Львівський державний університет безпеки життєдіяльності

Національний університет Львівська політехніка

Департамент кіберполіції Національна поліція України

Львівська міська рада

LVIV IT CLUSTER

softserve

UnderDefense

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей
IV Міжнародної науково-практичної конференції
ІБІТ 2022

30 листопада 2022 року

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

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей
IV Міжнародної науково-практичної конференції
ІБІТ 2022

30 листопада 2022 року

Львів
Растр-7
2022

УДК 351.746:007:004
І 74

Інформаційна безпека та інформаційні технології: збірник тез доповідей IV Міжнародної науково-практичної конференції, ІБІТ 2022, м. Львів, 30 листопада 2022 року. – Львів: Растр-7, 2022. – 380 с.

ISBN 978-617-8134-79-2

У збірнику опубліковано матеріали IV Міжнародної науково-практичної конференції "Інформаційна безпека та інформаційні технології". На основі теоретичних та експериментальних досліджень представлено інноваційні підходи у сфері кібербезпеки та інформаційних технологій. Обговорено та запропоновано сучасні шляхи щодо захисту інформації як на особистому, так і на державному рівнях.

УДК 351.746:007:004

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.

ISBN 978-617-8134-79-2

Zbigniew KOKOSIŃSKI – dr hab. Inż., prof. PK kierownik Katedry Politechnika Krakowska im. Tadeusza Kościuszki;

Volodymyr SAMOTYY – prof. dr hab. inż., professor, Katedra Automatyki i Informatyki Politechnika Krakowska im. Tadeusza Kościuszki;

Sergii TELENYK – prof. dr hab. inż., professor, Department of automatic control and computer engineering Cracow University of Technology;

Володимир РОМАКА – д.т.н., професор, професор кафедри захисту інформації Національного університету "Львівська політехніка";

Іван ОПІРСЬКИЙ – д.т.н., професор, професор кафедри захисту інформації Національного університету "Львівська політехніка";

Любомир СІКОРА – д.т.н., професор, професор кафедри автоматизованих систем управління Національного університету "Львівська політехніка";

Наталя ЛИСА – д.т.н., доцент, доцент кафедри кафедри автоматизованих систем управління Національного університету "Львівська політехніка";

Тетяна ГОВОРУЩЕНКО – д.т.н., професор, завідувач кафедри комп'ютерної інженерії та інформаційних систем Хмельницького національного університету;

Ольга МЕНЬШИКОВА – к.ф.-м.н., доцент, заступник начальника навчально-наукового інституту цивільного захисту Львівського державного університету безпеки життєдіяльності з навчально-наукової роботи;

Андрій Івануса – к.т.н., доцент, доцент кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності;

Валентина ЯЩУК – к.е.н., доцент, доцент кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності;

Орест ПОЛОТАЙ – к.т.н., доцент, доцент кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності;

Валерія БАЛАЦЬКА – викладач кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності;

Ігор МАЛЕЦЬ – к.т.н., доцент, доцент кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності;

Назарій БУРАК – к.т.н., доцент, доцент кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності;

Ольга СМОТР – к.т.н., доцент, доцент кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності;

Юрій БОРЗОВ – к.т.н., доцент, доцент кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності;

Роман ГОЛОВАТИЙ – к.т.н., старший викладач кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності;

Олександр ХЛЕВНОЙ – к.т.н., старший викладач кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності.

Інформаційні джерела

1. Zhmurko T., Kinzeryavyy V., Yubuzova Kh., Stojanovic A. Generalized classification of modern quantum cryptography and communication methods. Ukrainian Scientific Journal of Information Security, 2015, vol. 22, issue 3, p. 287-293.
2. Banerjee A., Pathak A. Efficient protocols for deterministic secure quantum communication using GHZ-like states. Quantum Physics, 2018.
3. Lili Yan, Shibin Zhang, Yan Chang, Zhibin Sun, and Zhiwei Sheng. Quantum secure direct communication protocol with mutual authentication based on single photons and Bell states. Computers, Materials & Continua, 63(3):1297–1307, 2020.
4. Banu N., Ghosal P. and Panigrahi P. K., "Quantum information splitting of an unknown two qubit state by using two three qubit GHZ like states, " 2014 International Conference on Electronics and Communication Systems (ICECS), 2014, pp. 1-4, doi: 10.1109/ECS.2014.6892773.
5. Shukla Ch., Banerjee A., Pathak A. Improved Protocols of Secure Quantum Communication Using W States. International Journal of Theoretical Physics, 2018, vol. 52, pp. 1914–1924.

УДК 004.6

КІБЕРЗАХИСТ В ІНТЕГРОВАНИХ СИСТЕМАХ САНКЦІОНОВАНОГО ДОСТУПУ ДО ІНФОРМАЦІЇ

Андрій Рудик, Юрій Рудик, Наталія Федінець

Кафедра управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності, м. Львів, Україна

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.*

Abstract. *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.*

Президент росії оголосив про початок “спецоперації” з метою “демілітаризації і денацифікації України” вранці 24 лютого. Цей день став початком повномасштабної війни проти України. Цілі “спецоперації” неодноразово змінювалися і зрештою трансформувалися у “захист населення Донбасу”. На сьогодні, в умовах військової повномасштабної агресії росії в Україні всі завдання цивільного захисту і безпеки громадян перебувають в нових вимірах [1–3].

Нині нашою головною метою є вдосконалення діяльності підрозділів ДСНС України, оснащення рятувальників сучасними технічними засобами та налагодження тісної взаємодії з органами місцевої влади у процесі забезпечення цивільного захисту населення. Російські інформаційні операції виявилися незграбними й були спростовані оприлюдненням розвідданих. А спроби росіян зруйнувати цифрову інфраструктуру України та посіяти розбрат за допомогою кіберможливостей були зустрінуті стійким, професійним та ефективним українським кіберзахистом. Це новий фронт війни в Україні, і його наслідки продовжуватимуться і після її завершення. У системах кіберзахисту слід вжити заходів, щоб протистояти організованим державним кампаніям з дезінформації та домогтися того, щоб їм не вдалося приглушити міжнародне обурення діями Росії [4–5].

У всіх цих сферах спостерігаються спроби російської держави узгодити та скоординувати кібернетичні можливості з більш традиційними аспектами військової потуги. На сьогодні ці гібридні наміри не мали успіху – їхній вплив виявився меншим, ніж очікували. Почасти це пояснюється тим, що Україна зарекомендувала себе надзвичайно ефективним кіберзахистом. Після анексії Криму у 2014 році в різних сферах і галузях створювали цифрову фортецю. Поряд із героїчною обороною українських військових, в інтернеті, можливо, була найефективніша оборонна кіберактивність дотепер. Діючи під постійним тиском проти дуже здібного противника, ця команда з представників бізнесу, розвідки, служб безпеки, а в деяких випадках і громадян, працювала пліч-о-пліч, попереджаючи, реагуючи та усуваючи наслідки.

У відповідь на стрімкий розвиток засобів несанкціонованого доступу до інформації в результаті загального прогресу сучасних інформаційних та комп’ютерних технологій є необхідність підтримки актуальності систем захисту підприємств від несанкціонованого доступу та контролю за працівниками [6].

Загроза безпеки активів об’єкту інформаційної діяльності складається з безлічі пов’язаних і автономних елементів. Розглядаючи загрозу безпеки, як комплекс, виникає ідея пошуку комплексного рішення до потенційної загрози.

Розробляючи комплексну систему санкціонованого доступу потрібно прослідкувати за вдосконаленням вже існуючих та появу нових організаційних, програмних та технічних способів, які б допомогли в побудові комплексної систем санкціонованого доступу та захисту інформації [7].

Саме правильне проведення процесу розробки комплексної системи санкціонованого доступу дозволяє оптимізувати як процес реалізації комплексу на практиці, так і гарантувати його максимальну ефективність під час експлуатації.

Підбір компонентів комплексу здійснено враховуючи характеристики об'єкту інформаційної діяльності, елементи якої формували зокрема і просторові та бюджетні вимоги [8].

Підійшовши до спроєктованої системи у ролі зловмисника вдалось сформувати картину вразливостей об'єкту під захистом комплексу, та запропонувати способи їх вирішити. З повторенням цієї процедури можна отримати кілька ітерацій комплексу, з різним рівнем захисту, який буде пропорційним до затрат на його реалізацію та підтримку. Вибір варіанту варто здійснювати оцінюючи ризики.

Інформаційні джерела

1. Три сценарії розвитку війни в Україні URL: https://texty.org.ua/tag/khid-vijny/

2. Парламентська асамблея НАТО визнала Росію державою-терористом URL: https://www.radiosvoboda.org/z/16697

3. Найкоротша історія російсько-української війни URL: https://www.radiosvoboda.org/a/31382202.html

4. Ткачук Р.Л., Сікора Л.С., Лиса Н.К., Навитка М.Л., Сабат В.І., Федина Б.І., Тупичак Л.Л. Інформаційні технології формування стратегій прийняття рішень інтелектуальним агентом в техногенних системах за умов когнітивних збоїв, НУЛП, 2020.

5. Полотай О.І. Важливість комплексної системи захисту інформації у забезпеченні інформаційної безпеки ГО "Наукова спільнота"; WSSG w Przeworsku. – Тернопіль, 2022 https://sci.ldubgd.edu.ua/jspui/handle/123456789/11113

6. Лагун А., Рудик А., Рудик Ю. Аналіз виявлення вразливостей сучасного хостингу при тестуванні на проникнення, Захист інформації в інформаційно-комунікаційних системах, Львів, 2019. С.53-55.

7. Полотай О.І., Масюк Н. Профілі можливостей порушників інформаційної безпеки структурних підрозділів безпекових структур Національна Академія Служби Безпеки України, 2021.

8. Ткачук Р.Л., Боднар О., Лагун А. Е. Виявлення небезпечних входжень у комп'ютерну мережу за допомогою систем виявлення вторгнень, ЛДУБЖД, 2021.

Наукове видання

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей
IV Міжнародної науково-практичної конференції
ІБІТ 2022

Відповідальні за випуск **Ростислав ТКАЧУК**
Олександр ПРИДАТКО

Оригінал-макет **Ростислав ТКАЧУК,**
Андрій ІВАНУСА

Видано в авторській редакції

Підписано до друку 30.11.2022 р.
Формат 60×84/16. Папір офсетний. Друк цифровий.
Умовн. друк. арк. 22,09. Обл.-вид. арк. 20,55.
Наклад 100 прим.

Видавець і виготовлювач: ТОВ "Растр-7"
79005, м. Львів, вул. Кн. Романа, 9/1.
Тел./факс: (032) 235 72 13. E-mail: rastr.sim@gmail.com
www.rastr-7.com.ua
Свідоцтво суб'єкта видавничої справи
ЛВ № 22 від 19.11.2002 р.