https://doi.org/10.31649/1997-9266-2019-146-5-49-54

УДК 004.02:004.77

І. П. Малініч[1]
В. І. Месюра[1]

ІН'ЄКТИВНИЙ МЕТОД ОТРИМАННЯ ДАНИХ КОРИСТУВАЦЬКОГО ДОСВІДУ В ІГРОВИХ СИМУЛЯТОРАХ КОМП'ЮТЕРНИХ МЕРЕЖ

[1]Вінницький національний технічний університет

Розглянуто способи організації роботи симуляторів комп'ютерних мереж, а також методи та підходи до отримання даних користувацького досвіду в них. Наведено особливості застосування цієї технології в розважальних та навчальних цілях. Визначено основні цілі збору користувацьких даних в ігрових симуляторах комп'ютерних мереж, які зокрема застосовуються в олімпіадних та конкурсних змаганнях з програмування та застосування IT-технологій. Приділено увагу проблемі збору даних користувацького досвіду в додатках, для доступу до яких використовується віддалене термінальне підключення з використанням стороннього програмного забезпечення.

Розглянуто особливості застосування програмних інтерфейсів технологій, функціонал яких можливо використати як основу для розробки методу: технології контейнеризації користувацького середовища операційної системи LXC та User Mode Linux, технологію перехоплення пакетів на основі мережевого екрану NetFilter та віртуального комутатора Open vSwitch. Приділено увагу ізоляції користувацьких процесів та трафіку від середовища хостової операційної системи, а також ризикам, які можуть виникнути в разі відсутності використання заходів та технологій роботи програмного коду в середовищі пісочниці.

Описано послідовність програмної реалізації ін'єктивного методу, а також особливості його використання в робочому середовищі. Приділено увагу журналюванню змін у журнальні файли та обліку активності користувачів у віртуальному середовищі у режимі реального часу. Описано особливості використання методу у кожному з двох варіантів базової технології контейнеризації: LXC та User Mode Linux. Запропоновано варіанти підвищення захищеності та надійності роботи самого методу при його інтеграції з технологією віртуалізації User Mode Linux. Розглядається можливість вдосконалення цього підходу завдяки використанню додаткових модулів ядра Linux.

Ключові слова: онлайн ігри, симулятори комп'ютерних мереж, користувацький досвід, віртуалізація, UI/UX, LXC, UML .

Вступ

Актуальність. Вивчення характеру взаємодії користувача з ігровими додатками потребує використання ефективних інструментів для отримання даних, необхідних для таких досліджень. Збір цих даних дозволяє визначати ефективність маркетингових заходів, швидше визначати пріоритетні для користувачів елементи, виявляти недоліки у використанні цих програмних рішень користувачами, а також фіксувати правильність застосування самого продукту. У різних веб-додатках, таких як онлайн-ігри [1], збір даних суттєво спрощується, оскільки майже вся активність користувача може бути зібрана на стороні сервера. У клієнт-серверних додатках, де користувацький інтерфейс побудований на інших ніж Web технологіях, для моніторингу активності користувача використовуються інструменти моніторингу користувацького досвіду (UI/UX) [2]. Подібні інструменти збирають дані користувацького досвіду, які є даними телеметрії і містять інформацію про подробиці використання графічного інтерфейсу. Модулі, які здійснюють збір даних користувацького досвіду, вбудовуються в клієнтську частину додатку, і з дозволу кінцевого користувача здійснюють цю функцію. В симуляторах комп'ютерних мереж та навчальних мережевих середовищах як клієнтів, крім основного інтерфейсу, доволі часто використовують додаткові утиліти для віддалених термінальних з'єднань, а також системні команди. Інтеграція модулів збору даних в подібне програмне забезпечення не дозволяє отримувати комплексні результати в межах цілого проекту, а

іноді взагалі є неможливою. Це також стосується аналізу трафіку, який створюється ними в процесі роботи. Прикладом є SSH-з'єднання [3], мережеві пакети яких є зашифрованими. Це перешкоджає аналізу виконуваних з терміналу користувача команд.

Зв'язок з важливими практичними завданнями. Отримання даних користувацького досвіду в ігрових симуляторах комп'ютерних мереж є необхідним для визначення стану виконання завдань кінцевими користувачами та забезпечення беззбійного проходження гри іншими учасниками. На відміну від звичайних симуляторів комп'ютерних мереж (таких як Cisco Packet Tracer), де завдання задаються курсами мережевої академії, в ігрових симуляторах користувач самостійно визначає необхідні цілі, для того щоб досягти бажаних результатів під час проходження ігрового сценарію. Крім безпосереднього застосування результатів досліджень в ігрових симуляторах, вивчення проблеми дозволить удосконалювати інструменти для виявлення мережевих вторгнень в реальному світі із застосуванням засобів штучного інтелекту (аналогічно як у мережах). Також цей метод матиме застосування у технологіях перевірки результатів олімпіад, конкурсів з програмування та використання ІТ-технологій.

Аналіз останніх досліджень і публікацій. Теоретичні і практичні аспекти застосування мережевих симуляторів з можливістю аналізу даних взаємодії об'єктів користувача наведені в роботах [4], [5]. Дослідження окремих проблем обміну даними рівня додатку описано в статтях [3], [6]. Побудова симуляційних моделей віртуальних мереж на основі LXC-контейнерів розглянута в статтях [7]—[9].

Методики побудови віртуальних обчислювально-мережевих середовищ для практичного вивчення роботи UNIX-подібних операційних систем з використанням контейнерів Linux описано в статтях [10], [11]. Методи збору користувацького досвіду для веб-додатків та CRM-систем опубліковані у публікаціях [2], [12].

У статтях, в яких розглянуто роботу мережевих симуляторів, описано методи аналізу моделей явного та фонового трафіку [5], симуляції, візуалізації, розширення та генерації сценаріїв [4]. Запропонована модель побудови віртуального мережевого середовища використовує симуляцію на основі реалізованого програмного додатку, який дозволяє організовувати роботу віртуального інтерфейсу, здатного пропускати пакети між віртуальною мережею та реальною мережею, яка може бути як лабораторною дослідницькою мережею, так і мережею, що має безпосередній доступ в мережу Інтернет.

Аналіз клієнт-серверної взаємодії на прикладному рівні (7-й рівень моделі OSI) в ігрових додатках здійснено у статті [6], де також розглянута робота P2P-протоколів та підходи до отримання даних про активність передачі даних. У публікації [3] розглядається специфіка виявлення зашифрованого трафіку для SSH та Skype. На основі матеріалів цих статей розглянуто метод отримання даних користувацької взаємодії на основі аналізу мережевих пакетів.

Невирішені аспекти проблеми. Оскільки користувач ігрових симуляторів комп'ютерних мереж крім користувацького веб-інтерфейсу може використовувати безпосередні способи підключення (такі як SSH та VPN), здійснення збору даних на боці клієнта або в проміжній точці не матиме жодного сенсу. Підключення здійснюються переважно за допомогою термінальних клієнтів з шифруванням, а також системного програмного забезпечення для організації VPN-з'єднань. Саме тому існує необхідність у пошуку нового способу для отримання даних про діяльність користувача на віртуальних вузлах симульованого ігрового середовища.

Метою дослідження є виявлення найефективніших способів отримання даних користувацького досвіду з додатків, які працюють всередині середовища ігрових симуляторів комп'ютерних мереж.

Розробка методу

В основу нового методу покладено використання технології контейнерів операційних систем, де передбачена можливість запуску довільного коду кінцевого користувача. На відміну від ігрових симуляторів, де застосовується емуляція роботи системних команд, повнофункціональний контейнер дає змогу організувати роботу справжнього випробувального середовища пісочниць.

Для здійснення збору даних користувацького досвіду у віртуальному середовищі основний процес на хостовій машині запускає модулі-агенти всередині кожного контейнера. Кожен модуль-агент при запуску отримує від основного процесу набір сигнатур процесів, відповідно з яких здійснюється збір даних користувацького досвіду. Сигнатури можуть бути таких типів: сигнатури файлів (хеш-суми або шлях у файловій системі), сигнатури UNIX-сокетів, сигнатури дій користу-

вача в системі, маски повідомлень журналів та сигнатури перехоплення для мережевого екрану.

Після отримання сигнатур внутрішній модуль відповідно до них запускає процеси монітору повідомлень системного журналу, монітору автентифікації користувачів, монітору процесів, а також монітору активності файлів та сокетів. Внутрішній модуль встановлює з'єднання з основним процесом на хостовій машині, через яке в режимі реального часу передаються та записуються в базу даних обліку активності (рис. 1) всі збіжності з сигнатурами, що виявляються моніторами.

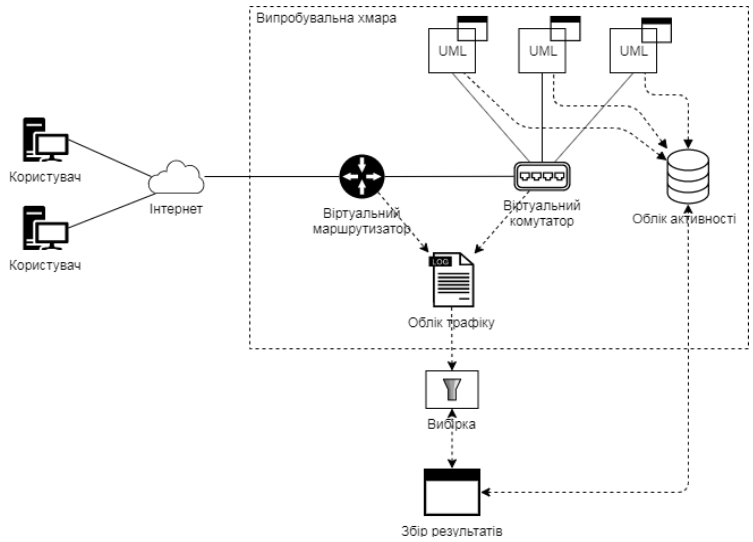

Рис. 1. Структурна схема випробувальної хмари, в якій здійснюється отримання даних користувацького досвіду

Для забезпечення гнучкості збору даних, метод передбачає можливість встановлення ієрархії різних сигнатур. Наприклад, при зв'язці двох сигнатур: файлової та мережевої, буде здійснюватись відслідковування мережевого трафіку лише процесів, виконавчі файли яких збігаються по хеш-сумі або певного шляху в системі. Так само є можливість пов'язати сигнатури активності користувачів та файлів: файловий монітор може сповіщати основний процес лише у випадку, якщо певний користувач створив відповідний файл.

Метод названо ін'єктивним тому, що робота основного модуля програмного забезпечення збору користувацьких даних передбачається на рівні хостової машини, де мають працювати контейнери, в яких повинні запускатись внутрішні модулі моніторингу. Необхідність застосування контейнерної архітектури у разі використання методу полягає в тому, що для процесу, який буде запускатись в такій пісочниці, сам процес збору даних залишатиметься невидимим. В традиційних контейнерах UNIX-подібних операційних систем через інтерфейс управління контейнером з'являється можливість здійснювати запуск резидентних модулів, які матимуть змогу відслідковувати активність запущених користувачами процесів.

Для збільшення можливостей відслідковування мережевих з'єднань пропонується використовувати додатковий рівень збору мережевих даних за межами контейнеру з використанням можливостей мережевих екранів або сенсорів. Збір пакетів або їх метаданих буде відбуватись за умови спрацювання тригерів сигнатур, встановлених на рівні контейнерів.

Особливості реалізації методу

Реалізація методу отримання даних користувацького досвіду в ігрових симуляторах комп'ютерних мереж значно ускладнюється через те, що кінцеві користувачі можуть встановлювати стороннє програмне забезпечення, а також створювати свій власний програмний код у своєму середовищі пісочниці. В цій статті розглядаються можливості двох технологій контейнеризації: Linux Containers (LXC) та User Mode Linux (UML), оскільки функціонал їх програмних інтерфейсів є достатньою мірою задокументований для потреб реалізації запропонованого методу. В ході дослідження випробувано можливість перехоплення пакетів засобами NetFilter. Як результат, використання можливостей цього програмного забезпечення створює помітні зміни в середовищі контейнера, які є видимими для кінцевого користувача. Через те, що користувач матиме змогу порушувати цей процес, перевага надається засобам перехоплення пакетів з використанням технології

OpenFlow на базі програмного пакету Open vSwitch, який використано для зв'язку між контейнерами (див. рис. 1). За потреби, функції обліку зовнішнього трафіку можуть також додатково здійснюватись за допомогою засобів віртуального маршрутизатора хмари.

Використання методу на основі технології LXC дозволяє програмним модулям збору даних безпосередньо запускати код підпрограм в середині самих контейнерів. Використання технології UML для реалізації методу передбачає створення додаткових програмних модулів для запуску агентів всередині внутрішнього середовища контейнерів.

Для обох платформ контейнерів розроблено програмні модулі моніторингу активності користувацьких процесів та збору даних користувацького досвіду. Програмну реалізацію модулів доповнено можливостями моніторингу активності користувачів, перехопленням повідомлень системного журналу, а також деталізованого збору даних роботи, обраних системою процесів, з яких проводиться подальша вибірка даних, вони є даними користувацького досвіду. Для управління детальністю та вибіркою повідомлень створено окремий програмний сервіс з відповідним програмним інтерфейсом.

З появою повідомлення про вразливість CVE-2019-5736, чимало розробників та спеціалістів безпеки приділили увагу можливості запуску шкідливого коду зсередини контейнера. Незважаючи на те, що розробниками знайдено рішення у вигляді латок та використання непривілейованого режиму, запропоноване рішення не повністю відповідає вимогам безпеки проекту.

Для цілей подальшого впровадження методу у виробничому середовищі приділено увагу технології UML та її можливостям для отримання даних користувацького досвіду в ігрових симуляторах комп'ютерних мереж. Така технологія використовує низькорівневі технології для управління та отримання даних з віртуальної машини. Замість програмного інтерфейсу для управління використовуються UNIX-сокети (рис. 2). Подібно до LXC, управління виділенням системних ресурсів для віртуальної машини може здійснюватись засобами бібліотеки libvirt.

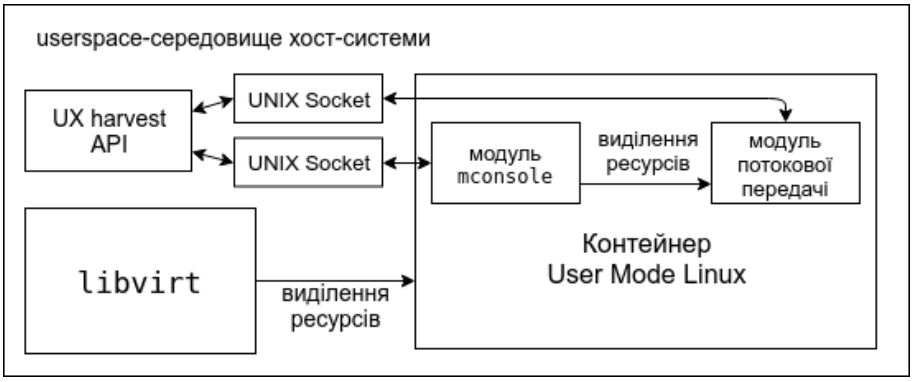

Рис. 2. Схема управління та збору користувацьких даних з контейнеру User Mode Linux

Для отримання користувацьких даних з файлів та виводу роботи системних утиліт здійснено модифікацію модуля mconsole та створено модуль потокової передачі, які подібно до створеного для технології LXC інструментарію можуть функціонувати повністю прозоро для кінцевого користувача. Перехоплення мережевих пакетів для технології UML, як і для LXC, можливе засобами Open vSwitch та не потребує особливих модифікацій, оскільки в обох них для приєднання до мережевого мосту використовується TAP-інтерфейс.

Технологія віртуалізації UML показала значно вищий рівень ізоляції, ніж той, що застосовується в технології LXC: в ній використовується окреме ядро операційної системи Linux, завдяки чому втрачається можливість взаємодії ізольованих процесів з ядром машини збору даних, що важливо при реалізації готових до використання в production-середовищі контейнерних рішень для побудови ігрових симуляторів комп'ютерних мереж. Крім того, ця технологія шляхом вбудовування відлагоджувальних модулів ядра була адаптована під виконання небезпечного програмного коду і нині має застосування як середовище пісочниці.

Висновки

В процесі розробки методу проаналізовано відомі підходи та методи збору даних користувацького досвіду в мережевих симуляторах. Запропоновано ін'єктивний метод отримання даних користувацького досвіду ігрових симуляторів комп'ютерних мереж, який дозволяє за рахунок

модульності процесів збору та ізоляції користувацьких процесів від основного процесу збору користувацьких даних забезпечити гнучкість збору даних та невидимість цих процесів для користувацького програмного забезпечення. Розглянуто різні платформи контейнерів, що мають необхідний для програмної реалізації методу функціонал. Запропоновано варіант підвищення захищеності та надійності роботи самого методу з інтеграцією з технологією віртуалізації UML.

Розроблений метод отримання даних користувацького досвіду в ігрових симуляторах комп'ютерних мереж дозволить спростити процес розробки та тестування подібних ігрових середовищ. Удосконалення методу збору та аналізу користувацької діяльності в таких середовищах дозволить в подальшій перспективі удосконалювати засоби для виявлення та нейтралізації спроб порушення ходу виконання гри з боку користувачів

Автори висловлюють подяку Міжнародному організаційному комітету студентської олімпіади «IT-Universe» за надання можливості випробування роботи експериментальних програмних модулів в рамках проведення олімпіади. Розроблені на основі запропонованого методу модулі використано для формування рейтингів учасників конкурсу та таблиці отриманих ними результатів в режимі реального часу.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

[1] Adams, Ernest. "Fundamentals of Game Design". 2nd edition. Berkeley, CA: New Riders, 2010, 700 p. ISBN 978-0321643377.

[2] І. П. Малініч, і В. І. Месюра, «Загальні підходи до здійснення збору користувацького досвіду ігрових додатків для попереднього аналізу пріоритетності вподобання елементів ігрового простору» в *Матеріали XLVIII Науково-технічної конференції ВНТУ*, Вінниця, 13-15 березня 2019 р, 2019. [Електронний ресурс]. Режим доступу: https://conferences.vntu.edu.ua/index.php/all-fitki/all-fitki-2019/paper/view/7238.

[3] R. Alshammari, and A. N. Zincir-Heywood, "Machine learning based encrypted traffic classification: Identifying ssh and skype," in *2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications.* 2009, July, pp. 1-8.

[4] L. Breslau, D. Estrin, H. Yu, and ather. "Advances in network simulation?", *Computer*, no. 1(5), pp. 59-67, 2000, May.

[5] A. Cohen, G. Cathey, and P. J. Malloy, inventors; OPNET Technologies Inc, assignee. "Mixed mode network simulator," United States patent US 6,820,042, 2004, Nov 16.

[6] S. D. Webb, W. Lau, and S. Soh, "An application layer network game simulator," in *Proceedings of the 3rd Australasian conference on Interactive entertainment*, Murdoch University, 2006, Dec 4, pp. 15-22. [Electronic resource]. Available: https://espace.curtin.edu.au/bitstream/handle/20.500.11937/47551/20019_downloaded_stream_7.pdf?sequence=2&isAllowed=y .

[7] C. Rotter, L. Farkas, G. Nyíri, G. Csatári, L. Jánosi, & R. Springer, "Using Linux containers in telecom applications," in *Proc. ICIN*, 2016. pp. 234-241. [Electronic resource]. Available: http://dl.ifip.org/db/conf/icin/icin2016/1570229487.pdf .

[8] G. Calarco, & M. Casoni, "On the effectiveness of Linux containers for network virtualization," *Simulation Modelling Practice and Theory*, no. 31, pp. 169-185, 2013, [Electronic resource]. Available: https://www.sciencedirect.com/science/article/pii/S1569190X1200161X .

[9] Lee Kyungwoon, Kim Youngpil, & Yoo Chuck, "The Impact of Container Virtualization on Network Performance of IoT Devices," *Mobile Information Systems*, 2018, 1-6. 10.1155/2018/9570506. [Electronic resource]. Available: https://www.researchgate.net/publication/324917584_The_Impact_of_Container_Virtualization_on_Network_Performance_of_IoT_Devices

[10] А. Батюк, Д. Ванькевич, і Г. Злобін, «Використання технологій віртуалізації в спецкурсі «Системне адміністрування ОС LINUX,» *Електроніка та інформаційні технології*, вип. 3, с. 220-225, 2013. [Електронний ресурс]. Режим доступу: http://nbuv.gov.ua/UJRN/Telt_2013_3_25 .

[11] O. M. Spirin, and O. S. Holovnia, «Застосування технологій віртуалізації unix-подібних операційних систем у підготовці бакалаврів інформатики,» *Information Technologies and Learning Tools*. 65. 201. (2018). 10.33407/itlt.v65i3.2055. [Електронний ресурс]. Режим доступу: https://www.researchgate.net/publication/331403054_ZASTOSUVANNA_TEHNOLOGIJ_VIRTUALIZACII_UNIX-PODIBNIH_OPERACIJNIH_SISTEM_U_PIDGOTOVCI_BAKALAVRIV_INFORMATIKI .

[12] К. А. Чернишов, І. П. Малініч, і П. П. Малініч, «Методи збору даних досвіду взаємодії користувача для випробувального етапу розробки через тестування,» на *Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення*, Міжнародна наукова Інтернет-конференція, м. Тернопіль, 5 лютого 2019 р., збірник тез доповідей. Тернопіль, 2019, вип. 35, с. 43.

Рекомендована кафедрою комп'ютерних наук ВНТУ

Стаття надійшла до редакції 9.10.2019

Малініч Ілля Павлович — аспірант кафедри комп'ютерних наук, e-mail: goosyara@vntu.edu.ua ;
Месюра Володимир Іванович — канд. техн. наук, доцент, професор кафедри комп'ютерних наук.
Вінницький національний технічний університет, Вінниця

I. P. Malinich[1]
V. I. Mesiura[1]

Injective Method of Data Harvesting of the User Experience Data in the Gaming Simulators of Computer Networks

[1]Vinnytsia National Technical University

In the paper the ways of organizing the simulator's work of computer networks are described, as well as methods and approaches for harvesting user experience. The application of this technology for entertainment and educational purposes is described. The main goals of collecting user data in gaming simulators of computer networks, which are used in particular in the competitions and contests for programming and application of IT technologies, are defined. Attention is drawn to the issue of collecting user experience data in applications that use a remote terminal connection using third-party software.

Features of application of software interfaces of technologies which functionality can be used as a basis for method development are reviewed: technologies of containerization of the user environment of the operating system LXC and User Mode Linux, technology of packet interception based on the NetFilter network firewall and Open vSwitch virtual switch. Attention is also paid to isolating user processes and traffic from the host operating system environment, as well as the risks that may arise in the absence of measures and technologies of the sandbox software isolation.

In the paper described the sequence of software implementation of the injective method, as well as the features of its use in the production environment. Attention is paid to logging changes to log files and real-time user activity logging. The features of the method are described in each of two variants of the basic containerization technology: LXC and User Mode Linux. The ways of increasing the security and reliability of the method itself when it is integrated with User Mode Linux virtualization technology are presented. Also ways of improving this approach by using additional Linux kernel modules are provided.

Keywords: online games, computer network simulators, user experience, virtualization, UI/UX, LXC, UML .

Malinich Illia P. — Post-Graduate Student of the Chair of Computer Sciences, e-mail: goosyara@vntu.edu.ua ;
Mesiura Volodymyr I. — Cand. Sc. (Eng.), Associate Professor, Professor of the Chair of Computer Sciences

И. П. Малинич[1]
В. И. Месюра[1]

Иньективный метод получения данных пользовательского опыта в игровых симуляторах компьютерных сетей

[1]Винницкий национальный технический университет

Рассмотрены способы организации работы симуляторов компьютерных сетей, а также методы и подходы к получению данных пользовательского опыта в них. Приведены особенности применения этой технологии в развлекательных и учебных целях. Определены основные цели сбора пользовательских данных в игровых симуляторах компьютерных сетей, в частности, применяются в олимпиадных и конкурсных соревнованиях по программированию и применению IT-технологий. Уделено внимание проблеме сбора данных пользовательского опыта в приложениях, для доступа к которым используется удаленное терминальное подключение с использованием стороннего программного обеспечения.

Рассмотрены особенности применения программных интерфейсов технологий, функционал которых возможно использовать за основу для разработки метода: технологии контейнеризации пользовательского среды операционной системы LXC и User Mode Linux, технологию перехвата пакетов на основе сетевого экрана NetFilter и виртуального коммутатора Open vSwitch. Уделено внимание изоляции пользовательских процессов и трафика от среды хостовой операционной системы, а также рискам, которые могут возникнуть в случае отсутствия использования мер и технологий работы программного кода в среде песочницы.

писана последовательность программной реализации иньективного метода, а также особенности ее использования в рабочей среде. Уделено внимание журналированию изменений в журнальные файлы и учету активности пользователей в виртуальной среде в режиме реального времени. Описаны особенности использования метода в каждом из двух вариантах базовой технологии контейнеризации: LXC и User Mode Linux. Предложены варианты повышения защищенности и надежности работы самого метода при его интеграции с технологией виртуализации User Mode Linux. Рассматривается возможность совершенствования такого подхода благодаря использованию дополнительных модулей ядра Linux.

Ключевые слова: онлайн игры, симуляторы компьютерных сетей, пользовательский опыт, виртуализация, UI/UX, LXC, UML .

Малинич Илья Павлович — аспирант кафедры компьютерных наук, e-mail: goosyara@vntu.edu.ua ;
Месюра Владимир Иванович — канд. техн. наук, доцент, профессор кафедры компьютерных наук