

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»

ТЕНДЕНЦІЇ РОЗВИТКУ ТА ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ СУЧАСНИХ ІОТ-ПРИСТРОЇВ

Інтернет речей (IoT) все більше входить в наше життя та розширює можливості платформ і пристроїв. За інформацією Gartner до IoT щодня підключається понад 5,5 млн. нових «речей». Цьому сприяє:

- поширена комунікаційна інфраструктура;
- можливість глобальної ідентифікації кожного об'єкта;
- виняткова здатність кожного об'єкта відправляти і отримувати

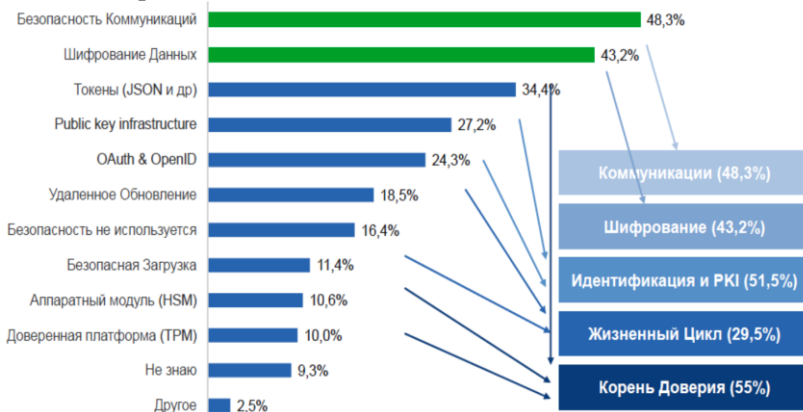
дані за допомогою персональної мережі, або мережі Інтернет, до якої він підключений тощо.

У 2016 році до IoT було підключено 6,4 млрд. пристроїв. На кінець 2016 року їх загальна кількість досягла 4,9 billion. До кінця 2025 року кількість таких «речей» може збільшитися майже втричі. Як наслідок, за прогнозами Mckinsey Global Institute щорічний економічний ефект від індустрії IoT сягатиме щорічно до 2025 року від 2,7 трлн. до 6,2 трлн.доларів. Переваги від впровадження IoT знайдуть відображення у: зменшенні експлуатаційних втрат; підвищенні операційної ефективності, зменшенні відходів, а також набагато більший продуктивності не тільки людської праці, а й обладнання.

Разом з тим, поширення IoT тягне за собою й велику відповідальність. Причиною тому є певні «слабкі місця» IoT, що пов'язані з переходом на IPv6, неможливістю забезпечення постійного живлення датчиків, відсутністю стандартизації архітектури і протоколів пристроїв, слабкою аутентифікацією, відсутністю підтримки з боку виробника для усунення вразливостей, неможливістю поновлення ПЗ і ОС, використанням незахищених мобільних технологій та хмарної інфраструктури, використанням небезпечного ПЗ тощо. Саме тому такий стан справ вимагає зосередження уваги, перш за все, на забезпеченні безпеки таких пристроїв на всіх етапах їх життєвого циклу - від створення до

розгортання і після нього. Підтвердженням такому можуть слугувати результати досліджень компанії Raconteur, згідно яких 25% усіх кібератак до 2020 року будуть доводитися на сферу IoT.

Зважаючи, що на поліпшення безпеки бізнес-структур і підприємств нині спрямовується лише до 10% від загальної суми бюджету ІТ, - стратегії безпеки IoT впроваджено нині лише на 78% у сфері телекомунікацій, на 73% - у сфері інформаційних технологій та на 69% - у сфері транспорту. З цього приводу Gagan Singh, старший віце-президент і генеральний директор департаменту мобільних розробок компанії Avast, відмічає таке: «Мы активно пользуемся устройствами интернета вещей дома и на работе, однако их безопасность до сих пор не идеальна. Это значит, что пользователи и сегодня остаются под угрозой. Ожидания пользователей возрастают: мы хотим получать комфорт и удовольствие от использования умных гаджетов. Поэтому перед производителями встает вопрос обеспечения безопасности умных устройств». Коментуючи стан розвитку власне IoT та засобів їх захисту менеджер корпорації ARM по продуктам IoT Майк Эфтимакіс відмічає таке: «Потенциал устройств IoT и сенсоров огромен. Однако, если мы не сумеем обеспечить безопасность каждого устройства, весьма вероятно, что использование незакрытых уязвимостей остановит прогресс, не позволив нам когда-либо полностью воспользоваться этим колоссальным потенциалом». Головними сферами проблем безпеки IoT-рішень вони, як і більшість інших експертів, вважають:



Основними компонентами захисту середовища IoT при цьому є:



- автентифікація;
- авторизація;
- мережева політика;
- безпечна аналітика: видимість і контроль.

Автентифікація.

Використовується для надання та перевірки ідентифікуючої інформації об'єкта IoT.

Коли підключені пристрої IoT потребують доступу до інфраструктури IoT, довірчі відносини ініціюються на основі ідентифікатора пристрою.

Авторизація. Дозволяє контролювати доступ пристрою по всій мережевій інфраструктурі. Цей рівень ґрунтується на основному рівні аутентифікації, використовуючи ідентифікаційну інформацію об'єкта. З компонентами перевірки автентичності та авторизації встановлюється довірче відношення між пристроями IoT для обміну відповідною інформацією.

Мережева політика.

Дозволяє підсилювати безпечну маршрутизацію всіх елементів IoT та транспортувати трафік кінцевої точки інфраструктурою, будь то управління або фактичний трафік даних. Як і рівень авторизації, вже встановлені протоколи і механізми для захисту мережевої інфраструктури впливають на політику, яка добре підходить для використання IoT.

Безпечна аналітика. Дозволяє визначити служби, за допомогою яких всі елементи (кінцеві точки і мережева інфраструктура, включаючи центри обробки даних) можуть брати участь у забезпеченні телеметрії з метою отримання видимості і, в кінцевому рахунку, контролю екосистеми IoT.

Характерним є те, що окрім захисту власне самих IoT-пристроїв від загроз, необхідно забезпечити й захист даних, що передаються мережею та команд управління, що будуть отримувати такі пристрої



тощо. Головними методами вирішення цих завдань на етапах розробки та експлуатації є передусім забезпечення цілісності коду, що виконується на пристроях та конфіденційності даних (інформації) за рахунок перевірки справжності користувачів і пристроїв, визначення чітких прав володіння для пристроїв (в тому числі даних, створених цими пристроями) та стійкості до віртуальних і фізичних атак.

На етапі розробки	На етапі експлуатації
Захист інтерфейсу управління Авторизація користувачів і вбудованого обладнання Обмеження доступності мережевих портів і служб Реалізація крипто захисту на транспортному і каналному рівнях Захист персональних даних, що містить IoT-пристрій Обмеження конфігурування IoT-пристрою користувачем тощо	Сегментація мережі, ізолювання або розділення шлюзами IoT сегментів та криптичних сегментів мережі Створення надійних політик безпеки для IoT-пристроїв

Висновок: IoT стає все більш поширеним явищем і все частіше з'являється в системах, від яких залежить життя людей, наприклад, автомобілях, літаках і промислового обладнанні. IoT спирається на новий стандарт мобільного зв'язку LTE Advanced Pro та відповідне обладнання, що підпадає під обов'язкове підтвердження відповідності. Для IoT-пристроїв необхідно будувати комплексні системи захисту, які були б здатні покрити різні рівні - рівні хмар і підключень.

Література:

1. Адам Тернер. Интернет вещей и носимые технологии : решение тайны частной жизни и безопасности, не сорвать инноваций. – 21 Rich. – JL & Технология. – № 6 (2015), – Режим доступа : <http://jolt.richmond.edu/v21i2/article6.pdf>;
2. Internet of Things: Privacy & Security in a Connected. – World Federal Trade Commission (FTC) Staff Report. – January 2015. – Режим доступа : <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127IPrpt.pdf>

3. Интернет вещей. – Режим доступа : <http://igate.com.ua/tag/internet-veshhej/4>; <http://revo.lverlab.com/chto-takoe-internet-veschey>

4. Интернет вещей : всё подключается к сети. – Режим доступа : <http://igate.com.ua/news/6309-internet-veshhej-vse-podklyuchaetsya-k-seti>

УДК 004.056.53

**Д.В.Палко¹, В.І.Вялкова¹,
Л.В.Мирутенко¹**

*Київський національний університет імені Тараса Шевченка¹
palko.dmytro@gmail.com*

ЗАХИСТ ІНФОРМАЦІЙНИХ РЕСУРСІВ ТА ТРАНЗАКЦІЙ В КОРПОРАТИВНИХ МЕРЕЖАХ

Єдиний інформаційний простір на сьогодні являється запорукою успішної діяльності сучасної організації в умовах жорсткої конкурентної боротьби. Саме розвинена інформаційна система є основною передумовою ефективного обігу потоків інформації на підприємстві, що в свою чергу зменшує час реакції на зміни, що відбуваються в компанії, сприяє оперативному прийняттю рішень, і забезпечує оптимальне управління усіма процесами в реальному масштабі часу.

Корпоративна мережа - це складна взаємопов'язана система, що являє собою сукупність мереж і служб передачі даних, які призначені для надання єдиного захищеного мережевого простору обмеженому рамками корпорації колу користувачів.

Такі мережі використовують розподілену модель обчислень. Основними функціональними компонентами корпоративних мереж є робочі місця (абоненти), інформаційні сервери корпорації, засоби телекомунікації, телеслужби, а також різноманітні централізовані системи забезпечення надійності, контролю, діагностики, управління безпекою та ефективністю функціонування. Головною особливістю корпоративних мереж є те, що доступ до інформації надається тільки обмеженій групі осіб у внутрішній мережі організації, що відділена від глобальних мереж брандмауерами. Але при цьому використовується той же

ЗМІСТ

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

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

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

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. Dmitruk, 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

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

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

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

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

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

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

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

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

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