

МВС України  
Харківський національний університет  
внутрішніх справ

Координатор проектів ОБСЄ в Україні

**АКТУАЛЬНІ ПИТАННЯ ПРОТИДІЇ  
КІБЕРЗЛОЧИННОСТІ ТА ТОРГІВЛІ  
ЛЮДЬМИ**

**Збірник матеріалів  
Всеукраїнської науково-практичної  
конференції**

**(23 листопада 2018 року, м. Харків)**

Харків  
ХНУВС  
2018

УДК [351.74:343.85](062.552)  
А43

*Друкується за рішенням оргкомітету  
відповідно до доручення ХНУВС від 19.09.2018 № 122*

**А43** **Актуальні** питання протидії кіберзлочинності та торгівлі людьми : збірник матеріалів Всеукр. наук.-практ. конф. (23 листоп. 2018 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ ; Координатор проектів ОБСЄ в Україні. – Харків : ХНУВС, 2018. – 436 с.

У матеріалах конференції окреслено найбільш актуальні проблеми протидії кіберзлочинності та торгівлі людьми на сучасному етапі; проаналізовано питання правового та організаційного забезпечення протидії кіберзлочинності та торгівлі людьми; кримінально-правові, процесуальні та криміналістичні аспекти протидії цьому негативному явищу; розглянуто відповідний міжнародний досвід, а також кадрове забезпечення правоохоронних органів. Досліджено використання інформаційних технологій і технічних засобів у протидії кіберзлочинності та торгівлі людьми.

УДК [351.74:343.85](062.552)

*Публікації наведено в авторській редакції з незначними коректорськими правками. Оргкомітет не завжди поділяє погляди авторів публікації. За достовірність наукового матеріалу, професійного формулювання, фактичних даних, цитат, власних імен, географічних назв, а також за розголошення фактів, що не підлягають відкритому друку, тощо відповідають автори публікацій та їх наукові керівники.*

*Електронна копія збірника безоплатно розміщується у відкритому доступі на сайті Харківського національного університету внутрішніх справ (<http://www.univd.edu.ua>) у розділі «Видавнича діяльність. Матеріали науково-практичних конференцій, семінарів тощо», а також у репозитарії ХНУВС (<http://dspace.univd.edu.ua/xmlui/>).*

*Видано Координатором проектів ОБСЄ в Україні в рамках проекту «Посилення кримінального переслідування торгівлі людьми з використанням інформаційних технологій в Україні», за фінансової підтримки уряду Сполучених Штатів Америки.*

*Усі права захищено. Зміст посібника можна безкоштовно копіювати та використовувати в освітніх та інших некомерційних цілях за умови посилання на джерело інформації.*

**Координатор проектів ОБСЄ в Україні та уряд Сполучених Штатів Америки не несуть відповідальності за зміст та погляди, висловлені у цій публікації.**

© Харківський національний університет  
внутрішніх справ, 2018  
© Координатор проектів ОБСЄ в Україні, 2018

- Можасв О. О., Можасв М. О., Логвиненко М. О., Чорний С. В.**  
Автоматизована система накопичення емпіричних даних у сфері комп'ютерно-технічних експертиз..... 302
- Мордвинцев М. В., Хлестков О. В., Ницюк С.П.**  
Використання автоматизованих систем відеодокументування переміщень об'єкта для протидії торгівлі людьми..... 304
- Осіпов Я. В., Світличний В. А.**  
Атака нульового дня (N-day attack). Що це і як з цим боротися?.. 306
- Передерій Т. С., Маковоз О. С.**  
Система fraud-моніторингу в запобіганні та виявленні шахрайств з платіжними картками ..... 310
- Світличний В. А., Онищенко Ю. М.**  
Протоколи, методи і технології захисту комп'ютерних мереж на транспортному рівні ..... 314
- Семенов С. Г., Давидов В. В., Волошин Д. Г.**  
Про завдання позиціонування безпілотних літальних апаратів в умовах кібератак..... 317
- Скрилюк В. Д.**  
Порівняльний аналіз апаратних та програмних криміналістичних рішень для роботи з даними з мобільних пристроїв, комп'ютерної техніки з функцією телефону ..... 320
- Стрельбицький М. А., Андрощук О. С., Равлюк В. В.**  
Проблема спільного функціонування моделей розмежування доступу на загальному полі даних гетерогенних інформаційних систем..... 322
- Струков В. М., Узлов Д. Ю., Власов О. В.**  
Максимінний критерій визначення первинних центрів в алгоритмах кластеризації K-means..... 326
- Тулупов В. В., Лашенко А.О.**  
Особливі питання реагування на DOS та DDOS атаки..... 329
- Узлов Д. Ю., Струков В. М., Власов О.В.**  
Використання інтелектуального аналізу даних у протидії інформаційній злочинності..... 331
- Філіппов С. О.**  
Значення біометричних технологій для протидії транскордонній злочинності ..... 334

УДК 004.056.5

**Віталій Анатолійович СВІТЛИЧНИЙ,**

*кандидат технічних наук,*

*доцент кафедри кібербезпеки факультету № 4 (кіберполіції)*

*Харківського національного університету внутрішніх справ;*

*ORCID: <https://orcid.org/0000-0003-3381-3350>;*

**Юрій Миколайович ОНИЩЕНКО,**

*кандидат наук з державного управління, доцент,*

*доцент кафедри кібербезпеки факультету № 4*

*Харківського національного університету внутрішніх справ;*

*ORCID: <https://orcid.org/0000-0002-7755-3071>*

## **ПРОТОКОЛИ, МЕТОДИ І ТЕХНОЛОГІЇ ЗАХИСТУ КОМП'ЮТЕРНИХ МЕРЕЖ НА ТРАНСПОРТНОМУ РІВНІ**

**Вступ і постановка проблеми.** В останнє десятиліття широке застосування комп'ютерних технологій в автоматизованих системах обробки інформації та управлінні процесами призвело до загострення проблеми захисту інформації, що циркулює в комп'ютерних системах OSI (Open System Interconnection). Особливістю протоколів транспортного рівня таких систем, є відсутність перевірки джерел інформації, що сприяє таким загрозам, як перехоплення та підключення до відкритих портів протоколів транспортного рівня.

Захист від перехоплення потребує застосування додаткових протоколів, які підтримують шифрування даних та автентифікацію суб'єктів обміну даними. Для вирішення цієї задачі використовується протокол SSL/TLS (Secure Socket Layer / Transport Layer Security), який реалізує шифрування і автентифікацію між транспортними рівнями приймача і передавача.

Процедура роботи протоколу SSL/TLS включає в себе три основних фази:

- діалог між сторонами, метою якого є вибір алгоритму шифрування;
- обмін ключами на основі криптосистем з відкритим ключем або автентифікація на основі сертифікатів;
- передачу даних за допомогою симетричних алгоритмів шифрування [1].

Тобто протокол SSL/TLS виконує функції автентифікації, шифрування даних і забезпечення цілісності даних. Автентифікація здійснюється шляхом обміну цифровими сертифікатами при встановленні з'єднання [1]. Так як протокол SSL/TLS реалізується на транспортному рівні, захищене з'єднання встановлюється «з кінця в кінець» (захищений віртуальний тунель транспортного рівня).

Протокол прикладного рівня SSL/TLS зазвичай використовується для забезпечення шифрування HTTP трафіку (режим HTTPS).

Відкритий характер протоколів прикладного рівня зумовлює значну кількість загроз, пов'язаних з основною проблемою цих протоколів – передачею інформації у нешифрованому вигляді. Використання на прикладному рівні процедур ідентифікації та автентифікації користувачів із подальшою авторизацією утворює також загрозу перехоплення або підбору облікових записів та паролів. Значну загрозу також становлять віруси та шпигунське програмне забезпечення, які діють саме на прикладному рівні, DoS та DDoS-атаки на інформаційні системи.

Зазвичай, для засобів захисту комп'ютерних мереж на прикладному рівні, існує два підходи: використання проку-серверів та використання механізмів контролю сесій (Statefull Inspection). Обидва ці підходи реалізують контроль за з'єднанням, але не вирішують задачу аналізу змісту пакетів та фільтрації пакетів з небажаним змістом, що не дозволяє запобігти розповсюдженню вірусів через електронну пошту, встановленню несанкціонованих програмних додатків через Інтернет на робочі станції, несанкціонованій зміні змісту веб-сайтів тощо. Для захисту від таких порушень може бути використана контентна фільтрація, яка базується на сигнатурному аналізі пакетів. Цей механізм передбачає аналіз інформації у пакеті, при чому як заголовка пакета, так поля даних. Це дозволяє встановити відповідність між інформацією з поля даних та конкретними додатками, контролювати передачу даних між конкретними додатками та проводити фільтрацію небажаної інформації. Враховуючи, що інформація аналізується окремими пакетами, цей механізм не дозволяє повністю аналізувати трафік мережних додатків [2].

Окремо слід відзначити забезпечення безпеки гетерогенних віртуальних обчислювальних середовищ, до яких відносять GRID-системи та «хмарні обчислення» (cloud computing). З кожним роком все більше різних підприємств і вищих навчальних закладів переводять обчислювальні та інформаційні ресурси у віртуальну інфраструктуру. У таких середовищах виникають нові загрози. Перш

за все, це атаки на засоби управління віртуальними машинами, хмарні контролери, сховища даних, неавторизований доступ до вузлів віртуалізації, використання віртуального середовища для несанкціонованої передачі даних.

Можливість проведення наведених атак із віртуальної мережі суттєво обмежує використання традиційних для комп'ютерних мереж методів захисту та потребує розробки спеціалізованих рішень. В основу таких рішень може бути покладено механізми контролю сесій (Statefull Inspection) та пакетної фільтрації. Так, у роботі [2] пропонується підхід до розмежування доступу на основі контролю віртуальних з'єднань та використання скритої фільтрації. Правила фільтрації можуть бути створені для різних рівнів опису потоків даних на підставі заголовків каналних, мережних, транспортних та прикладних протоколів.

Таким чином, враховуючи велику кількість та різноплановість протоколів та програмних додатків прикладного рівня, організувати ефективну протидію загрозам прикладного рівня можна тільки шляхом розробки та реалізації комплексних систем захисту інформації з використанням спеціалізованих механізмів розмежування та контролю доступу до ресурсів мережі, застосування технологій криптографічного захисту та електронних цифрових підписів, але розгляд останніх технологій виходить за рамки даних тез доповіді.

Одним з ефективних рішень комплексного захисту інформаційних систем корпоративних мереж є використання мережі доставки/поширення контенту (Content Delivery Network або Content Distribution Network, CDN). Системи на базі CDN ефективно вирішують питання захисту від DoS та DDoS-атак не тільки на прикладному, а і на мережевому і транспортному рівнях [3].

Провідні виробники мережевого обладнання пропонують спеціалізовані рішення для вирішення задач комплексного захисту корпоративних мереж. Наприклад компанія Cisco пропонує рішення за допомогою технології NAC (Network Admission Control) [4]. Дана технологія дозволяє не тільки перевіряти пристрої та користувачів ще на етапі підключення до корпоративної мережі, а і заблокувати доступ комп'ютерів, які не відповідають політиці безпеки (в тому числі заражених вірусами та шкідливими програмами, де не оновлено антивірусні бази, відсутні необхідні оновлення операційної системи тощо). Контроль відповідності політиці безпеки реалізується максимально близько до можливого джерела порушень – на порту комутатора, точки доступу Wi-Fi або маршрутизатора, які підтримують технологію NAC.

**Висновок.** Задача створення ефективних комплексних систем захисту комп'ютерних мереж може бути вирішена з використанням сукупності методів та технологій, які реалізовані в сучасному телекомунікаційному обладнанні для комп'ютерних мереж, як основи технічної складової таких систем. При виборі та реалізації технологій

захисту для конкретної мережі необхідно враховувати особливості структури мережі, спеціалізації роботи підприємства, вірогідність проведення конкретних атак. Налаштування відповідного функціоналу на мережевому обладнанні дозволяє здійснювати контроль відповідності політиці мережевої безпеки та реалізовувати захист максимально близько до можливого джерела порушень, що, у свою чергу, мінімізує можливі негативні наслідки для корпоративної мережі моделі OSI.

#### **Список бібліографічних посилань**

1. Кучернюк В. П. Методи і технології захисту комп'ютерних мереж (фізичний та каналний рівні). *Мікросистеми, електроніка та акустика*. 2017. № 6. Том 22. С. 64-70. URL: <http://elc.kpi.ua/article/view/113191> (дата звернення: 24.10.2018).

2. Заборовский В. С., Лукашин А. А., Купреенко С. В., Мулюха В.А. Архитектура системы разграничения доступа к ресурсам гетерогенной вычислительной среды на основе контроля виртуальных соединений. *Вестник Уфимского государственного авиационного технического университета*. 2011. 5 (45). Том. 15. С. 170-174. URL: <https://elibrary.ru/item.asp?id=18863047> (дата звернення: 24.10.2018).

3. Козлова М. 7 лучших сервисов защиты от DDoS-атак для повышения безопасности // HOSTING.cafe. 28 марта 2017 14:47. URL: <https://habrahabr.ru/company/hosting-cafe/blog/324848/> (дата звернення: 24.10.2018).

4. Cisco Network Admission Control (NAC) Solution Data Sheet // Cisco. January 23, 2017. URL: [https://www.cisco.com/c/en/us/products/collateral/security/nac-appliance-clean-access/product\\_data\\_sheet0900aecd802da1b5.html](https://www.cisco.com/c/en/us/products/collateral/security/nac-appliance-clean-access/product_data_sheet0900aecd802da1b5.html) (дата звернення: 24.10.2018).

*Одержано 24.10.2018*