Контейнер є запущеним екземпляром образу, який функціонує як ізольований процес у системі. Контейнери створюються на основі образів і забезпечують виконання застосунків у відокремленому середовищі.

Dockerfile — це текстовий файл, що містить інструкції для автоматизованого створення образу. У ньому визначається базове середовище, необхідні залежності та команди, які потрібно виконати для підготовки контейнера до роботи.

4. Порівняння контейнерів та віртуальних машин

Контейнеризація та віртуалізація є різними підходами до ізоляції процесів, які мають суттєві відмінності в архітектурі та ефективності використання ресурсів. Контейнери створюють ізольовані середовища, що використовують спільне ядро операційної системи хоста, тоді як віртуальні машини функціонують як повноцінні незалежні системи з власним ядром.

Порівняння основних характеристик контейнерів і віртуальних машин наведено у таблиці 1.

Таблиця 1

Порівняння контейнерів і віртуальних машин

| Характеристика | Контейнери | Віртуальні машини |
|---|---|---|
| Ядро ОС | Спільне | Окреме |
| Час запуску | 1–3 секунди | 20–60 секунд |
| Витрати пам’яті | 50–200 МБ | 512 МБ – 2 ГБ |
| Накладні витрати | 2–5% | 5–15% |
| Рівень ізоляції | Частковий | Повний |

1. Роль контейнеризації та віртуалізації на рівні операційної системи в розвитку хмарно орієнтованих додатків. Наукова періодика Міжрегіональної Академії управління персоналом. URL: https://journals.maup.com.ua/index.php/it/article/view/4822/5115 (дата звернення: 26.04.2026).
2. Docker Inc. What is Docker?. Docker Documentation. URL: https://docs.docker.com/get-started/docker-overview/ (date of access: 28.04.2026).
3. Docker Inc. What is an image?. Docker Documentation. URL: https://docs.docker.com/get-started/docker-concepts/the-basics/what-is-an-image/ (date of access: 28.04.2026).

## Critical Infrastructure Security: Electronic Communications Networks of Electronic Communications Operators

UDK: 004.056:004.7:621.39:351.86

Olena Shelest-Polishchuk [1],
Bohdan Skybun[2]

*Kyiv Professional College of Communication,*
*[1] deksog@ukr.net, [2] skubyn.bogdan@gmail.com*

The further development of digital technologies, digitization of information, communication, social, management and production processes together with the growth of levels of virtual cyberspace form a new digital reality and digital space. In turn, cyberspace combines with physical space to form a new cyber-physical space. At the same time, electronic communications ensure the full functioning of the cyber-physical space, and also provide an opportunity to receive, transmit, process, store and protect huge arrays of digital information produced by humanity. Thus, in modern realities, electronic communications act as an important transport system for the transmission of information, data and communication on a global world level. Also, electronic communications act as a catalyst for further development of digital society, digital economy and digital infrastructure.

Currently, the digital infrastructure creates the prerequisites for building a new level of critical infrastructure that is able to function in the modern realities of the growth of cyber threats. At the same time, the level of dependence of critical infrastructure on modern electronic communications is increasing, because computer networks, information and information and communication systems of enterprises, organizations, institutions, companies and corporations are built on their basis.Also, the globalization of management and production processes takes place on the basis of the use of international electronic communications and the global data transmission network, namely, monitoring, management, and security systems are created at the facility, corporate, and sectoral levels of production and management. Thus, "security of critical infrastructure" is characterized as "a state of protection of critical infrastructure, which ensures the functionality, continuity of work, restoreability, integrity and stability of critical infrastructure" [3, Article 1].

Today, stability and stability are quite important factors that characterize the functioning of the infrastructure under the influence of external and internal factors of influence.

All this requires electronic communications operators to build their own infrastructure, which would be resistant to external and internal factors of influence, as well as ensure sustainable functioning under the influence of cyber threats. Thus, "resilience of critical infrastructure" is defined as "the state of critical infrastructure, which ensures its ability to function normally, to adapt to constantly changing conditions, to withstand and quickly recover from threats of any

species" [3, Article 1]. It should be taken into account that in accordance with Government Resolution No. 1109, electronic communications are included in the List of critical infrastructure sectors [1], and therefore electronic communications operators need to ensure a sufficient level of security, stability and stability in relation to their own networks and infrastructure for the possibility of providing electronic communication services and electronic networks for other sectors of critical infrastructure. Thus, an important feature of electronic communications is that, on the one hand, they are a sector of critical infrastructure, and on the other hand, they are part of other sectors of critical infrastructure. Currently, the financial and banking spheres, the energy sphere, the security and defense sphere, the educational and medical spheres are quite sensitive to the stable and sustainable functioning of electronic communications.

In addition, electronic communication services and services based on electronic communications are the basis of the modern development of digital technologies, digitalization of society and economy, namely: e-education, e-banking, mobile banking, e-services, telemedicine, e-government, etc. Also, the development and spread of electronic communications among many countries and broad segments of the population gave impetus to the rapid development (quantitative and qualitative indicators) of mobile applications, various software products, various software products (specialized software), as well as the rapid growth of the number of users of messengers and social networks. The next important step was the transition to the virtual space of organizations, institutions, and enterprises. Yes, today almost all authorities (central, regional, district and local levels have their own websites and communicate with the population online), educational institutions of all levels, medical institutions, financial and banking institutions, the sphere of service provision, etc. All this also requires stable and sustainable functioning for the possibility of providing various services to the population.

At the same time, experts within the framework of the study "Increasing resilience by accelerating the digital transformation of business in Ukraine" consider digitization and digital transformation as an important element "for increasing resilience and facilitating recovery" [2, p.17], which directly depend both on the level of development of electronic communications and the global data transmission network, as well as on access to them by broad sections of the population.

1. Some issues of critical infrastructure objects, Resolution of the CMU dated October 9, 2020 No. 1109. https://zakon.rada.gov.ua/laws/show/1109-2020-%D0%BF#Text
2. Increasing sustainability by accelerating the digital transformation of business in Ukraine. https://surl.li/asaeds
3. On critical infrastructure: Law of Ukraine of November 16, 2021 No. 1882-IX Vedomosti Verkhovna Rada (VVR), 2023, No. 5, Article 13. https://zakon.rada.gov.ua/laws/show/1882-20#Text

## Інтерактивні сценарії як інструмент викладання стандартів технічного захисту інформації

УДК 004.94:004.921

Юрій Скоренький[1], Руслан Козак[2],
Наталія Загородна[3], Тетяна Вітенько[4]

*Тернопільський національний технічний університет імені Івана Пулюя,*
*[1]skorenkyy@tntu.edu.ua, [2]zagorodna.n@gmail.com, [3]ruslank@tntu.edu.ua*
*[4]vitenko@tntu.edu.ua*

Стрімка цифровізація вищої освіти зумовила нагальну потребу в зміні парадигми в бік модульних, стійких та інтерактивних педагогічних моделей. У контексті трансформації української вищої освіти інституційне виживання значною мірою залежить від переходу від екстреного дистанційного викладання до сталої цифрової педагогіки. Викладання основ технічного захисту інформації та узгодження зі стандартами (зокрема, ISO/IEC 27001) становить значний