Міністерство освіти і науки України
Державна служба України з надзвичайних ситуацій
Львівський державний університет безпеки життєдіяльності
Національний університет «Львівська політехніка»

# ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

Збірник тез доповідей
III Всеукраїнської науково-практичної конференції
молодих учених, студентів і курсантів

**28 листопада 2019 року**

Львів – 2019

**ББК 32.81+78.362**

*Захист інформації в інформаційно-комунікаційних системах: з*бірник тез доповідей ІІІ Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 28 листопада 2019 року. Львів, ЛДУ БЖД, 2019, 290 с.



За точність наведених фактів, самостійність наукового аналізу та нормативність стилістики викладу, а також за використання відомостей, що не рекомендовані до відкритої публікації відповідальність несуть автори опублікованих матеріалів.

# АНАЛІЗ ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ СУЧАСНОГО ХОСТИНГУ ПРИ ТЕСТУВАННІ НА ПРОНИКНЕННЯ

**Лагун А., Рудик А., Рудик Ю.**
***Львівський державний університет безпеки життєдіяльності, Львів***

**Summary.** The levels of cloud computing and cyber security are considered. Approaches to information security of cloud hosting are given. Their essence is based on principle: the security of the cloud – is the responsibility of the provider, the security in the cloud – is the responsibility of the client. Therefore, the issue of improving the safety of cloud services and hosting requires a variety of attention.
**Keywords:** hosting, cyber security, vulnerability, cloud computing, safety, quality.

**Анотація.** Розглядаються рівні хмарних обчислень та кібербезпеки. Наведено підходи до інформаційної безпеки хмарного хостингу. Їх суть заснована на принципі: безпека хмари - це відповідальність провайдера, безпека в хмарі - це відповідальність клієнта. Тому питання підвищення безпеки хмарних сервісів та хостингу потребує різноманітної уваги.
**Ключові слова:** хостинг, кібербезпека, вразливість, хмарні обчислення, безпека, якість.

Враховуючи ріст потреби присутності в мережі інтернет більшості галузей людської діяльності все більше підприємців звертаються до послуг хостинг провайдерів. Адже вони дають можливість розмістити свій веб-ресурс на середовищі яке часто можна шкалювати в залежності від потреби споживача, що значно заощадить останнім кошти [1].

Але при цьому користувач хостингу розміщує свої особисті дані на апаратурі яка може знаходитись на іншому континенті, лише з надією на те що надавач хостингових послуг вбереже їх від потенційної небезпеки. При цьому користувач хостингу на своєму веб ресурсі може зберігати і дані своїх клієнтів, втрата яких може завдати чималої шкоди.

Надавачі послуг хостингу впевнені в безпеки своїх серверів з технічного боку, і наразі чималі зусилля прикладаються щоб закрити прогалину яку по собі лишає так званий людський фактор. При цьому кошти на ліцензоване ПЗ для захисту від вірусів, фаєрволи, ОС економляться за рахунок безкоштовних прогам з відкритим кодом.

Метою дослідження є проведення аналізу вразливостей які можна виявити у системах які користуються попитом у численної кількості хостинг провайдерів: cPanel на CentOS. Попри надзвичайну гнучкість та простоту у використанні, це ПЗ потребує постійних оновлень оскільки виявляються все нові вразливості в коді, що ставить під загрозу інформацію яка зберігається на таких системах.

Таким чином, виникає потреба у надійному та якісному обміні даними та застосуванні методів та інструментів програмного забезпечення. Це підвищить ефективність роботи пожежно-рятувальних підрозділів, якість взаємодії, обміну даними та оцінку результатів. Економічний ефект виправданий скороченням часу реагування та усуненням наслідків надзвичайних ситуацій, зменшенням залежності від апаратного старіння обладнання, гнучкості застосування веб-програмного забезпечення та незалежності платформи [2].

Методи дослідження. У роботі використовується комплексний метод дослідження, який включає: аналіз та узагальнення наукових досягнень у галузі інформаційних технологій, застосування статистики хостингу.

SQL – це тип вразливості безпеки веб-додатків, при якому зловмисник намагається використовувати код програми для доступу чи пошкодження вмісту бази даних. Якщо це вдасться, це дозволяє зловмиснику маніпулювати даними, які зберігаються в бек-енд-базі, будь-яким чином їм подобається. Інжекція SQL – це один з найпоширеніших типів уразливості безпеки веб-додатків [3].

Неправильна конфігурація безпеки охоплює кілька типів уразливості, все зосереджено на недостатньому обслуговуванні або недостатній увазі до налаштування сервера. Потрібно визначити та розгорнути безпечну конфігурацію для програми, рамок, сервера додатків, веб-сервера, сервера баз даних та платформи. Неправильні налаштування безпеки надають хакерам доступ до приватних даних або функцій і можуть призвести до повного системного компромісу. Оскільки ресурси на хостинговому сервері розтягуються, деякі хостинг-провайдери часто скорочують кути в своїх конфігураціях, щоб менше ресурсів витрачалося, коли служби безпеки виконують заплановані перевірки / завдання. Це, безумовно, ставить власників веб-сайтів у важке місце, часто вибираючи між ціною добре захищеного сервера або більш дешевою, менш безпечною альтернативою.

Завдяки програмному забезпеченню, що охоплює потенційний шкідливий код, вони часто заважатимуть роботі фактичного власника. Це так звані "помилково-позитивні" тригери, які зупинятимуть показ оновлень завдяки тому, що містять ключові слова, які потенційно можуть бути використані шкідливим чином. У цих випадках користувачі виберуть зручність користування перед безпекою шляхом дозволу цих ключових слів, відкривши вікно можливостей для тих, хто має наміри проникнення.

Безпека як складова є важливим елементом загальної якості обслуговування PQoS - це оцінка якості інформаційного обслуговування з точки зору сприйняття користувача як споживача цієї послуги.

Буде створена віртуальна лабораторія, що максимально близько імітуватиме середовище хостингу. Саме тестування на проникнення буде реалізовуватись за допомогою інструментарію який пропонується системою Kali Linux та іншим відповідним ПЗ.

Нарешті, у кожному заході цифрової безпеки завжди існує людський фактор, оскільки соціальні інженери намагатимуться ввести власників хостингу чи постачальників послуг хостингу в обмін даними входу на ресурси, інакше недоступні для них. Цей спосіб злому не вимагає поглиблених технічних знань і складних сценаріїв, тому жоден брандмауер не може захистити його. Люди, що працюють в галузі IT, повинні бути пильними щодо того, якими деталями вони діляться та кому. Провівши серію з тестувань на проникнення, можна зробити висновки щодо обґрунтованості виходу безпеки з точки зору ПЗ на другий план на фоні фокусу щодо зменшення витрат та зосередження на навчанні персоналу безпечної поведінки.

Також буде можливість співставити рівень опору тестуванню на проникнення з можливими затратами на ліцензійне ПЗ на прикладі Cloud-Linux та ConfigServer eXploit Scanner, що дасть можливість користувачам послуг хостингу підібрати надавача послуг таким чином, щоб впевненість в безпеці їхніх даних була непохитною.

**Література**

1. Maksymiv O, Rak T, Menshikova O, Deep convolutional network for detecting probable emergency situations, Data Stream Mining & Processing (DSMP), IEEE First International Conference, 2016.

2. Рак Т., Рудик Ю., Рудик А. Засоби оперативного управління діяльністю підрозділів ДСНС з використанням IT-технологій на базі геоінформаційного комплексу, Львів, АСВ, 2015– С. 267-270.

3. Most common web security vulnerabilities [online source] https://www.commonplaces.com/blog/6-common-website-security-vulnerabilities/

# З М І С Т

## Секція 1

## КІБЕРБЕЗПЕКА

### Напрям 1. УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ



### Напрям 2. ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

**Напрям 3. ТЕХНІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ**



**Напрям 4. БЕЗПЕКА ІНФОРМАЦІЇ У ХМАРНИХ СХОВИЩАХ**

*Наукове видання*

# ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

Збірник тез доповідей
ІІІ Всеукраїнської науково-практичної конференції
молодих учених, студентів і курсантів


Відповідальні за випуск **Олександр Придатко**
**Назарій Бурак**

Оригінал-макет **Олександр Хлевной**

Друк на різографі **Маріанна Климус**

Підписано до друку 12.11.2019 р.
Формат 60×84/16. Гарнітура Times New Roman.
Друк на різографі. Папір офсетний.
Ум. друк. арк. 17,8.

**Друк ЛДУ БЖД**
79007, Україна, м. Львів, вул. Клепарівська, 35
тел./факс: (032) 233-32-40, 233-24-79.