

УДК 519.8

ВІРТУАЛІЗАЦІЯ НАВЧАЛЬНИХ СИСТЕМ

Маслова Н.О., к. т.н., доцент, nataliia.maslova@donntu.edu.ua, ДВНЗ «ДонНТУ»

Любименко О.М., к. ф.-м.н., доцент, olena.liubymenko@donntu.edu.ua, ДВНЗ «ДонНТУ»

Програмне забезпечення освітнього призначення в даний час набуло широкого поширення в освітньому процесі, тому питання безпеки систем навчання, особливо в умовах збільшення кількості загроз, стає все більш актуальним. З розвитком хмарних обчислень з'явилася можливість подальшого вдосконалення тестових та навчальних систем.

Хмарні технології передбачають віддалену обробку та зберігання даних, звільняють користувача від необхідності забезпечувати високу продуктивність свого комп'ютера та керувати програмним забезпеченням. Достатньо мати доступ до Інтернет та використовувати хмарні сервіси й працювати з системою через браузер. Це зручно, й, тим більш, сприяє підвищенню захищеності системи, бо однією з істотних вимог, які висуваються до хмарних структур є забезпечення необхідного рівня безпеки.

Але контроль безпеки залишається актуальною проблемою і самі навчальні системи повинні відповідати високим вимогам, включаючи: захист від копіювання, шахрайства та несанкціонованого доступу до матеріалів; велику тестову базу даних (або базу знань); простий програмний інтерфейс; зручне керування тестами для адміністраторів; повну автоматизацію процесу тестування; мінімізацію часу між відправкою запиту та отриманням відповіді від системи.

Метою роботи є дослідження захищеності навчальних систем, та можливостей механізмів використання хмарних технологій для розміщення систем й освітнього контенту на хмарах різного типу.

У попередніх дослідженнях [1] показано, що розміщення розподілених навчальних систем на гібридній хмарі і шифрування даних на стороні клієнта покращують показники безпеки.

У сфері інформаційної безпеки важливим є поняття інформаційного ризику, що визначається як функція трьох змінних: ймовірності наявності загрози, ймовірності наявності незахищеності та потенційного впливу. Таке дослідження з виділенням погроз безпеці навчальних систем наведено в [2].

Провівши аналіз впливу усіх аспектів для забезпечення безпеки навчальних систем, можна виділити, наступне: використання віртуального середовища може спричинити появу нових ризиків безпеки, ці ризики можна знизити за допомогою контрзаходів, переважно управлінського та організаційного характеру. Розміщення навчального ресурсу на хмарних

платформах збільшує рівень захищеності системи, оскільки інфраструктура належить і керується організацією, що надає хмарні послуги, і вона вживає всіх необхідних заходів для забезпечення безпеки своїх сервісів.

Ризики безпеки можна знизити за допомогою гібридної хмари як моделі розгортання хмарних обчислень, оскільки провайдеру послуг можна передати лише частину функцій системи, а частину даних розмістити на власних надійно захищених ресурсах або на структурах інших постачальників хмарних послуг. Також важливо забезпечити інформаційну безпеку на стороні клієнта шляхом застосування стандартних механізмів, таких як ідентифікація, автентифікація, шифрування, захист від перехоплення, запобігання несанкціонованому доступу до системи та інші.

Перед створенням моделі навчальної системи, необхідно чітко визначити набір функцій та вимог до неї, далі розглянути можливість розподілу системи для її подальшого розміщення в «хмарі», й перейти до реалізації поставленої задачі. При використанні гібридної моделі допускається вибір найкращого за параметрами захищеності, швидкості зчитування інформації та максимально допустимого розміру файлу сховища. Матеріали навчальних посібників можуть бути розміщені як на локальному комп'ютері, так і в Інтернеті, залежно від технічних можливостей та застосованих політик безпеки. А переконфігурація системи з розміщенням програмного модуля й контенту на різних хмарах дозволяє підвищити захищеність структури в цілому.

Висновок. Впровадження сучасних інформаційних технологій у навчання дозволяє досягти запланованих результатів лише за умови надійної, безпечної та продуктивної роботи всієї ІТ-інфраструктури. Зі зростанням обсягів оброблюваної інформації зростають вимоги до підвищення продуктивності та захищеності навчальних систем. З розвитком технологій віртуалізації з'являється можливість подальшого вдосконалення освітніх систем й систем дистанційного навчання.

Сучасним напрямком є розміщення систем й їх контенту на хмарних ресурсах. Але перехід на технологію віртуалізації вимагає зміни конфігурації системи. Тому необхідно ретельно та усвідомлено підходити до вирішення питань забезпечення безпеки при такому переході, враховувати нові ризики та перетворювати чи проектувати систему таким чином, щоб її архітектура якнайкраще вписувалася у хмарні сервіси.

Список використаних джерел

1. Маслова Н. О., Сорокін Р. О. Використання хмарних технологій як спосіб підвищення захищеності тестових учнів систем. Штучний інтелект. № 4; 2013: 463 – 475
2. Narasymchuk, O., Opriskyu, I., Sovyn, Y., Tyshyk, I., Shtefaniuk, Y.. Організація захисту результатів контролю знань в системах дистанційного навчання. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», № 2(10); 2020: 144–157, <https://csecurity.kubg.edu.ua/index.php/journal/article/view/215>