибно вважати, що певні об'єкти існують або відсутні в реальному світі. Шкідливі програми можуть використовувати подібні методики, щоб викликати сенсорне перевантаження для користувачів: надто яскраве миготіння світла на дисплеї, відтворення гучних звуків або надання інтенсивного зворотного зв'язку. Все це може завдати фізичної шкоди користувачам. Такі атаки не є безпрецедентними: зловмисники публікують повідомлення, що містять миготіння анімованих файлів gif, для запуску головних болів або судом [6]. Розробники нових платформ доповненої реальності повинні розглянути ці типи атак та запобігти їм. Ці вихідні атаки є більш серйозними у додатках AR, ніж у сучасних настільних ПК чи портативних комп'ютерах, тому що, по-перше, користувачам важче відрізняти віртуальну реальність від реальних зворотних зв'язків і, по-друге, користувачам складніше видалити чи вимкнути систему. В якості останнього засобу відхилення атак користувачі повинні мати можливість легко і надійно повернутися до реального світу, тобто вимкнути всі вихідні пристрої.

У найближчій перспективі найпростішим способом повернення до реальності є видалення AR-системи. Проте AR-системи, які, в перспективі, будуть носити користувачі (наприклад, контактні лінзи [7] або імплантовані пристрої), і сьогоднішні системи, які не носяться, доволі часто складно вимкнути. Наприклад, декілька автомобільних виробників виготовляли лобове скло, яке демонструє розширений зміст погляду користувача на дорогу [8]. У цих випадках система повинна мати надійний спосіб повернення користувача до реальності, аналогічно Ctrl-Alt-Del на комп'ютерах Windows. Визначення такого способу є однією з головних задач при розробленні кожної AR-системи. Інший підхід може полягати у резервуванні надійної області дисплея, яка завжди буде відображати реальний світ.

Вхідні дані. Додатки доповненої реальності, як і звичайні програми, зіткнуться з проблемами перевірки вхідних даних та їх «лікуванням». Наприклад, програма для перекладу, яка аналізує текст у реальному світі, може експлуатуватися зловмисним текстом. Для перевірки вхідних даних можна використовувати традиційні методи, але дизайнери AR-систем повинні враховувати специфіку додатків доповненої реальності.

Доступ до даних. Для забезпечення своєї передбачуваної функціональності, додатки AR можуть потребувати доступу до різних датчиків, включаючи відео- та аудіоканали, GPS-дані, температуру, показники акселерометра тощо. Як і в настільних комп'ютерах та операційних системах для смартфонів, важливою задачею для AR-систем буде збалансування доступу, необхідного для функціональності, із загрозою крадіжки даних або неправильного використання цього доступу. Наприклад, шкідлива програма може відправляти місцезнаходження користувача або відеопотік на свої сервери. Існуючий доказ концепції атаки PlaceRaider [9] показує, що сенсори смартфонів можуть використовуватися для збору необхідної інформації для створення тривимірних моделей внутрішніх середовищ.

На відміну від більшості сучасних додатків для ПК і смартфонів, комплексні додатки AR потребуватимуть різноманітного, постійно присутнього сприйняття. Наприклад, програма, яка автоматично визначає та сканує QR-коди, потребує постійного доступу до даних відеопотоку. У результаті, загрози для приватності тут набагато більші, ніж у звичайних системах.

AR-системи повинні використовувати підходи, які обмежують ці загрози. Наприклад, окремі програми, імовірно, не матимуть доступу до всіх даних датчиків. Можливо, програма

потребує лише доступу до частини екрана, коли користувач перебуває в певному місці, або лише потребує знання про певні об'єкти, які система розпізнає (наприклад, через розпізнавальну скриньку Kinect), а не доступу до всієї інформації з камери. Дизайнери AR-системи повинні враховувати відповідний ступінь деталізації для цих дозволів, а тому важливе значення буде мати дизайн доступних інтерфейсів для керування дозволами. Існуючі маніфестові рішення або підказки, які використовуються в смартфонах навряд чи будуть корисними, а довгострокові (а не одноразові) потреби доступу до даних додатків AR-значно ускладнюють застосування рішень контролю доступу за допомогою користувача [10].

Завжди ввімкнені камери та інші датчики також будуть створювати загрозу конфіденційності для сторонніх людей, яку Кревелен і Поелман визначають як перешкоду для широкого суспільного визнання доповненої реальності. Сторонні люди повинні мати гарантію своєї анонімності. Цього можна досягти, використовуючи камери, які миготять світлом під час запису, чим і будуть їх попереджувати [11].

Проект CVDazzle [12] використовує інший підхід, який базується на використанні макіяжу для заплутування алгоритмів розпізнавання обличчя, що забезпечує конфіденційність без відповідних камер. Ключовим обмеженням є те, що CVDazzle ретельно налаштовується вручну для одного конкретного алгоритму розпізнавання обличчя. Проблема дослідження полягає в тому, щоб знайти загальний алгоритм синтезу макіяжу, який буде обдурювати алгоритми розпізнавання обличчя.

Проблеми безпеки та конфіденційності в кількох додатках однієї AR-платформи. Незважаючи на те, що додатки AR часто проектуються як ізольовані, ми можемо сподіватися, що майбутні AR-платформи, на зразок тих, що побудовані на Google Glass або Microsoft Kinect, будуть підтримувати одночасне використання декількох додатків, сумісне використання пристроїв введення та виведення, а також надання різних даних та інтерфейсів для кожного з додатків. Розробники повинні передбачити ці фактори та забезпечити, щоб "операційна система для доповненої реальності" була створена з урахуванням міркувань щодо безпеки та конфіденційності.

Вихідні дані. У багатопрограмній AR-системі додатки поділяють вихідні пристрої, включаючи дисплеї, аудіовихід та зворотний зв'язок. Конфлікти між кількома додатками, які намагаються використовувати ці вихідні пристрої, можуть призвести до проблем безпеки. Наприклад, шкідливий додаток може намагатися затуманити вміст, представлений іншою програмою (наприклад, візуально або акуратно замінити правильний переклад неправильним).

Тим не менш, обмін продуктами буде необхідним для забезпечення бажаної функціональності в AR-системах. Наприклад, користувач може побажати одночасно переглядати вміст, накладений на реальність з кількох додатків, таких як напрямки, надані програмою для карт, соціальна мережа, що підсумовує діяльність друзів, відстежувати поточне відтворення в музичній програмі тощо. Отже, просте рішення, в якому тільки один додаток контролює дисплей в даний момент (як, наприклад, це відбувається у Android сьогодні) є недостатнім для багатопрограмної AR-системи.

Таким чином, майбутні AR-системи мають справлятися з конфліктами між кількома додатками, які намагаються виробляти вихідні дані. Наприклад, п'ять програм можуть хотіти коментувати один і той же об'єкт (наприклад, з субтитрами перекладу), і система повинна визначити їх пріоритет. Крім того, користувачам важливо знати, який вміст був сформований і в якій програмі, наприклад, чи рекомендація з анотованого продукту надходить від друга чи рекламодавця. Дизайнери AR-системи повинні створювати інтерфейси, які роблять вихідні зображення відображуваного контенту зрозумілими і легко доступними для користувачів.

Традиційні атаки, засновані на маніпулюванні виводом, можуть потребувати нових підходів або нових формулювань у контексті AR. Наприклад, в сучасних системах додатки можуть встановлювати атаки за допомогою clickjacking, які обманюють користувачів, натискаючи на чутливі елементи призначеного для користувача інтерфейсу з іншого додатка (наприклад, щоб публікувати щось в профілі соціальних мереж користувача). Ці атаки зазвичай

працюють або маніпулюючи відображенням чутливого елемента, шляхом його прозорого чи часткового затінення за допомогою розумного способу, або шляхом раптового відображення чутливих елементів безпосередньо перед тим, як користувачі натиснуть у передбачуваному місці. Майбутні додатки на AR-системах можуть розробляти нові методи для обману користувачів, які взаємодіють з елементами. Наприклад, додаток AR може намагатися змусити користувача взаємодіяти з об'єктом у фізичному, а не у віртуальному світі. Тому розробники AR-системи повинні передбачати ці загрози.

Вхідні дані. Користувачі, швидше за все, не взаємодіють із AR-системами за допомогою традиційних методів введення, таких як натискання миші або використання сенсорного екрана. Натомість користувачі можуть взаємодіяти із цими системами, використовуючи тонкий вхід для тактильних датчиків (наприклад, вбудованих у рукавички), голосові дані або за допомогою технологій відстеження погляду. Коли використовуються такі методи введення і одночасно запущено декілька програм, системі буде проблемно вирішити, яка прикладна програма є активною і повинна отримувати вхідні дані.

Наприклад, сьогоднішні голосові взаємодії відбуваються або за явними діями користувача, що вказують на призначення програми (наприклад, натискання кнопки "Siri" на iPhone4), або в системах, у яких тільки одна програма може отримувати голосовий вхід (наприклад, на Xbox). Коли декілька додатків є активними та можуть отримувати голосовий або інший вхід у будь-який момент часу, має бути спосіб, що дасть змогу користувачам вибрати потрібний додаток для вводу. Очевидно, що майбутні AR-системи, ймовірно, запускатимуть декілька додатків одночасно, багато з яких працюватимуть і слухатимуть інформацію без будь-яких видимих результатів. Неправильно розроблений доступ до конкретних додатків може полегшити шкідливим програмам викрадення вхідних даних користувача, призначених для іншої програми (наприклад, для викрадення пароля, призначеного для поля входу іншої програми).

Доступ до даних. Як і в традиційних операційних системах, додатки AR, ймовірно, захочуть надати API-інтерфейси один одному, і користувачі можуть захотіти спільно використовувати віртуальні об'єкти між додатками. Розробники повинні вивчити відповідні моделі контролю доступу для спільного використання програм. Звичайно, в цьому просторі можна використати підходи традиційного управління доступом, але для нових технологій та середовищ можуть знадобитися нові підходи. Наприклад, копіювання, вставлення та перетягування - це встановлені жести користувача для обміну даними між традиційними програмами і, звичайно, вони мають певні наслідки для контролю доступу. AR-системи повинні будуть розробляти нові жести користувача, щоб вказати на намір спільного використання додатків. Крім того, AR-системи, напевно, не будуть відображати додатки на маркованих вікнах так, як це роблять традиційні операційні системи для настільних комп'ютерів, тому потрібні нові парадигми взаємодії, щоб користувачі могли ідентифіковувати додатки та вказувати, який додаток повинен отримувати спільні дані.

Проблеми безпеки та конфіденційності в кількох AR-системах. Переходячи за межі однієї AR-системи, яка працює з кількома додатками, розглянемо взаємодію між декількома системами AR, що належать різним користувачам. Наприклад, багатокористувацькі ігри, телеприсутність для дистанційної конференції та спільна співпраця. Ці типи додатків створюють додаткові проблеми безпеки та конфіденційності.

Вихідні дані. Безліч користувачів можуть мати різні погляди на світ, представлені відповідними їхніми AR-системами. Наприклад, різні користувачі можуть бачити різні віртуальні реклами, накладені на реальні рекламні щити, або різні користувачі, які переглядають презентацію, можуть показувати різний контент на основі рівнів доступу (тобто один користувач може бачити надсекретні виноски, а інші – ні). Такі суперечливі погляди вимагатимуть від користувачів керування ментальними моделями того, хто може сприймати і яку інформацію, щоб вони ненавмисно не розкривали приватну інформацію, призначену лише для себе. Розв’язання цієї проблеми потребує інновацій у дизайні інтерфейсу для надання допомоги користувачам у цьому завданні.

Вхідні дані. Підвищення складності AR-систем і додатків буде тісно пов'язане зі збільшенням кількості та складності вхідних даних датчиків, які забезпечуються технологіями. Ця велика кількість вхідних сигналів датчиків від багатьох користувачів, у свою чергу, призведе до появи нових додатків для спільного використання, які самі можуть передавати дані назад у додатки AR. Наприклад, Google вже використовує дані, зібрані смартфонами користувачів, для оцінки умов руху, які потім повідомляються на телефони користувача. Цей тип даних необхідний, наприклад, для того, щоб майбутні додатки AR могли відображатися на вітровому склі автомобіля. Проте, такий тип спільного вводу може використовуватися зловмисними користувачами, щоб обдурити системи збору даних. Наприклад, веб-сайт огляду може використовувати відстеження місця розташування для оцінки популярності ресторану, зазначивши середню кількість людей, присутніх протягом дня. Хитрий ресторатор може потім заплатити людям, щоб вони сиділи в ресторані, нічого не замовляючи. В результаті, популярність ресторану зростає, але не має ніякого відношення до його якості.

Технології AR, які постійно збирають дані, сприятимуть впровадженню таких додатків для спільного використання, отже, ці проблеми безпеки стануть все більш важливими. Як ще один приклад, Спільнота Сейсмічної мережі об'єднує дані датчиків акселерометра від багатьох людей для виявлення та прогнозування землетрусів. Зловмисник може маніпулювати датчиками, щоб сфабрикувати незвичну сейсмічну активність. Надійні датчики [13], які є важливими для запобігання інших нападів, не допомагають у цих випадках, оскільки реальні умови є зманіпульованими.

Доступ до даних. Окрім відображення різного контенту для різних користувачів, взаємодіючі AR-системи дають змогу користувачам обмінюватися віртуальним контентом один з одним. Наприклад, один користувач може створити віртуальний документ у своїй приватній AR-системі, а потім вирішити поділитися ним із системами інших користувачів. Деякий обмін може бути навіть неявним. Уявіть собі AR-систему, яка автоматично використовує канали камери сусідніх користувачів, щоб надати даному користувачеві свою 3D-модель в реальному часі.

Неявне або явне спільне використання даних в окремих AR-системах зробить можливим використання корисних додатків. Проте, необхідні відповідні моделі та інтерфейси управління доступом, які дадуть змогу користувачам управляти цим спільним використанням. Сьогодні користувачі вже відчувають труднощі з формуванням ментальних моделей своїх налаштувань конфіденційності в таких сервісах, як Facebook, через складність взаємовідносин між людьми і елементами даних [14]. Величезна кількість даних, зібраних AR-системами, та інтеграція віртуальних об'єктів у реальний світ, зробить цю проблему ще більш складною.

Напрямки захисту. Виходячи з вище наведених проблем захисту інформації в AR-технологіях, окреслимо кілька напрямків їх вирішення. Деякі проблеми безпеки та конфіденційності, пов'язані з AR-технологіями, схожі на ті, з якими стикаються сьогодні користувачі смартфонів. Це, зокрема, конфіденційність даних датчиків та спільне використання програм. У деяких випадках відповідним захисним напрямком для доповненої реальності є адаптація рішень для смартфонів.

У довгостроковій перспективі, однак, є кілька причин, з яких підходи в контексті AR повинні відрізнятися від рішень для смартфонів. По-перше, аналіз потреб ресурсів смартфонів показав, що для більшості з них потрібен лише одноразовий або короткостроковий доступ до більшості ресурсів, що вимагають взаємодії з користувачами. Навпаки, додатки AR вимагатимуть довготермінового або постійного доступу до датчиків у масштабі, відмінному від програм для смартфонів. По-друге, доступ до ресурсів AR не буде таким явним для користувачів та спостерігачів, як у контексті смартфона. Наприклад, камера AR-системи завжди буде ввімкнена, тоді як камера смартфона, навіть якщо вона вмикається зловмисним програмним забезпеченням, надає набагато менше даних, коли телефон знаходиться в кишені користувача. Отже, можна зробити висновок, що при розробці рішень у цьому просторі важливо розглядати повноцінні майбутні контексти AR. До того ж потрібні нові дослідження щодо конкретних AR-рішень. Наприклад, дослідники почали розглядати підтримку специфічної

для AR операційної системи [15]. Додатки AR та базова ОС працюють таким чином: на першому етапі - сприйняття, додаток (або ОС) збирає необроблені сенсорні дані, такі як аудіо-, відео- або радіохвилі. Предметом дослідження тут буде обмеження того, як збирається інформація (наприклад, ввічливі камери) або обмеження їх використання (наприклад, політика збереження). На другому етапі – розпізнавання, алгоритми машинного навчання витягують об'єкти за допомогою семантики високого рівня. Предмет дослідження на цьому етапі - це зміна об'єктів, яку спричиняють помилкові негативи (наприклад, CV Dazzle [12]) та політика, що регулює доступ додатків до об'єктів. Нарешті, додаток (або ОС) відображається поверх почуттів користувача, таких як бачення та слух. Дослідження на цьому етапі включає виявлення інваріантів, яких необхідно дотримуватися, щоб не завдати шкоди користувачеві, та створення "надійного візуалізатора", який визначає ці інваріанти.

Не всі захисні напрямки для доповненої реальності складаються з технічних рішень. Деякі проблеми можуть потребувати соціальних, політичних або правових підходів. Прикладом може бути згадана вище потенційна політика виключення спостерігачів і сумісних камер.

Нарешті, очевидною стає необхідність тестування доповненої реальності розробниками. Більшість експериментальних додатків AR сьогодні покладаються на платформи Microsoft Kinect або смартфонів, таких як Layar, які включають в себе лише окремі додатки, що працюють одночасно, чим приховують проблеми, які виникають у зв'язку зі зростанням складності AR-системи.

Висновки. Системи доповненої реальності з їх складними і розповсюдженими можливостями введення, виведення та обробки даних будуть допомагати багатьом користувачам швидко і якісно сприймати та обробляти отриману інформацію. На додаток до постійних нововведень в технологіях AR, потрібно усвідомити, що настав час визначити «дорожню карту» для захисту комп'ютерної безпеки і конфіденційності AR-систем перш, ніж ці системи набудуть широкого розповсюдження. Щоб каталізувати цю «дорожню карту», потрібно розглянути нові проблеми безпеки і конфіденційності, що виникають в AR-системах, і дослідити можливості, надані цими технологіями, для створення нових додатків, що забезпечують конфіденційність та підвищують безпеку. Не варто забувати про те, що саме проблеми з даними і відсутність захищеності інших людей змусили перший пристрій доповненої реальності – окуляри Google Glass – піти з масового ринку. Тому захист даних і конфіденційності має бути головним завданням при розробленні технологій доповненої реальності. Ця технологія майбутнього повинна стати досконалим інструментом.

Список літератури:

1. Самотий В.В. Безпека інформації у технології доповненої реальності / В.В. Самотий, У.Ю. Дзелендзяк // Інформаційна безпека в сучасному суспільстві: зб. тез доповідей II Міжнародної наук.-техн. конф., 24-25 листопада 2016 р., м. Львів, Україна. – Львів: ЛДУ БЖД, 2016.– С. 92-93.

2. Горячев А. Защита мобильных приложений от кибератак / А. Горячев // Журнал “Information Security/ Информационная безопасность” №4, 2014.

3. Контактні лінзи доповненої реальності [Електронний ресурс]. – Режим доступу до ресурсу: http://vremya.eu/stati/kompyuternye-i-mobilnye-tehnologii/-ioptik-kontaktn-l-nzi-dopovneno-realnost1986544137.html.

4. Дуайт Дэвис. Реальные риски дополненной реальности / Дуайт Дэвис [Електронний ресурс]. – Режим доступу до ресурсу: http://www.osp.ru/cw/2016/12/13050187/.

5. Roesner F. Security and Privacy for Augmented Reality Systems / F. Roesner, T. Kohno, D. Molnar // Communications of the ACM, 2014, Vol. 57, № 4, 88-96 pp.

6. Poulsen, K. Hackers assault epilepsy patients via computer / K. Poulsen // WIRED Magazine, 2008. http://www.wired.com/ politics/security/news/2008/03/epilepsy.

7. Parviz, B. For your eye only / B. Parviz // IEEE Spectrum 46 (2009), 36–41.

8. CNN. Augmented-reality windshields and the future of driving, 2012 [Електронний ресурс].– Режим доступу до ресурсу: http://virtual.vtt.fi/virtual/proj2/multimedia/alvar.html.

9. Templeman, R. Placeraider: Virtual theft in physical spaces with smartphones /R. Templeman, Z. Rahman, D. J. Crandall, A. Kapadia // CoRR abs/1209.5982 (2012).

10. Roesner, F. User-Driven Access Control: Rethinking Permission Granting in Modern Operating Systems / F. Roesner, T. Kohno, A. Moshchuk, B. Parno, H. J. Wang, C. Cowan // In IEEE Symposium on Security and Privacy (2012).

11. Van Krevelen. A survey of augmented reality technologies, applications, and limitations / D.Van Krevelen, R. Poelman // The International Journal of Virtual Reality 9 (2010), 1–20.

12. Harvey, A. Cvdazzle: Camouflage from Computer Vision /A. Harvey [Електронний ресурс]. – Режим доступу до ресурсу: http://cvdazzle.com/.

13. Saroiu, S. I am a sensor, and I approve this message / S. Saroiu, A. Wolman // In Proceedings of the 11th Workshop on Mobile 8 Computing Systems and Applications (HotMobile) (2010), ACM.

14. Madejski, M. The Failure of Online Social Network Privacy Settings / M. Madejski, M.Johnson, S. M. Bellovin // Tech. Rep. CUCS-010-11, Dept. of Comp. Science, Columbia University, 2011.

15. D'antoni, L. Operating system support for augmented reality applications /L. D'antoni, A.Dunn, S. Jana, T. Kohno, B. Livshits, D. Molnar, A. Moshchuk, E. Ofek, F. Roesner, S.Saponas, M. Veanes, H. J. Wang. // In USENIX Workshop on Hot Topics in Operating Systems (2013).

References:

1. Samotyj, V. V., Dzelendzyak, U. Yu. (2016) Bezpeka informatsiyi v tekhnolohiyi dopovnenoyi realnosti // Informatsiyna bezpeka v suchasnomu suspilstvi: Materialy II Mizharodnoyi naukovo-tekhnichnoyi conferentsiyi: Tezy dopovidey. Lviv: LDU BZHD, 92-93.

2. Goryachev, A. Zashchita mobilnykh prilozheniy ot kiberatak. Information Security Journal, №4, 2014.

3. Kontaktni linzy dopovnenoyi realnosti: http://vremya.eu/stati/kompyuternye-i-mobilnye-tehnologii/-ioptik-kontaktn-l-nzi-dopovneno-realnost1986544137.html.

4. Duayt Devis. Realnye riski dopolnenoy realnosti: http://www.osp.ru/cw/2016/12/13050187/

5. Roesner, F., Kohno, T., Molnar, D. (2014) Security and Privacy for Augmented Reality Systems // Communications of the ACM, Vol. 57, № 4, 88-96 pp.

6. Poulsen, K. (2008) Hackers assault epilepsy patients via computer. WIRED Magazine http://www.wired.com/ politics/security/news/2008/03/epilepsy.

7. Parviz, B. (2009) For your eye only // IEEE Spectrum 46, 36–41.

8. CNN. Augmented-reality windshields and the future of driving (2012)// http://virtual.vtt.fi/virtual/proj2/multimedia/alvar.html.

9. Templeman, R., Rahman, Z., Crandall, D. J., Kapadia, A. (2012) Placeraider: Virtual theft in physical spaces with smartphones. CoRR abs/1209.5982.

10. Roesner, F., Kohno, T., Moshchuk, A., Parno, B., Wang, H. J., cowan, C. (2012) User-Driven Access Control: Rethinking Permission Granting in Modern Operating Systems // In IEEE Symposium on Security and Privacy.

11. Van Krevelen, D., Poelman, R. (2010) A survey of augmented reality technologies, applications, and limitations. The International Journal of Virtual Reality 9, 1–20.

12. Harvey, A. Cvdazzle: Camouflage from Computer Vision. http://cvdazzle.com/.

13. Saroiu, S., Wolman, A. (2010) I am a sensor, and I approve this message // In Proceedings of the 11th Workshop on Mobile 8 Computing Systems and Applications (HotMobile), ACM.

14. Madejski, M., Johnson, M., Bellovin, S. M. (2011) The Failure of Online Social Network Privacy Settings. Tech. Rep. CUCS-010-11, Dept. of Comp. Science, Columbia University.

D'antoni, L., Dunn, A., Jana, S., Kohno, T., Livshits, B., Molnar, D., Moshchuk, A., Ofek, E., Roesner, F., Saponas, S., Veanes, M., Wang, H. J. (2013) Operating system support for augmented reality applications. In USENIX Workshop on Hot Topics in Operating Systems.

❖❖❖