

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**  
**Київський національний університет**  
**імені Тараса Шевченка**

**I МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА**  
**КОНФЕРЕНЦІЯ**

**“ПРОБЛЕМИ КІБЕРБЕЗПЕКИ ІНФОРМАЦІЙНО-**  
**ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ” (PCSITS)**

**05-06 квітня 2018 року**

**Київ – 2018**

**УДК 621.39:351.861(06)**  
**ББК 32.88:67.401.212.431**  
**П 78**

**Редакційна колегія:** *О.Г. Оксіюк*, д-р. техн. наук, проф., (голова); *В.С. Наконечний*, д-р техн. наук, с.н.с., проф. (заступ. голови); *В.Л. Бурячок*, д-р техн. наук, проф.; *Є.А. Мачуський*, д-р, техн. наук, проф.; *І.Ю. Субач*, д-р техн. наук, доц.; *С.В. Толюпа*, д-р техн. наук, проф.; *О.К. Юдін*, д-р техн. наук, проф.

П78 Проблеми кібербезпеки інформаційно-телекомунікаційних систем: Збірник матеріалів доповіді та тез; м. Київ, 05-06 квітня 2018 року р.; Київський національний університет імені Тараса Шевченка / Редкол.: Оксіюк О.Г. (голова) та ін. – К.: ВПЦ «Київський університет», 2018. – 510с.

Тексти виступів і тез опубліковано в авторській редакції однією з робочих мов конференції: українською, російською, англійською.

**УДК 621.39:351.861(06)**  
**ББК 32.88:67.401.212.431**

Київський національний університет імені Тараса Шевченка,  
2018

## ВСТУП

Завдяки поєднанню досягнень у сфері новітніх інформаційно-комунікаційних технологій (ІКТ) із надбаннями, що постали на базі стрімкого розвитку інформаційно-телекомунікаційних систем (ІТС), сформувалися принципово нові глобальні субстанції — інформаційне суспільство, а також інформаційний та кібернетичний простори, які мають нині практично необмежений потенціал і відіграють провідну роль в економічному та соціальному розвитку кожної країни світу. Однак, поряд з перевагами побудови інформаційного суспільства, збільшуються і ризики, пов'язані з існуванням загроз безпеки інформаційним і телекомунікаційним засобам і системам. Захист інформаційних ресурсів від несанкціонованого доступу, знімання інформації засобами технічних розвідок, забезпечення безпеки інформаційних і телекомунікаційних систем, також є одним з основних національних інтересів в інформаційній сфері. У зв'язку з цим виникає необхідність розробки сучасних методів і систем захисту інформації від різних типів загроз у всіх перерахованих системах. Досить велика кількість засобів і систем захисту інформації створюються на основі математичних моделей, з використанням методів цифрової обробки сигналів а також використовують у своїй роботі інтенсивні логічні обчислення.

У збірнику матеріалів науково-практичної конференції опубліковано тези доповідей вчених, науково-педагогічних працівників, аспірантів, студентів Київського національного університету імені Тараса Шевченка та інших вищих навчальних закладів та організацій України, в яких розглядаються науково-технічні та практичні аспекти створення та використання засобів безпеки інформаційно-телекомунікаційних систем та методи управління інформаційною безпекою таких систем.

**В роботі конференції взяли участь представники:** Київського національного університету імені Тараса Шевченка, Харківського національного університету радіоелектроніки, Одеського національного політехнічного університету, Харківського університету Повітряних Сил імені І. Кожедуба,

Інституту проблем моделювання в енергетиці ім. Г.Є. Пухова  
НАН України, Державного університету телекомунікацій,  
Національного авіаційного університету, Державний науково-  
дослідний інститут спеціального зв'язку та захисту інформації  
України, Харківського Національного Університету  
ім.В.Н.Каразіна, ООО «ІТЦ «Хай-Тек Бюро», Військовий  
інститут телекомунікацій та інформатизації, АТ «Інститут  
інформаційних технологій», Військової частини А0515,  
Національного університету біоресурсів і природокористування  
України, Національного технічного університету України  
«Київський політехнічний інститут імені Ігоря Сікорського»,  
Державної наукової установи Інститут модернізації змісту  
освіти, Державного університету інфраструктури та технологій,  
Дніпропетровського національного університету залізничного  
транспорту імені академіка В. Лазаряна, Інституту проблем  
математичних машин і систем НАН України, Київського  
університету імені Бориса Грінченко, Одеської національної  
академії харчових технологій, Чернівецького національного  
університету ім.Ю.Федьковича, Кавказського університету,  
Міжнародного чорноморського університету, Національного  
університету «Львівська політехніка», Національної академії  
Служби безпеки України, Національної академії внутрішніх  
справ, Східноукраїнського національного університету імені  
В. Даля, та інші

**СЕКЦІЯ 1.**  
**«НАУКОВО-ТЕХНІЧНІ ТА ПРАКТИЧНІ АСПЕКТИ**  
**СТВОРЕННЯ ТА ВИКОРИСТАННЯ ЗАСОБІВ БЕЗПЕКИ**  
**ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ»**

## **РАЦІОНАЛЬНИЙ ВИБІР СТЕПЕНІ ПІДСТАНОВОК ШИФРУ БАГАТОАЛФАВІТНОЇ ЗАМІНИ ТА ДЖЕРЕЛА РІВНОМІРНО РОЗПОДІЛЕНОЇ ВИПАДКОВОЇ ПОСЛІДОВНОСТІ**

У сучасному світі спостерігається постійне зростання сфер застосування системах управління технологічними процесами (СУТП), починаючи з енергетики, зв'язку, повітряного та залізничного транспорту й завершуючи високотехнологічними галузями економіки країн світу, як металургійні та хімічні виробництва тощо. Використання у якості транспортної мережі в СУТП глобальної мережі Інтернет підвищує ризики порушення їх гарантоздатності, що включає, зокрема, потенціал виконання визначених завдань, уникаючи можливості непередбачуваних змін системи та послуг, що надаються (властивість цілісності, інакше - імітостійкості), а також неавторизованого доступу до інформації про послуги (властивість конфіденційності) [1].

В роботі [2] запропоновано швидкий алгоритм реалізації шифру багатоалфавітної заміни з використанням шифрувальної послідовності від блокового шифру в режимі OFB, доведено коректність відповідної процедури та можливість формування будь-якої підстановки з симетричної групи підстановок  $S_n$ . Проведено імітаційне моделювання алгоритму, що дозволило підтвердити необхідні статистичні якості матриці перехідних ймовірностей шифру, який забезпечить високий рівень стійкості шифрування та імітостійкості команд і службової інформації, що циркулює в СУТП. В роботі Зубова А.Ю. [3] отримані фундаментальні результати в плані оцінки імітостійкості,

зокрема, доведено, що для будь-якого шифру для ймовірності  $p_n$  підміни повідомлення в каналі зв'язку справедлива нерівність:

$$p_n \geq \frac{|\mathcal{M}|-1}{|\mathcal{C}|-1}, \quad (1)$$

де  $|\mathcal{M}|$  - потужність множини припустимих відкритих повідомлень,  $|\mathcal{C}|$  - потужність множини шифрованих повідомлень.

Посилив вимогу щодо криптографічної стійкості шифру, оцінку (1) можливо посилити, для цього доведемо наступну лему.

**Лема.** В випадку практичної криптографічної стійкості шифру та джерела повідомлень без пам'яті для ймовірності  $p_n$  підміни шифрованого повідомлення в каналі зв'язку справедлива нерівність:

$$p_n \geq 2^{-(1-H_0)L}, \quad (2)$$

де  $H_0 = -p_0 \log_2 p_0 - p_1 \log_2 p_1$  - бітова ентропія відкритого повідомлення, величина  $L$  є довжиною відкритих та шифрованих повідомлень.

Слід зазначити, що для інформаційного обміну в рамках СУТП, за звичай, характерний високий ступінь формалізації повідомлень, які переважно мають деяку фіксовану довжину, тому обмеження щодо довжини можна вважати припустимим.

По-перше, звернемо увагу, що і теоретично, і практично стійкі шифри забезпечують розподіл ймовірностей знаків шифрованого тексту, який не відрізняється від випадкового та рівномірно. Тому потужність шифрованих текстів  $|\mathcal{C}|$  дорівнює величині  $2^L$ .

Оскільки, виконані умови другої теореми Шеннона [18], то для  $|\mathcal{M}|$  потужності множини припустимих відкритих повідомлень справедлива оцінка:

$$|\mathcal{M}| = 2^{H_0 L}.$$

Далі скористаємось нерівністю (1) і отримаємо:

$$p_n \geq \frac{|\mathcal{M}|-1}{|\mathcal{C}|-1} = \frac{2^{H_0 L}-1}{2^L-1} \approx 2^{-(1-H_0)L}, \text{ для достатньо великих } L, \text{ що і було потрібно довести.}$$

Слід відмітити, що імітостійкість шифру можливо характеризувати за допомогою складності  $C_n$  підробки зловмисником повідомлення, яку можна оцінити наступним чином. Нехай, за допомогою шифру багатоалфавітної заміни с ключем  $K$  легальним користувачем системи було зашифроване та передане в канал зв'язку деяке істинне повідомлення  $M = (m_1, m_2, \dots, m_l)$  із множини припустимих відкритих повідомлень:  $M \in \mathcal{M}$ :

$$C = E_K(M).$$

Зловмисник, який перехопив шифротекст  $C = (c_1, c_2, \dots, c_l)$ , намагається провести атаку з відомим відкритим повідомленням для нав'язування фіктивного повідомлення  $\tilde{M} = (\tilde{m}_1, \tilde{m}_2, \dots, \tilde{m}_l)$ . Вважаємо, що дані  $M$  та  $\tilde{M}$  відрізняються лише на  $r$  місцях, тобто маємо:

$$|\{i: m_i \neq \tilde{m}_i\}| = r$$

Тоді зловмисник на  $(l - r)$  місцях співпадаючих знаків  $m_i = \tilde{m}_i$  використовує відомі йому символи шифротексту, оскільки:

$$E_K(m_i) = E_K(\tilde{m}_i) = \left( \dots \begin{matrix} m_i \\ c_i \end{matrix} \dots \right).$$

На інших місцях він буде вимушений обирати один з невідомих  $(n - 1)$  варіантів переходів навмання, а загальна кількість варіантів підбору шифротексту  $\tilde{C}$ , який після розшифрування буде сприйнятий як  $\tilde{M} = E_K^{-1}(\tilde{C})$ , становить величину:

$$C_n = (n - 1)^r.$$

Звідси отримуємо ймовірність вгадування зловмисником  $r$  символів з першого разу, яка може слугувати оцінкою для рівня імітостійкості шифру багатоалфавітної заміни:

$$q_r = (n - 1)^{-r}. \quad (3)$$

Тобто, складність задачі підробки повідомлень, які зашифровані за допомогою багатоалфавітної заміни зростає залежно від кількості символів, що підробляються, за експоненціальним законом (відповідно, зменшується ймовірність правильного угадування).

Загалом оцінка, нерівність, а також рівняння (2-3) дозволяють раціонально обрати величину степені підстановок. Зважаючи на необхідність врахування вимоги що зручності

застосування запропонованої методики у вигляді програмних реалізацій доцільно обирати значення степені підстановки такі, що узгоджуються з форматами даних у мікропроцесорах, а саме:  $n = 2^m$ , де  $m = 2,4,8$  (зауважимо, що для  $m = 1$  шифр багатоалфавітної заміни перетворюється у звичайний шифр гамування по mod 2).

В таблиці 1 наведені характеристики методики генерації послідовності підстановок для випадків  $n = 4,16,256$ .

№ №	Характеристики методики		Степінь підстановки		
			4	16	256
1.	$q_1$	Імовірність вгадування 1 символу	0.333	0.067	0.008
2.	$N$	Стійкість при повторі ключа	2	8	128
3.	$S$	Швидкодія порівняно з МБН (%)	138.6	277.2	554.5
4.	$V$	Обсяг двійкової РРВП для генерації однієї підстановки (біт)	8	64	4096

**Табл. 1. Розрахункові характеристики розробленої методики генерації підстановок**

На підставі аналізу таблиці можливо відмітити, що характеристики імітостійкості та криптографічної стійкості при повторі ключа для  $n = 2^2$  є найгіршими, а у випадку  $n = 2^8 = 256$  найкращими. Але останній варіант внаслідок занадто великого обсягу вихідної РРВП призведе до суттєвого уповільнення процесу шифрування порівняно з іншими варіантами. Тому для практичного застосування пропонується обирати степінь підстановок  $n = 2^4 = 16$ .

## Література:

1. Гулак Г.М. Формування вимог щодо забезпечення гарантоздатності автоматизованих систем переробки інформації й управління критично-важливими об'єктами інфраструктури. / Гулак Г.М., Складанний П.М. // II Всеукраїнська науково-практична конференція «Кібербезпека в Україні: правові та організаційні питання» (Одеса, 17 листопада 2017р.). – Одеса: ОДУВС, 2017 – С.12-14.

2. Гулак Г. М. Швидкий алгоритм генерації підстановок багатоалфавітної заміни / Г. М. Гулак, В. Л. Бурячок, П. М. Складанний // Захист інформації. – 2017. – №2. – С. 173–177.

3. Зубов А.Ю. Криптографические методы защиты информации. Совершенные шифры: Учебное пособие. – М.: Гелиос АРВ, 2005, - 160 с.

4. Духин А.А. Теория информации: Учебное пособие. – М.; Гелиос АРВ, 2007. -248с., ил. ISBN 978-5-85438-168-0

УДК 004.056.5:004.75

**Т.А.Радівілова<sup>1</sup>, М.Х. Тавалбех<sup>1</sup>**

*<sup>1</sup>Харківський національний університет радіоелектроніки  
tamara.radivilova@gmail.com  
tavalbeh@icloud.com*

## **СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ ПРИ НАЯВНОСТІ САМОПОДІБНИХ ВЛАСТИВОСТЕЙ ВХІДНОГО ТРАФІКУ**

Виявлення вторгнень (атак) - це процес моніторингу подій, що відбуваються в комп'ютерній системі або мережі з метою пошуку ознак можливих інцидентів. Мережеві системи виявлення та запобігання вторгнень (NIDS/NIPS, Network Intrusion detection system/Network Intrusion prevention system) це необхідний елемент захисту від мережевих атак. Найбільш часто використовується розподілена архітектура, в якій кожен датчик NIDS аналізує отриманий трафік на наявність незаконних мережевих дій і, при необхідності, генерує попередження. Вузким місцем, що впливає на продуктивність мережі, є швидкість обробки вхідних даних мережевим пристроєм безпеки.

## ЗМІСТ

<b>СЕКЦІЯ 1.</b> <b>«НАУКОВО-ТЕХНІЧНІ ТА ПРАКТИЧНІ АСПЕКТИ</b> <b>СТВОРЕННЯ ТА ВИКОРИСТАННЯ ЗАСОБІВ БЕЗПЕКИ</b> <b>ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ».</b>		
<b>1.</b>	<i>О.В. Лемешко, О.С. Єременко, А.В. Персіков</i> МАТЕМАТИЧНА МОДЕЛЬ РОЗРАХУНКУ МАКСИМАЛЬНОЇ КІЛЬКОСТІ ШЛЯХІВ, ЩО НЕ ПЕРЕТИНАЮТЬСЯ, ПРИ БЕЗПЕЧНІЙ МАРШРУТИЗАЦІЇ	<b>6</b>
<b>2.</b>	<i>С.М. Білан, О.І. Левчук, М.М. Галушко</i> ДОСЛІДЖЕННЯ ВПЛИВУ ДОДАТКОВОЇ ДІЇ НА ЯКІСТЬ ГЕНЕРАТОРІВ ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ НА ОСНОВІ КЛІТИННИХ АВТОМАТІВ	<b>10</b>
<b>3.</b>	<i>Е.Д. Годун, Д.О. Капшученко, Д.А. Остапец</i> БИОМЕТРИЯ ЛИЦА В СИСТЕМАХ УЧЕТА РАБОЧЕГО ВРЕМЕНИ	<b>14</b>
<b>4.</b>	<i>О.О. Кузнецов, А.С. Кіян, Т.Ю. Кузнецова</i> ЦИФРОВИЙ ПІДПИС НА АЛГЕБРАІЧНИХ КОДАХ ДЛЯ ПОСТ-КВАНТОВОГО ЗАСТОСУВАННЯ	<b>18</b>
<b>5.</b>	<i>V. Chaikovska, A. Oksiuk</i> ANALYSIS AND PROTECTION METHODS OF THE AUTHENTICATION INTO THE CLOUD TECHNOLOGIES	<b>22</b>
<b>6.</b>	<i>Ю.В. Ковальова, Т.В. Бабенко</i> АНАЛІЗ ВРАЗЛИВОСТЕЙ ІНТЕЛЕКТУАЛЬНИХ ЛІЧИЛЬНИКІВ В БЕЗДРОТОВІЙ МЕРЕЖІ МОНІТОРИНГУ ЕНЕРГОРЕСУРСІВ	<b>24</b>
<b>7.</b>	<i>Г.М. Гулак, П.М. Складанний</i> РАЦІОНАЛЬНИЙ ВИБІР СТЕПЕНІ ПІДСТАНОВОК ШИФРУ БАГАТОАЛФАВІТНОЇ ЗАМІНИ ТА ДЖЕРЕЛА РІВНОМІРНО РОЗПОДІЛЕНОЇ ВИПАДКОВОЇ ПОСЛІДОВНОСТІ	<b>27</b>
<b>8.</b>	<i>Т.А. Радівілова, М.Х. Тавалбех</i> СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ ПРИ НАЯВНОСТІ САМОПОДІБНИХ ВЛАСТИВОСТЕЙ ВХІДНОГО ТРАФІКУ	<b>31</b>

9.	<i>Г.В. Берестовенко, О.Р. Погіба, С.В. Толюпа</i> АНАЛІЗ БЕЗПЕКИ ХМАРНИХ ОБЧИСЛЕНЬ	35
10.	<i>О.И. Ковтун, О.А. Лещенко</i> ИССЛЕДОВАНИЕ ТЕХНОЛОГИИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ	37
11.	<i>В.М. Бурлаков, В.Г. Кононович, І.В. Кононович</i> ЯКА КІБЕРБЕЗПЕКА ПОТРІБНА ДЛЯ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ ЗАГАЛЬНОГО КОРИСТУВАННЯ?	41
12.	<i>К.Ю.Шеханін, А.О.Колгатін, Є.Є.Деменко, О.О.Кузнецов</i> УДОСКОНАЛЕНИЙ МЕТОД ПРИХОВУВАННЯ ДАНИХ У СТРУКТУРУ ФАЙЛОВОЇ СИСТЕМИ СІМЕЙСТВА FAT	45
13.	<i>О.О.Кузнецов, В.О.Фроленко, Д.В.Іваненко, Е.С.Єрьомін</i> ПОРІВНЯЛЬНІ ДОСЛІДЖЕННЯ КРОСПЛАТФОРМНИХ РЕАЛІЗАЦІЙ ПОТОКОВИХ СИМЕТРИЧНИХ ШИФРІВ	49
14.	<i>О.О. Кузнецов, А.С. Кіян, М.С. Луценко</i> ДОСЛІДЖЕННЯ І ПОРІВНЯЛЬНИЙ АНАЛІЗ КОДОВИХ СХЕМ ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ З NIST PQC	53
15.	<i>М.С. Луценко, А.С. Кіян, Т.Ю. Кузнецова, А.А. Кузнецов</i> АНАЛИЗ И СРАВНИТЕЛЬНЫЕ ИССЛЕДОВАНИЯ КОДОВЫХ СХЕМ ИНКАПСУЛЯЦИИ КЛЮЧЕЙ, ПРЕДСТАВЛЕННЫХ НА КОНКУРС NIST PQC	57
16.	<i>В.С. Наконечний, В.Г. Сайко, С.Ю. Даков</i> АНАЛІЗ ПРОБЛЕМ ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ В МЕРЕЖАХ НОВОГО ПОКОЛІННЯ	61
17.	<i>І.В. Пислар, В.В. Браїловський, М.Г. Рождественська, М.М. Іванчук</i> ОПТИЧНА ІНФОРМАЦІЙНА СИСТЕМА З ЕЛЕМЕНТАМИ МАСКУВАННЯ	65
18.	<i>В.В. Ліпінський, Ю. В. Мякухін, В.С. Наконечний, Я.В. Шестак</i> МЕТОД ВИБОРУ СКЛАДУ ПЕРИМЕТРОВИХ ВОЛОКОННО-ОПТИЧНИХ ТЕХНІЧНИХ ЗАСОБІВ ОХОРОНИ ДЛЯ ОСОБЛИВО ВАЖЛИВИХ ОБ'ЄКТІВ ЕНЕРГЕТИКИ	69

<b>19.</b>	<i>А.А. Кобозева, И.И. Бобок, Л.Е.М. Батиене, К.Р. Шерфединов</i> РАСШИРЕНИЕ ОБЛАСТИ ПРИМЕНИМОСТИ СТЕГАНОГРАФИЧЕСКОГО АЛГОРИТМА, УСТОЙЧИВОГО К АТАКАМ ПРОТИВ ВСТРОЕННОГО СООБЩЕНИЯ	<b>72</b>
<b>20.</b>	<i>О.В. Труш, О.О. Лещенко</i> КРИТЕРІЇ ОЦІНКИ ЕФЕКТИВНОСТІ БЕЗПРОВІДНИХ СЕНСОРНИХ МЕРЕЖ	<b>76</b>
<b>21.</b>	<i>S.V. Toliura, O.A Uspenskyi</i> SIGNATURE AND STATISTICAL ANALYZERS IN THE CYBER ATTACK DETECTION SYSTEM	<b>80</b>
<b>22.</b>	<i>П.О. Тадеєв</i> ІТ КЛАСТЕР ЯК ЕФЕКТИВНЕ СЕРЕДОВИЩЕ ДЛЯ РЕАЛІЗАЦІЇ ОСВІТНІХ ПРОГРАМ	<b>84</b>
<b>23.</b>	<i>Є.А. Сірий, А.О. Барліт, В.С. Наконечний</i> ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗАХИСТУ ОБ'ЄКТІВ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ СУЧАСНИМИ ЗАСОБАМИ КОНТРОЛЮ ДОСТУПУ	<b>88</b>
<b>24.</b>	<i>М. Iavich, A. Gagnidze, G. Iashvili</i> QUANTUM OTP	<b>92</b>
<b>25.</b>	<i>A. Gagnidze, M. Iavich, G. Iashvili</i> KEY EXCHANGE PROTOCOL	<b>94</b>
<b>26.</b>	<i>І.Д.Горбенко, О.О.Кузнецов, Ю.І.Горбенко,В.А. Тимченко</i> МАТЕМАТИЧНА СТРУКТУРА ПОТОКОВОГО ШИФРУ «СТРУМОК»	<b>96</b>
<b>27.</b>	<i>В.В. Коваль, О.В. Самков, Д.О. Кальян, В.Г. Дубович-Костецький</i> ЗАСОБИ АВТОМАТИЗОВАНОГО ПОЛІКАНАЛЬНОГО МОНІТОРИНГУ СИНХРОСИГНАЛІВ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ	<b>100</b>
<b>28.</b>	<i>О.В.Думітраш, Г.В.Берестовенко</i> ПРОГРАМНИЙ КОМПЛЕКС КРИПТОГРАФІЧНО ЗАХИЩЕНОГО ОБМІНУ МИТТЄВИМИ ПОВІДОМЛЕННЯМИ З ВИКОРИСТАННЯМ БІБЛІОТЕКИ MIRACLE	<b>104</b>

29.	<i>Є.В.Редзюк</i> ВИЗНАЧЕННЯ ФІЗИЧНОЇ ЦІЛІСНОСТІ ОБ'ЄКТА КОНТРОЛЮ	108
30.	<i>А.О.Зарубенко</i> ЗАБЕЗПЕЧЕННЯ ВИМОГ ДО СИСТЕМИ ЗВ'ЯЗКУ ШЛЯХОМ ЗМІНИ КОНСТРУКТИВУ АНТЕНИ СУПУТНИКОВОГО ЗВ'ЯЗКУ	112
31.	<i>І.А. Сорокін, С.С. Штаненко, Г.В. Берестовенко</i> МОДУЛЬ ЗАХИСТУ ПРОГРАМНОГО ЗАПЕЧЕННЯ ВІД НЕСАНКЦІОНОВАНОГО КОПІЮВАННЯ	116
32.	<i>О.В. Залужний, С.С. Штаненко, Г.В. Берестовенко</i> МЕТОД ВИБОРУ ДОВЖИНИ КОДОВОГО СЛОВА ДЛЯ СИСТЕМ РАДІОЗВ'ЯЗКУ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ З ВІДКЛАДЕНИМ ПІДТВЕРДЖЕННЯМ	120
33.	<i>В.В. Гречко, Т.В. Бабенко</i> ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ НАДІЙНОСТІ КЛЮЧІВ СЕАНСУ ОБМІНУ ІНФОРМАЦІЄЮ	123
34.	<i>А. Romanova, S.V. Toliupa</i> PERSPECTIVE STEGANOGRAPHY: OVERVIEW OF THE METHODS AND THEIR IMPLEMETATION	126
35.	<i>Є.О. Агапова, С.В. Толюпа</i> АНАЛІЗ ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ	130
36.	<i>К. Алексеева, Є.О. Толюпа</i> АНАЛИЗ НЕДОСТАТКОВ СОВРЕМЕННЫХ СИСТЕМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ	133
37.	<i>V. Dmtruk, S.V. Toliupa</i> INSIDERS IN CYBER SECURITY: THEORETICAL AND PRACTICAL ASPECTS OF INFORMATION PROTECTION FROM INTERNAL THREATS	137
38.	<i>А.С. Зінченко, М.М.Браїловський</i> АНАЛІЗ ТА МОДЕЛЮВАННЯ ЗАГРОЗ ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ МІЖМЕРЕЖЕВОЇ ВЗАЄМОДІЇ НА ПРИКЛАДІ DDOS АТАК	142
39.	<i>В.Г. Сайко, В.С. Наконечний</i> МЕТОДИКА ЕНЕРГЕТИЧНОГО РОЗРАХУНКУ ЗАХИЩЕНИХ РАДІОЛІНІЙ ТЕРАГЕРЦОВОГО ДІАПАЗОНУ ДЛЯ МОБІЛЬНИХ МЕРЕЖ 5 G	144

<b>40.</b>	<i>А.В. Ахмаметьева</i> СТЕГАНОАНАЛИЗ ЦИФРОВЫХ ИЗОБРАЖЕНИЙ В УСЛОВИЯХ ПОГРУЖЕНИЯ ДОПОЛНИТЕЛЬНОЙ ИНФОРМАЦИИ В ОБЛАСТЬ ДКП	<b>148</b>
<b>41.</b>	<i>А.С. Сторіжко, І.І. Пархоменко</i> АНАЛІЗ ЗАГРОЗ ТА СПОСОБИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ДАНИХ ПРИ ВИКОРИСТАННІ ХМАРНИХ ТЕХНОЛОГІЙ	<b>151</b>
<b>42.</b>	<i>Г.К. Папірна, А.О. Фесенко</i> СУЧАСНІ ПІДХОДИ ДО ОЦІНКИ ЗАХИЩЕНОСТІ СИСТЕМ	<b>155</b>
<b>43.</b>	<i>Д.О.Третьяк, М.М.Брайловський, Я.В.Шестак</i> АНАЛІЗ ЗАГРОЗ І ВРАЗЛИВОСТЕЙ ТА СПОСОБИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ДАНИХ У ВЕБ-ДОДАТКАХ	<b>159</b>
<b>44.</b>	<i>М.К. Жердєв, В.В. Кузавков, В.О. Данько</i> СХЕМА АВТЕНТИФІКАЦІЇ ПОВІДОМЛЕНЬ КАНАЛЬНОГО РІВНЯ	<b>162</b>
<b>45.</b>	<i>М.И. Огурцов</i> РАЗРАБОТКА ПРОТОКОЛА ЗАЩИЩЕННОГО ОБМЕНА ДАННЫМИ ДЛЯ СЕТЕЙ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ	<b>166</b>
<b>46.</b>	<i>Н.В. Мордвинцев, И.В. Терещенко, А.И. Терещенко</i> ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ РОБАСТНОГО ПРОЕКТИРОВАНИЯ ДЛЯ ДОСТИЖЕНИЯ БЕЗОПАСНОСТИ ПРОДУКЦИИ	<b>170</b>
<b>47.</b>	<i>М.С. Стремецька, А.Б. Качинський</i> СУЧАСНІ ЗАСОБИ ЗАХИСТУ ПЛАТІЖНИХ СИСТЕМ ЩОДО ОБСЛУГОВУВАННЯ КРИТИЧНИХ СЕРВІСІВ ДЕРЖАВИ	<b>174</b>
<b>48.</b>	<i>І.А. Терейковський, М.Є. Кривомаз</i> ДИНАМІЧНА КОМПІЛЯЦІЯ PYTHON-ПРОГРАМ В ЗАДАЧАХ ЗАХИСТУ ІНФОРМАЦІЇ	<b>178</b>
<b>49.</b>	<i>К. Aliksieieva, S.V. Toliupa</i> IMPROVEMENT OF THE EFFECTIVENESS OF INCIDENTS MANAGEMENT USING INTELLIGENCE TECHNOLOGY	<b>181</b>

50.	<i>К.О. Трифонова</i> PERLIN NOISE FORGERY DETECTION OF DIGITAL IMAGE	187
51.	<i>М.М. Климаш, О.М. Шпур, Н.В. Пелех</i> МОДЕЛЬ КЛАСТЕРИЗАЦІЇ ХМАРНИХ ДАТА-ЦЕНТРІВ В УМОВАХ ПЕРЕДАЧІ ТА ЗАХИСТУ ПОТОКІВ BIG DATA	191
52.	<i>Б.М. Стрихалюк, О.М.Шпур, Ю.В.Климаш</i> МЕТОД ОПТИМІЗАЦІЇ МАРШРУТИЗАЦІЇ ІНФОРМАЦІЙНИХ ПОТОКІВ ДЛЯ УДОСКОНАЛЕННЯ ЗАСОБІВ БЕЗПЕКИ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ	197
53.	<i>М.І.Бешлей, М.М.Климаш, О.М.Панченко, Г.В.Бешлей</i> РОЗРОБЛЕННЯ СИСТЕМИ МОНІТОРИНГУ ТА АНАЛІЗУ ТРАФІКУ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ ДЛЯ ВИЯВЛЕННЯ АНОМАЛІЇ І ЗАПОБІГАННЯ АТАК	201
54.	<i>Д.С. Дженджеро, С.В. Толюпа</i> ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ФІЗИЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ	205
55.	<i>А.С. Руденко, А.О.Фесенко</i> СПОСОБИ ЗАХИСТУ РЕСУРСІВ ТА КАНАЛІВ РОЗПОДІЛЕНИХ КОРПОРАТИВНИХ МЕРЕЖ	207
56.	<i>Т. Максимюк, О. Петренко, М. Климаш</i> МЕТОД ПЕРЕДАВАННЯ СИГНАЛІВ ІЗ ЗАХИСТОМ ВІД ПРОСЛУХОВУВАННЯ ДЛЯ СИСТЕМ РАДІОЗВ'ЯЗКУ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ	211
57.	<i>В.С. Наконечний, С.Ю. Даков, Д.О. Жир, О.О. Козак</i> ПРОБЛЕМА НАДІЙНОСТІ ТА ЗАХИСТУ ТЕХНОЛОГІЙ MACHINE-TO-MACHINE M2M	216
58.	<i>В.В. Бараннік, В.В.Бараннік, Д.В.Бараннік, О.М.Шатун</i> МЕТОД НЕПРЯМОГО СТЕГANOГРАФІЧНОГО ВБУДОВУВАННЯ ДАНИХ В ЗОБРАЖЕННЯ З УРАХУВАННЯМ ІНФОРМАЦІЇ КОНТУРУ	220
59.	<i>В.В.Бараннік, Т.В.Белікова, О.В.Довбенко, С.О. Сідченко</i> ВИЯВЛЕННЯ ПРИХОВАНИХ ІНФОРМАЦІЙНИХ ВПЛИВІВ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНОМУ ПРОСТОРИ	223

<b>60.</b>	<i>Т.В. Мелешко, В.А. Швець, М.Ю. Магас</i> ПРИСТРІЙ ДЛЯ ВИЗНАЧЕННЯ НОРМ ЗАХИСТУ КОНФЕДИЦІАЛЬНОЇ ІНФОРМАЦІЇ ВІД ЛАЗЕРНИХ СИСТЕМ РОЗВІДКИ	<b>227</b>
<b>61.</b>	<i>А.О. Фесенко, В.А. Швець, В.О. Фесенко</i> ФОРМУВАННЯ ФАЗОВИХ ТЕКСТУРНИХ ОЗНАК РАЙДУЖНОЇ ОБОЛОНКИ ОКА НА БАЗІ DOG-ФІЛЬТРА	<b>231</b>
<b>62.</b>	<i>І.Ю. Субач, В.В. Фесьоха</i> УДОСКОНАЛЕННЯ СИСТЕМ ВИЯВЛЕННЯ КІБЕРНЕТИЧНИХ АТАК ВІДКРИТИХ НА ОСНОВІ ЗАГАЛЬНОДОСТУПНИХ ЛІЦЕНЗІЙ	<b>235</b>
<b>63.</b>	<i>Л.О. Сліпачук</i> ОРГАНІЗАЦІЙНО-ТЕХНІЧНІ АСПЕКТИ ЗАХИСТУ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ У КОНТЕКСТІ «СИСТЕМИ НАЦІОНАЛЬНОЇ КІБЕРБЕЗПЕКИ»	<b>239</b>
<b>64.</b>	<i>V.E. Chevardin, I.V. Samoilo, A.S. Shevchenko, O.V. Marchuk.</i> BRIEF REVIEW OF THE NETWORK SECURITY TESTING METHODS	<b>244</b>
<b>65.</b>	<i>С.Б. Гордієнко, О.О. Манько, О.М. Скубак,</i> ЗАХИСТ ЛІНІЙНИХ СПОРУД ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ	<b>249</b>
<b>66.</b>	<i>В.Г. Сайко, В.С. Наконечний</i> АНАЛІЗ ОСОБЛИВОСТЕЙ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В БЕЗДРОТОВИХ САМООРГАНІЗУЮЧИХ МЕРЕЖАХ 5- ГО ПОКОЛІННЯ	<b>252</b>
<b>67.</b>	<i>М. Явич, Г. Иашивили</i> ВЗАИМОДЕЙСТВИЯ ЧЕЛОВЕКА С КОМПЬЮТЕРОМ И КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ	<b>256</b>
<b>68.</b>	<i>Д.Д. Вергелес, Г.П. Леоненко</i> РОЗРОБКА СУЧАСНОЇ СТРУКТУРИ МЕРЕЖІ ДЛЯ ПОТРЕБ УРЯДОВОГО ЗВ'ЯЗКУ	<b>259</b>

<b>СЕКЦІЯ 2. “МЕТОДИ, ЗАСОБИ ТА ЗАХОДИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ</b>		
<b>1.</b>	<i>Л.В. Кузьменко, В.Л. Бурячок</i> ТЕНДЕНЦІЇ РОЗВИТКУ ТА ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ СУЧАСНИХ ІОТ- ПРИСТРОЇВ	<b>264</b>
<b>2.</b>	<i>Д.В. Палко, Л.В. Мирутенко, В.І. Вялкова</i> ЗАХИСТ ІНФОРМАЦІЙНИХ РЕСУРСІВ ТА ТРАНЗАКЦІЙ В КОРПОРАТИВНИХ МЕРЕЖАХ	<b>268</b>
<b>3.</b>	<i>В.М. Місько</i> ПРИСКОРЕННЯ МЕТОДУ КВАДРАТИЧНОГО РЕШЕТА НА ОСНОВІ РІШЕННЯ МАТРИЦІ НА ХОДУ	<b>272</b>
<b>4.</b>	<i>А.В. Собчук, Ю.В. Кравченко,</i> ПРОБЛЕМИ ВПРОВАДЖЕННЯ ТА ЗАСТОСУВАННЯ DLR СИСТЕМ, ЯК ЗАСОБУ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В КОМПАНІЇ	<b>274</b>
<b>5.</b>	<i>О.В. Дашковська, В.П. Погребняк, А.К. Солоденко</i> ЗАКОН УКРАЇНИ «ПРО ВИЩУ ОСВІТУ»: ПІДСУМКИ ІМПЛЕМЕНТАЦІЇ	<b>277</b>
<b>6.</b>	<i>М.С. Труш, А.М. Валенок</i> ВИКОРИСТАННЯ ТЕХНОЛОГІЙ PR ТА РЕКЛАМИ В УПРАВЛІННІ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НАЦІОНАЛЬНИХ ПІДПРИЄМСТВ	<b>281</b>
<b>7.</b>	<i>М.О. Євдокименко, М. Ельсаєд</i> МЕТОДИКА РОЗРАХУНКУ ІНТЕГРАЛЬНИХ ПОКАЗНИКІВ БЕЗПЕКИ ІНФОКОМУНІКАЦІЙНОЇ МЕРЕЖІ	<b>285</b>
<b>8.</b>	<i>О.В. Соснін, В.В. Повидиш</i> ПРО ВИТОКИ ПРОБЛЕМ ІНФОРМАЦІЙНО- КОМУНІКАЦІЙНОЇ БЕЗПЕКИ В СУСПІЛЬСТВІ	<b>289</b>
<b>9.</b>	<i>В.О. Бородуля, Т.В. Бабенко</i> СИНТЕЗ МОДЕЛЕЙ ІДЕНТИФІКАЦІЇ МЕРЕЖЕВИХ АНОМАЛІЙ	<b>293</b>

<b>10.</b>	<i>Л.Ф. Політанський, С.Д. Галюк</i> ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ВИКОРИСТАННЯ НЕЛІНІЙНОЇ ДИНАМІКИ В ІНФОКОМУНІКАЦІЯХ	<b>295</b>
<b>11.</b>	<i>А.М. Соболев, Д.В. Ланде</i> АНАЛІЗ КРИТИЧНОСТІ ВУЗЛІВ У КВАЗІПСЕРАРХІЧНИХ МЕРЕЖАХ СОЦІАЛЬНОГО ХАРАКТЕРУ	<b>299</b>
<b>12.</b>	<i>Д.Ю. Хлапонін</i> ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ КІБЕРФІЗИЧНИХ СИСТЕМ В УКРАЇНІ	<b>302</b>
<b>13.</b>	<i>М.М. Браїловський, Ю.Я. Самохвалов, В.С. Орленко</i> ВИКОРИСТАННЯ ІНФОРМАЦІЙНОГО ВПЛИВУ В ЯКОСТІ СКЛАДОВОЇ ПРОЦЕСУ УПРАВЛІННЯ СКЛАДНИМИ СИСТЕМАМИ	<b>307</b>
<b>14.</b>	<i>О.В. Рибальський, В.В. Журавель, В.І.С оловійов, Л.М. Тимошенко</i> ПОБУДОВА ВІТЧИЗНЯНОЇ ІНСТРУМЕНТАЛЬНОЇ СИСТЕМИ ДЛЯ ПРОВЕДЕННЯ ЕКСПЕРТИЗИ АУДІОЗАПИСУ	<b>311</b>
<b>15.</b>	<i>Ю.В. Мяхухин, В.С. Наконечный, А.Г. Оксюк</i> ВЕРОЯТНОСТЬ ПРОПУСКАНИЯ КИБЕРАТАКИ МЕХАНИЗМОМ ЗАЩИТЫ	<b>315</b>
<b>16.</b>	<i>О.А. Курченко, Ю.М. Щебланін</i> ДЕЯКІ ПИТАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ХМАРАХ	<b>318</b>
<b>17.</b>	<i>В.А. Савченко</i> ПРОБЛЕМА ФОРМУВАННЯ ІННОВАЦІЙНОГО ЗМІСТУ НАВЧАННЯ ЗА СПЕЦІАЛЬНІСТЮ 125 КІБЕРБЕЗПЕКА	<b>321</b>
<b>18.</b>	<i>І.Д. Боков, І.В. Бондар</i> УПРАВЛІННЯ ОРГАНІЗАЦІЙНОЮ ПОВЕДІНКОЮ І КУЛЬТУРОЮ НА ПІДПРИЄМСТВІ В СФЕРІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ	<b>324</b>
<b>19.</b>	<i>Є.О. Толюпа</i> ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ CISCO MARS В СИСТЕМІ ПРОТИДІЇ ВИЯВЛЕННЯ, УПРАВЛІННЯ І ВІДДЗЕРКАЛЕННЯ ЗАГРОЗ КІБЕРБЕЗПЕКИ	<b>328</b>

<b>20.</b>	<i>С.В. Толюпа, Н.В. Лукова-Чуйко</i> НЕДОЛІКИ ТА ПЕРЕВАГИ СИСТЕМ ВИЯВЛЕННЯ МЕРЕЖЕВИХ ВТОРГНЕНЬ І ОЗНАК КІБЕРАТАК НА ОСНОВІ СИГНАТУРНОГО АНАЛІЗУ	<b>332</b>
<b>21.</b>	<i>Р. В. Огієвич, О.Г. Оксіюк</i> ПЕРСПЕКТИВИ ДЕЦЕНТРАЛІЗОВАНИХ СИСТЕМ НА ОСНОВІ БЛОКЧЕЙН ТЕХНОЛОГІЙ. СХОВИЩЕ ДАНИХ З ВИКОРИСТАННЯМ БЛОКЧЕЙНУ	<b>340</b>
<b>22.</b>	<i>М.В. Плєскач</i> КІБЕРБЕЗПЕКА ЛЮДИНИ ЯК ВАЖЛИВА СКЛАДОВА КІБЕРБЕЗПЕКИ	<b>346</b>
<b>23.</b>	<i>О.Р. Черняк,</i> ОСНОВНІ ТЕНДЕНЦІЇ У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ	<b>349</b>
<b>24.</b>	<i>В.М. Домрачев, В.В. Третиник</i> МОДЕЛЮВАННЯ БАНКІВСЬКИХ РИЗИКІВ В УКРАЇНІ	<b>354</b>
<b>25.</b>	<i>С.І. Рабченюк, В.С.Наконечний</i> ДЕРЖАВНЕ УПРАВЛІННЯ У СФЕРІ КІБЕРБЕЗПЕКИ УКРАЇНИ	<b>355</b>
<b>26.</b>	<i>Д.О.Кирилюк, М.М. Браїловський</i> ЗАСТОСУВАННЯ ВІРТУАЛЬНИХ ПРИВАТНИХ МЕРЕЖ ДЛЯ ЗАБЕЗПЕЧЕННЯ АНОНІМНОСТІ В МЕРЕЖІ ІНТЕРНЕТ	<b>359</b>
<b>27.</b>	<i>К.С. Савченко, А.А. Кулько, С.В. Толюпа</i> ПРОБЛЕМИ АВТОРИЗАЦІЇ ТА АВТЕНТИФІКАЦІЇ В ХМАРНИХ ТЕХНОЛОГІЯХ	<b>363</b>
<b>28.</b>	<i>А.А. Лобода, І.І. Пархоменко</i> ЗАХИСТ ІНФОРМАЦІЙНИХ РЕСУРСІВ ТА ПЛАТФОРМ МОБІЛЬНИХ ПРИСТРОЇВ	<b>365</b>
<b>29.</b>	<i>М.С. Іващенко, І.І.Пархоменко</i> АНАЛІЗ ПРОБЛЕМ БЕЗПЕКИ СЕРВІСІВ ІНТЕРНЕТУ РЕЧЕЙ	<b>369</b>
<b>30.</b>	<i>А.О. Кошина, І.І. Пархоменко</i> ЗАХИСТ WEB-ДОДАТКІВ ТА ТРАНЗАКЦІЙ КЛІЄНТ- СЕРВЕРНОЇ ВЗАЄМОДІЇ	<b>373</b>

<b>31.</b>	<i>А.О. Заїка, Л.В. Мирутенко, В.І. Вялкова</i> СПОСОБИ ВИЯВЛЕННЯ СТЕГОКОНТЕЙНЕРІВ В ГРАФІЧНИХ ОБ'ЄКТАХ	<b>377</b>
<b>32.</b>	<i>Л.О. Терейковська, В.П. Шуліка,</i> ГОЛОСОВЕ УПРАВЛІННЯ КОМП'ЮТЕРНИМИ СИСТЕМАМИ	<b>380</b>
<b>33.</b>	<i>А.В. Соколов, Ю.С. Оверчук</i> О ВОЗМОЖНОСТИ СИНТЕЗА АЛГЕБРАИЧЕСКОЙ НОРМАЛЬНОЙ ФОРМЫ ЧЕТВЕРИЧНЫХ ФУНКЦИЙ НАД ПОЛЕМ( $GF_4$ )	<b>384</b>
<b>34.</b>	<i>М.В. Самойленко, Д.С. Нечаснюк, І.І. Пархоменко</i> АНАЛІЗ ЗАСОБІВ ЗАХИСТУ ПРИСТРОЇВ ІoT	<b>388</b>
<b>35.</b>	<i>А.В. Петричук, В.Г. Зайцев</i> РОЗПІЗНАВАННЯ ОБЛИЧ У ВІДЕОПОТОКАХ НА ОСНОВІ МЕТОДА ВІОЛІ-ДЖОНСА І ЛОКАЛЬНИХ БІНАРНИХ ШАБЛОНІВ	<b>392</b>
<b>36.</b>	<i>П.В. Хусайнов</i> ФОРМАЛЬНИЙ АПАРАТ АНАЛІЗУ І СИНТЕЗУ ЗАДАЧ, ПРОЦЕСІВ ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ ІТС	<b>395</b>
<b>37.</b>	<i>О.О. Фразе-Фразенко, Н.Ф. Казакова, Ю.В. Копитін</i> ВПРОВАДЖЕННЯ СИСТЕМИ ЦЕНТРАЛІЗОВАНОГО МОНІТОРИНГУ В ІНФОРМАЦІЙНИХ СИСТЕМАХ	<b>397</b>
<b>38.</b>	<i>Д.О. Сорокін, Д.С. Дженджеро., О.Д. Кулагін, С.В. Толіпа</i> ЗАСТОСУВАННЯ ТЕОРІЇ ІГОР В СИСТЕМАХ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ	<b>401</b>
<b>39.</b>	<i>М.Ю. Довбій, А.С. Ярошенко, В.С. Наконечний</i> ПРИНЦИПИ ПОБУДОВИ ТА ІНФОРМАЦІЙНОГО ЗАХИСТУ АВТОМАТИЗОВАНИХ СИСТЕМ УПРАВЛІННЯ У СФЕРІ ІНФОРМАТИЗАЦІЇ ОХОРОНИ ЗДОРОВ'Я УКРАЇНИ НА ПРИКЛАДІ УКРАЇНСЬКОГО СЕРВІСУ EHEALTH	<b>405</b>

<b>40.</b>	<i>І.Д. Горбенко, О.О. Кузнєцов, О.В. Потій, Ю.І. Горбенко, О.Г. Качко, М.В. Єсіна</i> ПРОБЛЕМИ СТВОРЕННЯ СТАНДАРТІВ ПОСТКВАНТОВИХ КРИПТОГРАФІЧНИХ ПЕРЕТВОРЕНЬ ТА ХІД ЇХ ВИРШЕННЯ	<b>408</b>
<b>41.</b>	<i>О. В. Соснін</i> НОВІ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ РЕАЛІЇ В СУСПІЛЬНО-ПОЛІТИЧНИХ ПРОЦЕСАХ	<b>415</b>
<b>42.</b>	<i>С.Ю. Магула, О.Г. Оксіюк</i> ЗАГРОЗИ ЕЛЕКТРОНИХ БАЗ ПЕРСОНАЛЬНИХ ДАНИХ	<b>425</b>
<b>43.</b>	<i>С.М. Савонік, В.В. Савчук, Т.В. Бабенко</i> ЕКСПЛУАТАЦІЯ BadUSB ВРАЗЛИВОСТЕЙ	<b>428</b>
<b>44.</b>	<i>А.О. Григорьєва, С.В. Толюпа, Я.В. Шестак</i> МЕТОДИ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ	<b>431</b>
<b>45.</b>	<i>А.Г. Мошняга, Н.В. Лукова-Чуйко</i> ТЕНДЕНЦІЇ КІБЕРАТАК ТА СПОСОБИ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ВЕБ-РЕСУРСІВ ОРГАНІЗАЦІЙ	<b>434</b>
<b>46.</b>	<i>Т.І. Конрад</i> ДОСЛІДЖЕННЯ ПИТАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В МУЛЬТИМОДАЛЬНИХ ІНТЕЛЕКТУАЛЬНИХ ТРАНСПОРТНИХ СИСТЕМАХ	<b>438</b>
<b>47.</b>	<i>С.В. Толюпа, О.І. Терейковський</i> ВИЗНАЧЕННЯ ВХІДНИХ ПАРАМЕТРІВ НЕЙРОМЕРЕЖЕВОЇ МОДЕЛІ РОЗПІЗНАВАННЯ ГОЛОСОВИХ СИГНАЛІВ	<b>440</b>
<b>48.</b>	<i>А.С. Ткаченко, М.М. Браїловський</i> ЗАХИСТ ТА ПРИХОВУВАННЯ ІНФОРМАЦІЇ В ГРАФІЧНИХ ТА МУЛЬТИМЕДІЙНИХ ОБ'ЄКТАХ НА БАЗІ СТЕГАНОТЕХНОЛОГІЙ	<b>444</b>
<b>49.</b>	<i>О.Є. Пасячнік, О.Г. Оксіюк</i> ПРОБЛЕМАТИКА НОРМАТИВНОГО РЕГУЛЮВАННЯ ПРОВЕДЕННЯ АУДИТУ БЕЗПЕКИ ВЕБ-РЕСУРСІВ В УКРАЇНІ	<b>447</b>
<b>50.</b>	<i>О.А. Ткаченко, О.І. Ткаченко, К.О. Ткаченко</i> КІБЕРПРОСТІР І КІБЕРБЕЗПЕКА: ОСНОВНІ ПОНЯТТЯ, ВИЗНАЧЕННЯ, ТЕНДЕНЦІЇ	<b>450</b>

51.	<i>Р. С. Юхименко, О.Г. Оксіюк</i> ЕФЕКТИВНИЙ ЩОДЕННИЙ МОНИТОРИНГ ЛОГІВ	454
52.	<i>П.М.Сніцаренко, Ю.О.Саричев, В.А.Ткаченко, В.В.Грицюк</i> СУТНІСТЬ ТА ПРОБЛЕМНІ ПИТАННЯ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ДЕРЖАВИ	457
53.	<i>Т. Ю. Розенвассер, В.І. Вялкова, Л.В. Мирутенко</i> РОЗРОБКА КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ	461
54.	<i>О.В. Матвійчук-Юдіна</i> ГЕНЕЗА ІНФОГРАФІЧНОЇ І ГОЛОГРАФІЧНОЇ КОМПЕТЕНТНОСТЕЙ ФАХІВЦІВ ПРИ НАВЧАННІ КОМП'ЮТЕРНОЇ ГРАФІКИ БАКАЛАВРІВ КІБЕРБЕЗПЕКИ	465
55.	<i>О.А. Баранов</i> ПРАВО НА ПОРОЗИ СІНГУЛЯРНОСТІ	468
56.	<i>М. Явич, А. Аракелян</i> ПРОГРАММНАЯ РЕАЛИЗАЦИЯ МЕРКЛЕ	479
57.	<i>А. Соломко</i> НЕПРЕРЫВНЫЙ МОНИТОРИНГ И УПРАВЛЕНИЕ УЯЗВИМОСТЯМИ ИТ-ИНФРАСТРУКТУРЫ (НА ПРИМЕРЕ СИСТЕМЫ TENABLE SECURITYCENTER CONTINUOUS VIEW)	481
58.	<i>В.В. Козловский, С.В. Лазаренко</i> АКТУАЛЬНОСТЬ ЗАЩИТЫ ИНФОРМАЦИИ, ПЕРЕДАВАЕМОЙ МОБИЛЬНЫМИ СРЕДСТВАМИ	483
59.	<i>Р. Утченко</i> ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. ВЫЯВЛЕНИЕ, УПРАВЛЕНИЕ И РЕАГИРОВАНИЕ (НА ПРИМЕРЕ СИСТЕМЫ MCAFEE SIEM)	487
60.	<i>А. Красюков</i> ЗАЩИТА ОТ ИЗВЕСТНЫХ И НЕ ИЗВЕСТНЫХ УГРОЗ НА УРОВНЕ СЕТИ И КОНЕЧНЫХ ТОЧЕК (НА ПРИМЕРЕ ПЛАТФОРМЫ PALO ALTO NETWORKS)	489
61.	<i>М. Гурбанов</i> ЗАЩИТА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ И КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ ОРГАНИЗАЦИИ (НА ПРИМЕРЕ СИСТЕМЫ DIGITAL GUARDIAN)	491
62.	<i>В. А. Швець</i> ЗАГРОЗИ НАВІГАЦІЙНОМУ СЕГМЕНТУ МЕРЕЖЕВИХ СУПУТНИКОВИХ СИСТЕМ	493