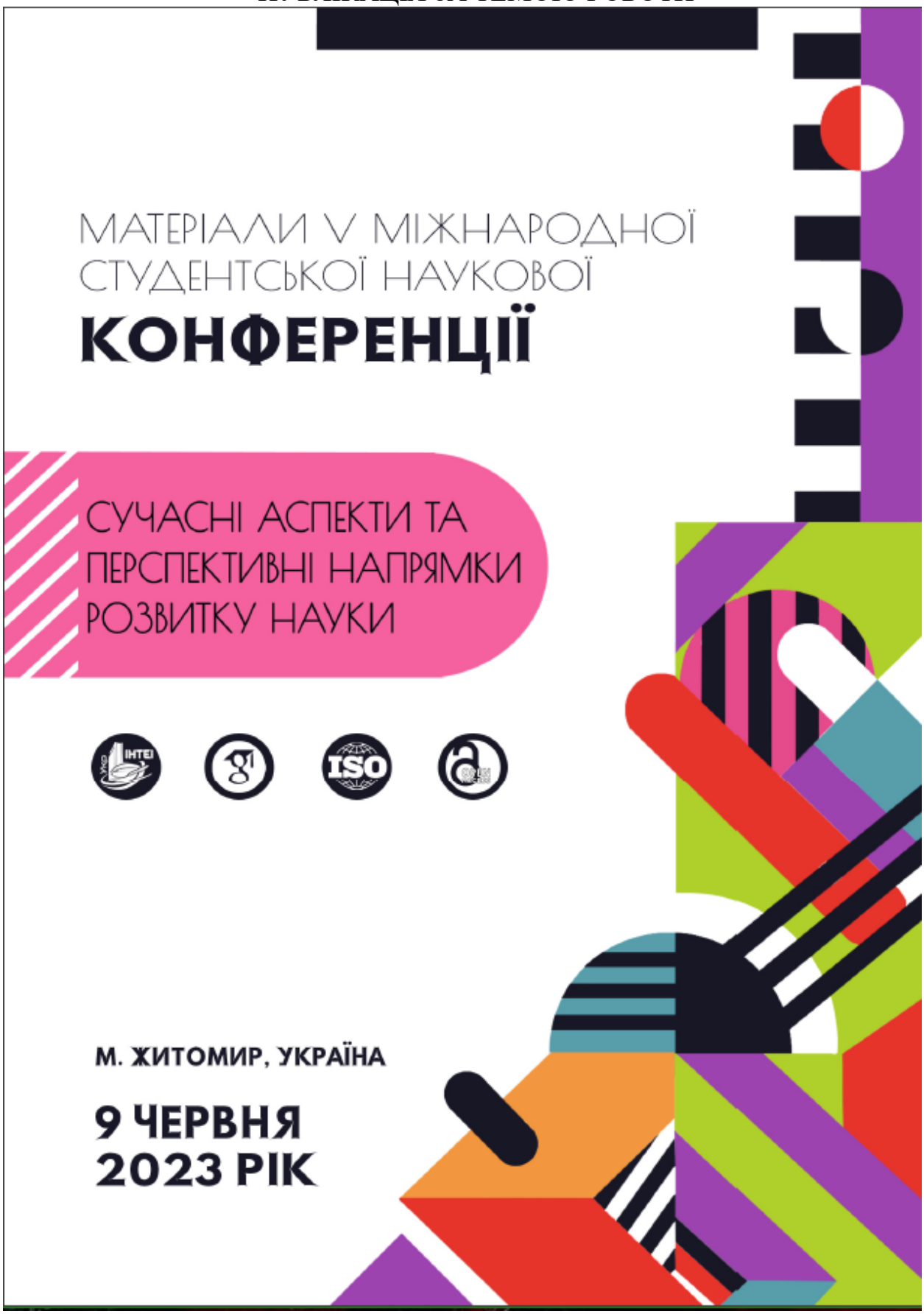
ДОДАТОК А
ПУБЛІКАЦІЯ ЗА ТЕМОЮ РОБОТИ



СЕКЦІЯ 11.
ЕЛЕКТРОНІКА ТА ТЕЛЕКОМУНІКАЦІЇ

СЕКЦІЯ 12.
КОМП'ЮТЕРНА ТА ПРОГРАМНА ІНЖЕНЕРІЯ

Москаленко Єгор Олександрович, здобувач вищої освіти
факультету інфокомунікацій
Харківський національний університет радіоелектроніки, Україна

Науковий керівник: Штих Інна Анатоліївна, старший викладач
кафедри радіотехнологій інформаційно-комунікаційних систем
Харківський національний університет радіоелектроніки, Україна

ПОБУДОВА ЗАХИЩЕНИХ МЕРЕЖ НА СЕАНСОВОМУ РІВНІ

Сеансовий рівень є максимально високим рівнем моделі OSI, на якому можливе формування захищених віртуальних каналів. При побудові захищених віртуальних мереж на цьому рівні досягаються найкращі показники щодо функціональної повноти захисту інформаційного обміну, надійності контролю доступу, а також простоти конфігурування системи безпеки. Протоколи формування захищених віртуальних каналів на сеансовому рівні є прозорими для прикладних протоколів захисту, а також високорівневих протоколів надання різних сервісів (протоколів HTTP, FTP, POP3, SMTP, NNTP та ін.). Однак, на сеансовому рівні починається безпосередня залежність від додатків, які реалізують високорівневі протоколи. Тому реалізація протоколів захисту інформаційного обміну, що відповідають цьому рівню, у більшості випадків потребує внесення змін до високорівневих мережних додатків [1].

Так як сеансовий рівень моделі OSI відповідає за встановлення логічних з'єднань та керування цими з'єднаннями, то на даному рівні з'являється можливість використання програм-посередників, які перевіряють допустимість запитаних з'єднань та забезпечують виконання інших функцій захисту міжмережної взаємодії. У загальному випадку програми-посередники, які традиційно використовуються у міжмережних екранах, можуть виконувати такі функції [1]:

- ідентифікація та аутентифікація користувачів;
- криптозахист даних, що передаються;
- розмежування доступу до ресурсів внутрішньої мережі;
- розмежування доступу до ресурсів зовнішньої мережі;
- фільтрація та перетворення потоку повідомлень, наприклад, динамічний пошук вірусів та прозоре шифрування інформації;
- трансляція внутрішніх мережних адрес для вихідних пакетів повідомлень;
- реєстрація подій і реагування на події, що задаються;
- кешування даних, що запитуються із зовнішньої мережі.

Таким чином, при побудові захищених віртуальних мереж на сеансовому рівні з'являється можливість не тільки криптографічного захисту інформаційного обміну, включаючи аутентифікацію, а й можливість реалізації ряду функцій посередництва між сторонами, що взаємодіють.

Для криптографічного захисту інформаційного обміну на сеансовому рівні найбільшу популярність отримав протокол SSL/TLS (Secure Sockets Layer/Transport Layer Security), розроблений компанією Netscape Communications [1].

Протокол Secure Sockets Layer (SSL), що спочатку орієнтований на захист

інформаційного обміну між клієнтом і сервером комп'ютерної мережі, є промисловим протоколом сеансового рівня моделі OSI, який використовує для забезпечення безпеки інформаційного обміну криптографічні методи захисту інформації. Конфіденційність даних, що передаються, забезпечується за рахунок їх криптографічного закриття, а аутентифікація взаємодіючих сторін, а також справжність і цілісність циркулюючої інформації – за рахунок формування та перевірки цифрового підпису [1].

Список використаних джерел:

1. Шаньгин В.Ф. Информационная безопасность. / В.Ф. Шаньгин – М.: ДМК Пресс, 2014. – 702 с.