

**ДЕРЖАВНА СЛУЖБА УКРАЇНИ
З НАДЗВИЧАЙНИХ СИТУАЦІЙ**

Львівський державний університет
безпеки життєдіяльності

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

Захист інформації в інформаційно-комунікаційних системах: збірник тез доповідей III Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 28 листопада 2019 року. Львів, ЛДУ БЖД, 2019, 288 с.

РЕДКОЛЕГІЯ:

Андрій КУЗИК – д.с.-г.н., професор, проректор Львівського державного університету безпеки життєдіяльності (ЛДУ БЖД);

Володимир САМОТИЙ – д.т.н., професор, завідувач кафедри управління інформаційною безпекою ЛДУ БЖД;

Євген МАРТИН – д.т.н., професор, завідувач кафедри управління проектами, інформаційних технологій та телекомунікацій ЛДУ БЖД;

Василь ПОПОВИЧ – д.т.н., доцент, начальник навчально-наукового інституту цивільного захисту ЛДУ БЖД;

Ольга МЕНЬШИКОВА – к.ф.-м.н., доцент, заступник начальника навчально-наукового інституту цивільного захисту ЛДУ БЖД з навчально-наукової роботи, полковник служби цивільного захисту;

Олександр ПРИДАТКО – к.т.н., заступник начальника кафедри управління проектами, інформаційних технологій та телекомунікацій ЛДУ БЖД;

Наталія КУХАРСЬКА – к.ф.-м.н., доцент, доцент кафедри управління інформаційною безпекою ЛДУ БЖД;

Тарас БРИЧ – к.т.н., доцент кафедри управління інформаційною безпекою ЛДУ БЖД;

Орест ПОЛОТАЙ – к.т.н., доцент кафедри управління інформаційною безпекою ЛДУ БЖД;

Марія ШАБАТУРА – к.т.н., доцент кафедри управління інформаційною безпекою ЛДУ БЖД;

Ігор МАЛЕЦЬ – к.т.н., доцент, доцент кафедри управління проектами, інформаційних технологій та телекомунікацій ЛДУ БЖД;

Назарій БУРАК – к.т.н., доцент кафедри управління проектами, інформаційних технологій та телекомунікацій ЛДУ БЖД;

Ольга СМОТР – к.т.н., доцент кафедри управління проектами, інформаційних технологій та телекомунікацій ЛДУ БЖД;

Роман ГОЛОВАТИЙ – к.т.н., викладач кафедри управління проектами, інформаційних технологій та телекомунікацій ЛДУ БЖД;

Олександр ХЛЕВНОЙ – викладач кафедри управління проектами, інформаційних технологій та телекомунікацій ЛДУ БЖД.

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.

З М І С Т

Секція 1

КІБЕРБЕЗПЕКА

Напрям 1. УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Дмитренко А., Мірошниченко В. СУТНІСТЬ ПОТЕНЦІЙНИХ ТА РЕАЛЬНИХ ЗАГРОЗ ІНФОРМАЦІЇ	4
Довганик С., Полотай О. СИСТЕМИ ЗБОРУ ІНФОРМАЦІЇ ПРО БЕЗПЕКУ ТА УПРАВЛІННЯ ПОДІЯМИ	7
Дубей С., Козловський В., Фірман В. УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ	10
Поворозник Ю.П., Малець І.О. ФОРМУВАННЯ АГРЕГОВАНИХ ДАНИХ	13
Реуцьонюк О., Гарасимчук О. ДОСЛІДЖЕННЯ УРАЗЛИВОСТІ МІЖСАЙТОВОГО ВИКОНАННЯ СЦЕНАРІЇВ	16
Самара Н.М. ОЦІНКА ЗАХИЩЕНОСТІ ПРОМИСЛОВИХ ІНФОРМАЦІЙНИХ СИСТЕМ SCADA	19
Сіренко Н.О., Малець І.О. ПРОЦЕСОР НА ПЛІС ДЛЯ СТИСНЕННЯ ВІДЕО ПОТОКУ ДЛЯ СИСТЕМИ ЗБОРУ НАУКОВОЇ ІНФОРМАЦІЇ МІКРОСУПУТНИКА	23
Смерека Б.А., Косиєв О. ТЕЛЕМЕТРІЯ ЧИ КІБЕРШПИГУНСТВО? ...	26
Требко А.О. ЗАХИСТ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО- КОМУНІКАЦІЙНИХ СИСТЕМАХ	28

Напрям 2. ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Yuliya Hrynyk, Bozhena Vysochanska, Roman Golovaty PROTECTION OF INFORMATION IN NETWORKS	32
Балацька В.С., Шабатура М.М. СКАНЕРИ ВРАЗЛИВОСТІ КОМП'ЮТЕРНОЇ МЕРЕЖІ	34
Болеківський Н., Полотай О. КЛАСИФІКАЦІЯ МЕРЕЖЕВИХ АТАК ТА МЕТОДИ ПРОТИДІЇ І ЗАХИСТУ	37
Бужанська М., Подолець Р., Палійчук Р. ЗАХИСТ ІНФОРМАЦІЇ ПРИ КОРИСТУВАННІ СОЦІАЛЬНИМИ МЕРЕЖАМИ	40
Градишук С. БЕЗПЕКА КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ДАНИХ: РЕАЛІЇ СЬОГОДЕННЯ	43
Димкар В. М., Фірман І. В. ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ	45

Гузела Н., Белей О. БЕЗПЕКА ПЕРЕДАЧІ ДАНИХ МІЖ ПРИБОРАМИ В БЕЗПРОВІДНИХ СЕНСОРНИХ МЕРЕЖАХ ІОТ	93
Дулова О. ІНФОРМАЦІЙНА БЕЗПЕКА ТА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В ХМАРНИХ СЕРВІСАХ	96
Масляк О.І., Григлевич М.О., Фірман В.М. ПРОБЛЕМИ БЕЗПЕКИ ІНФОРМАЦІЇ У ХМАРНИХ СХОВИЩАХ.....	99
Романчук Д. А. БЕЗПЕКА ІНФОРМАЦІЇ У ХМАРНИХ СХОВИЩАХ	101
Тютченко С.М., Воробець Х. О. БЕЗПЕКА ЗБЕРІГАННЯ ІНФОРМАЦІЇ В ХМАРНИХ СХОВИЩАХ.....	103
Шуцман Р.П., Дудикевич В.Б. ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ AMAZON WEB SERVICES.....	106

Напрямок 5. КРИПТОГРАФІЧНІ ТА СТЕГАНОГРАФІЧНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ

Кіріченко С. КРИПТОГРАФІЧНІ ТА СТЕГАНОГРАФІЧНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ.....	109
Кордунова Ю., Кухарська Н. РОЗРОБКА ПРОГРАМНОГО КОМПЛЕКСУ ДЛЯ ПРИХОВУВАННЯ У ПСЕВДОВИПАДКОВО ОБРАНИХ БІТАХ РАСТРОВОГО ЗОБРАЖЕННЯ ЗАШИФРОВАНОВОГО ЗА ДОПОМОГОЮ ШИФРУ RC4 ПОВІДОМЛЕННЯ.....	111
Онишко Т., Фірман Л. Ю. ВИКОРИСТАННЯ КРИПТОГРАФІЧНИХ ТА СТЕГАНОГРАФІЧНИХ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ ДЛЯ БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ	113
Петлеванна І., Зайва А. ОСОБЛИВОСТІ НЕЗБАЛАНСОВАНОЇ МЕРЕЖІ ФЕЙСТЕЛЯ.....	116
Тарабасва Д.Д., Шпінарева І.М. АНАЛІЗ ВБУДОВУВАННЯ ІНФОРМАЦІЇ У ЗОБРАЖЕННЯ ЗА ДОПОМОГОЮ ВЕЙВЛЕТ ПЕРЕТВОРЮВАНЬ	118
Тарасов А.І., Шпінарева І.М. СИСТЕМА ЕЛЕКТРОННОГО ГОЛОСУВАННЯ З ЗАСТОСУВАННЯМ ТЕХНОЛОГІЇ БЛОКЧЕЙН....	121
Хомич І., Кухарська Н. ПОБУДОВА КРИПТОСТЕГАНСИСТЕМИ НА ОСНОВІ ВИКОРИСТАННЯ ШИФРУ AES ТА МЕТОДУ БЛОКОВОГО ПРИХОВУВАННЯ ІНФОРМАЦІЇ	122

Напрямок 6. ІНФОРМАЦІЙНІ ВІЙНИ

Бойко В.С., Бурак Н.Є. ІНФОРМАЦІЙНА ВІЙНА ЯК ЗАГРОЗА БЕЗПЕЦІ ДЕРЖАВИ.....	124
Бородін І.В., Тарнавський А.Б. ІНФОРМАЦІЙНА ВІЙНА ЯК СЬОГОДЕННА РЕАЛЬНІСТЬ	127
Бужанська М., Манич Т. ВИДИ ІНФОРМАЦІЙНИХ ВІЙН	129

Інформаційні війни

УДК 004.62

ІНФОРМАЦІЙНА ВІЙНА ЯК ЗАГРОЗА БЕЗПЕЦІ ДЕРЖАВИ

Бойко В.С., Бурак Н.С.

Львівський державний університет безпеки життєдіяльності

У роботі здійснено огляд сучасних загроз інформаційній сфері діяльності громадян України. Проведено аналіз поточного стану безпеки інформації та шляхи виникнення загроз.

Ключові слова: інформаційна війна, захист, інформаційна безпека, загрози, кібератака.

In this paper were reviewed the current threats to the information sphere of Ukrainian citizens. Also were analyzed the current state of information security and the ways of threats emerged.

Keywords: information war, protection, information security, threats, cyberattack.

У сучасних умовах глобальної інформатизації, інформація є першочерговим та необхідним ресурсом для прийняття рішень з важливих питань у різних сферах діяльності людини. Тому, володіння даними в поєднанні з контролем інформаційного простору, управлінням його потоками та захистом є надзвичайно важливою та серйозною проблемою. Причиною цього є те, що за інформацію, як ресурс, яким можна користуватись та здійснювати вплив на інших, розгортається боротьба на всіх рівнях сучасних суспільних відносин.

Сьогодні виділяють наступні три рівня забезпечення інформаційної безпеки суспільства:

- рівень особи;
- суспільний рівень;
- державний рівень.

Вплив поширення кібератак призвів до виникнення нового методу боротьби – інформаційних війн, до яких на міжнародній арені цифрового простору особливий інтерес. По-перше, це пояснюється високим рівнем глобалізації та “ущільнення” простору існування націй і держав, а по-друге – з бажанням звести до мінімального можливий фізичний вплив, а також з метою запобігання застосуванню військової сили у сучасних міжнародних відносинах, оскільки технологічний розвиток ІТ постійно відкриває нові та

більші можливості по збору, обробці, зберіганню та розповсюдженню інформації, є основним зняряддям кібератак.

Поточний стан національної безпеки нашої держави свідчить, що інформаційні війни, які ведуться проти України призводять до появи наступного ряду загроз:

- військові дії на сході країни здійснюються у супроводі масових кібер та інформаційно-психологічних операцій;
- латентні (приховані, мережеві) заходи противника;
- неправомірні інформаційно-пропагандистські підпільні організації, розташовані в середині країни;
- низький рівень застосування заходів протидії, а саме: більшість внутрішніх загроз виникають на фоні сформованого у радянський період світогляду та успадкованої бюрократичної системи, яка сьогодні не відповідає вимогам сьогодення;
- високий рівень поширення кібератак, і як результат – ріст масштабів кібервійни.

Основною метою інформаційної війни – є послаблення моральної і матеріальної сили противника або ж конкурента, в той же час зміцнивши власні, застосувавши елементи пропагандистського впливу на свідомість людини в сферах її життєдіяльності та розвитку.

На основі аналізу даних сайту StopFake.org, який було засновано у 2014 році з метою перевірки та спростування пропагандистської неправдивої інформації у електронних сервісах, у період з березня 2014 р. по червень 2017 р командою даного сайту було опрацьовано більше 800 новин/повідомлень, які містили фіктивні дані та інформацію про Україну загалом та окремі сфери діяльності зокрема. Усі статті, які вони опрацьовали можна класифікувати на чотири категорії: російські ЗМІ, ЗМІ інших країн, українські ЗМІ, та ЗМІ невизнаних ЛНР та ДНР (див. Рис. 1). Частка російських засобів масової інформації, які поширюють неправдиву інформацію сягає 47 %, що підтверджує значний вплив на суспільство України проросійських ЗМІ. За останніх два роки (2018–2019 роки) команда сайту StopFake.org здійснила аналіз 1101 різних статей (див. рис. 2.).



Рисунок 1 – Розподіл опрацьованих статей за джерелами

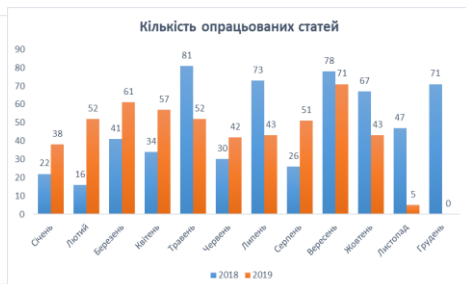


Рисунок 2 – Кількість опрацьованих статей за 2018-2019 року

Результати досліджень дають зрозуміти, що використання засобів масової інформації є важливою зброєю в інформаційній війні, які дають змогу маніпулювати суспільством та розхитувати ситуацію в середині країни, провокуючи там самим виникнення заворушень та протестів. Наслідки таких діянь можуть бути катастрофічні – знищення інфраструктури та падіння економіки країни через припинення роботи підприємств і державних установ. Однак основною зброєю в таких війнах є кібератаки.

Україна веде активну політику щодо протидії інформаційній війні та застосовує жорсткі методи боротьби з кібератаками. Результатами цього є забезпечення належної безпеки громадян, їх захист, блокування неправдивої інформації, що сприяє поширенню достовірних новин про події в державі, а це є основним фактором формування суспільної думки та підтримання безпечних умов життєдіяльності.

На сьогоднішній день для досягнення захисту здійснено багато, зроблено важливі кроки на «світовій шахматній дошці», отримано підтримку світових лідерів та організацій, однак до стану повної безпеки ще далеко. Значка кількість завдань ще повинна бути виконана, комбінації дій ґрунтовно продумані, і тоді результати не заставлять на себе чекати.

Література

1. Фейки, спростовані проектом StopFake в 2014-2017 роках: нарративи та джерела. [Електронний ресурс]. – Режим доступу: <https://www.stopfake.org/uk/fejky-sprostovani-proektom-stopfake-v-2014-2017-rokah-narratyvy-ta-dzherela/>
2. Brzhevska, Z., Dovzhenko, N., Kyrychok, R., Gaidur, G., & Anosov, A. (2019). ІНФОРМАЦІЙНІ ВІЙНИ: ПРОБЛЕМИ, ЗАГРОЗИ ТА ПРОТИДІЯ. Кібербезпека: освіта, наука, техніка, 3(3), 88-96. <https://doi.org/10.28925/2663-4023.2019.3.8896>
3. Горбань Ю. О. Інформаційна війна проти України та засоби її ведення / Ю. О. Горбань // Вісник Національної академії державного управління при Президентові України. – 2015. – № 1. – С. 136-141. – Режим доступу: http://nbuv.gov.ua/UJRN/Vnadu_2015_1_21.
4. Бурак Н.С. Управління проектом підготовки і навчання кіберрятувальника: компетентнісний підхід / Н.С. Бурак, Ю.П. Рак // Вісник Львівського державного університету безпеки життєдіяльності. – Львів, 2013. – №8. – С. 55-60
5. Головатий Р. Р. Управління безпекою на стадії планування проєктів створення об'єктів з масовим перебуванням людей : автореф. дис. канд. техн. наук: 05.13.22; Держ. служба України з надзвичайн. ситуацій, Львів. держ. ун-т безпеки життєдіяльності. Львів, 2018. 24 с.