Міністерство освіти і науки України
Державна наукова установа "Інститут модернізації змісту освіти"
Центральноукраїнський національний технічний університет

Комп'ютерна інженерія і кібербезпека: досягнення та інновації

Матеріали Всеукраїнської науково-практичної конференції здобувачів вищої освіти й молодих учених

(м. Кропивницький, 27–29 листопада 2018 р.)

Кропивницький ЦНТУ 2018

УДК 004
ББК 32.97
К63

К63 **Комп'ютерна інженерія і кібербезпека : досягнення та інновації** : матеріали Всеукр. наук.-практ. конф. здобувачів вищої освіти й молодих учених (м. Кропивницький, 27–29 листоп. 2018 р.) / М–во освіти і науки України, Держ. наук. установа "Інститут модернізації змісту освіти", Центральноукр. нац. техн. ун–т. — Кропивницький: ЦНТУ, 2018. — 448 с.

Збірник містить тези доповідей учасників Всеукраїнської науково-практичної конференції здобувачів вищої освіти та молодих учених "Комп'ютерна інженерія і кібербезпека: досягнення та інновації" (м. Кропивницький, 27–29 листопада 2018 року). Праці присв'ячені актуальним питанням інформаційних систем і технологій, технологій проектування комп'ютерних систем та мереж, інженерії програмного забезпечення, комп'ютерних систем штучного інтелекту, мережних ІТ, комп'ютерної електроніки, логіки, схемотехніки, графіки, нормативно-правових засад забезпечення кібернетичної безпеки, інформаційної безпеки національного сегмента кіберпростору, боротьби з кіберзлочинністю, захисту програм та даних в комп'ютерних системах і мережах.

Видання призначене для аспірантів, докторантів, науковців, викладачів і студентів технічних спеціальностей закладів вищої освіти та всіх, хто цікавиться питаннями комп'ютерної інженерії й кібернетичної безпеки.

УДК 004
ББК 32.97
К63

Рекомендовано до друку Науково-технічною радою Центральноукраїнського національного технічного університету (протокол № 11 від 29 листопада 2018 р.)

Відповідальний за випуск: канд. техн. наук Доренський О. П.

Тексти матеріалів конференції друкуються у авторській редакції, мовою оригіналу. За достовірність наведених у публікаціях даних, назв, імен, цитат та іншої інформації відповідальність несуть автори.

Адреса організаційного комітету конференції
Центральноукраїнський національний технічний університет
Кафедра кібербезпеки та програмного забезпечення
просп. Університетський, 8, м. Кропивницький, 25006
(0522) 55-10-49, 39-04-49; cntu-conference@ukr.net; www.kntu.kr.ua

© Автори матеріалів, 2018
© Центральноукраїнський національний технічний університет, 2018

ІНФОРМАЦІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ

Huskova V. H., Bidyuk P. I. A Combined Approach to Modeling Heteroscedastic Processes and Financial Risk Estimation 14

Litvinov A. A., Viniichuk Y. V., Dubovyi M. V., Bezotosnyi D. O. On Specific of Field Level Database Optimistic Locking for Increasing Information System Performance 17

Артеменко-Діденко А. І., Маковеєнко Д. О. Моделювання пропускної здатності мережі E-UTRA для адаптивних режимів MCS 18

Береговий С. М. Побудова інформаційних систем керування виробничими конвеєрними лініями засобами SCADA Wonderware System Platform 21

Бураков Р. А., Левицька Т. О. Автоматизована обробка класичних творів для фортепіано з використанням сіамської нейронної мережі 22

Вакуленко Д. О. Актуальні питання впровадження інфокомунікаційних технологій в агропромисловому комплексі України 24

Гвозденко В. О., Дем'янчик С. О., Давиденко Є. О. Технологія прийняття оптимального стратегічного рішення в військово-цивільний сфері 26

Голобородько Р. В. Дослідження захищеності мереж UMTS/LTE із використанням двостороннього підсилювача у комплексі зі спрямованою антеною 28

Гончар О. М., Дрєєва Г. М. Використання спеціалізованих мов програмування для операторів програмованого обладнання 30

Гринюк С. В., Кирилюк Л. М. Scratch як об'єктно-орієнтоване середовище візуального програмування 32

Грінченко Є. М., Колмик О. О. Методи управління інформаційними ризиками 35

Гура І. О., Александров Р. І. Важливість впровадження та розвитку кіберфізичних систем в Україні 37

Дмитрієва О. А., Клімаш О. В. Алгоритмічні методи кластеризації в рекомендаційних системах з колаборативною фільтрацією 39

Дмитрієва О. А., Гуськова Н. Г. Зведення чисельної реалізації рівнянь в частинних похідних до методу прямих на коллокаціонних блокових різницевих схемах 41

Дмитрієва О. А. Александров М. О. Підвищення ефективності методу контентної фільтрації з урахуванням розрідженності даних 43

Желєзняк Б. Ю. Переваги квантових комп'ютерів 45

Железняк Б. Ю. Огляд найбільш використовуваних на практиці алгоритмів 47

Железняк Б. Ю. Огляд історії розвитку квантової криптографії 49

Жолнер І. Д., Вялкова В. І. Використання теорії живих систем у СКЗІ 51

Заволодько Г. Е., Павлова Д. Б, Колеснікова Я. С. Інформаційна мережа систем спостереження як основа інформаційного забезпечення користувачів системи контролю повітряного простору 52

Ізотов Є. О. Аналіз сервісу управління персоналом як частина кіберфізичної системи університету 55

Ісмайлов К. Ю., Балтовський О. А. Концепція побудови динамічної інформаційної системи управління складної соціально-організованою структури 56

Казарінова М. В. Дослідження класифікаційних моделей для організації інформації в електронних бібліотечних системах 58

Коба О. В. Використання системи reCAPTCHA як засобу оцифровки друкованих носіїв 60

Коваленко О. В., Коваленко А. С. Аналіз основних підходів математичного моделювання та методологій для забезпечення максимальних показників безпеки програмного забезпечення 63

Ковальова К. М. Розробка методики діагностування цифрових систем 66

Кузнецов О. О., Агєєва М. М. Біометрична автентифікація на основі динамічної обробки зображень облич із використанням методу Eigenface 67

Кузнецов О. О., Власенко О. В. Біометрична автентифікація на основі відбитків пальців 69

Кузьменко Д. С., Луценко В. В., Тарасенко Ю. С. Питання підвищення рівня захищеності в інформаційно-телекомунікаційних системах 71

Кячев О. А. Аналіз механізмів захищеності систем Інтернету речей 73

Лозовий А. М. Використання віртуальних машин для завантаження криміналістичних образів жорстких дисків 74

Лудан Д. В. Розробка інформаційної технології для організації інтерактивних квестів 76

Можарівський В. В. Автоматизована торгівля на біржах криптовалют 78

Нетепенко В. В. Ідентифікації диктора за голосом 79

Окунь Є. В., Романько Д. В. Інтернет речей та проблеми його захисту 81

Остапенко А. О. Застосування кінетичного підходу до моделювання гідродинаміки 83

Підгорний П. Є., Сидорова М. Г. Розробка програмно-математичного забезпечення для аналізу траєкторій пересування об'єктів у просторі та часі 86

Пісарєв Д. С., Петрова О. О. Візуалізація «backtracking algorithm» 88

Пономаренко А. С. Місце генетичних алгоритмів у сучасному світі 89

Пономаренко А. С. Класифікація атак на інформаційні системи 91

Проніна О. І. Формалізація організації заказу в умовах індивідуальних потреб клієнта 93

Пронюк М. Я., Кропивницька В. Б. Порівняльний аналіз баз даних SQL та NoSQL 96

Рідозуб О. В. Розробка базових підходів до створення програмного забезпечення для роботи з напівпровідниковими детекторами CdTe, CdZnTe 97

Рудакова Є. О. Інформаційна система ідентифікації рослин 99

Савчук Т. О., Приймак Н. В. Інформаційна технологія пошуку асоціативних правил при розробці програмного забезпечення 100

Семенченко О. А. Аналіз розвитку інформаційних систем у світі 103

Середін О. Д., Шматок О. С. Порівняння потужності критерія Крамера - фон Мізеса і критерія хі-квадрат для малих тестових вибірок біометричних даних 106

Єлізаров А. Б., Симониченко Я. А., Симониченко А. А. Дослідження сучасних програмних стеганографічних засобів приховування інформації..... 108

Смірнова Т. В., Смірнов О. А., Дрєєв О. М., Смірнов С. А. Використання хмарних експертних систем в сфері інформаційного забезпечення обробки поверхні деталей 111

Стовманенко В. О., Григор'єв Д. О., Давиденко Є. О. Використання алгоритмів системного аналізу для роботи із медіа 114

Столяренко Є. Ю., Неласа Г. В. Розробка веб-сервісу для виконання операцій з елементами скінченних полів..... 116

Ткачук Р. О. Переваги операційної системи Linux 117

Фесечко Д. В. Порівняльний аналіз формату MP3..... 119

Фесечко Д. В., Конопліцька-Слободенюк О. К. Методології розробки програмного забезпечення 121

Четверик А. І. Визначення коефіцієнтів розподілу грошових коштів за заходами..... 122

Шевченко М. М. Хмарний сервіс зберігання даних..... 123

Шуліка Я. П. Сучасне on-page SEO 125

Шуліка Я. П. Біле та чорне SEO 126

Шуліка Я. П. Сучасне off-page SEO 127

Щербак В. К. Використання сенсору Kinect в системах диагностування рухомих об'єктів 129

Щербак Б. В. Розробка модулю автоматизованої системи для подачі матеріалу студентам за допомогою технологій доповненої реальності..... 131

ТЕХНОЛОГІЇ ПРОЕКТУВАННЯ КОМП'ЮТЕРНИХ СИСТЕМ ТА МЕРЕЖ

Берладін В. К., Конопліцька-Слободенюк О. К. Квантові технології сьогодення та перспективи їх розвитку 132

Горбань А. С., Цололо С. О. Декомпозиція першого технологічного циклу синтезу оксидних нанопорошків 134

Жесан Р. В., Голик О. П. Коротке узагальнення основних причин вразливості сучасних комп'ютеризованих систем 137

Колосов А. А. Моделювання компонентів керування МЕМС зі зворотними зв'язками з використанням Matlab / Simulink..... 140

Колосов Є. А. Моделювання мікроелектромеханічних актюаторів з використанням Matlab/Simulink 141

Кумченко Ю. О., Нагін Р. Ю. Платформа віртуалізації Proxmox VE для керування кластерами високої доступності 142

Кумченко Ю. О., Шевченко О. В. Комплексна система захисту серверного приміщення 144

Маркова О. М., Дяченко Д. О. Інформаційна система для контролю безпеки підйомних сосудів у залізорудних шахтах 146

Минайленко Р. М., Дрєєв О. М., Собінов О. Г., Денисенко О. О. Програмна компенсація дрейфу нуля в системі вимірювання вологості зерна в потоці 148

Незамай В. О. Використання методу автоматного програмування при побудові систем комунікації «Smart House» 150

Пасічко Є. В. Верифікація кінцевого автомата з допогомогою UVM 151

Покотило О. А. Аналіз протоколу динамічної маршрутизації BGP та його вразливостей 152

Сіленко М. О. Вибір системи числення для побудови комп'ютерних систем 154

ІНЖЕНЕРІЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Liubchenko O. S. Research Generation Register Model Components Methods for Verification Environment 155

Бабич Є. Ю. Кооперативна багатозадачність в RTOS 157

Банченко В. О. Дослідження та програмна реалізація стиснення звукової інформації за допомогою вейвлетних методів 158

Башинська О. О. Особливості розшифровки телеметричних логів безпілотних авіаційних комплексів в умовах неповноти інформації про перелік типів повідомлень 160

Бобилєва О. С., Дмитрієва О. А. Дослідження методу стрільби при розв'язанні крайових задач 163

Газдюк К. П., Жихаревич В. В., Остапов С. Е., Чижевський В. В. Розробка системи для комп'ютерного моделювання біологічних процесів 166

Ганістрат Д. О., Карабут Н. О. Методи інтеграції програмного забезпечення 167

Згара К. Г. Компоненти та архітектура корпоративної соціальної мережі 168

Золотухін Б. Є. Актуальні питання стандартизації та регламентації процесів реалізації програмних засобів 169

Іванова О. Т., Сидорова М. Г. Опанування проблеми управління часом за допомогою інформаційних технологій 170

Константинова А. А., Константинова Л. В. Дослідження засобів для підвищення транзакційної продуктивності MySQL 171

Косолап М. В., Михальчук Г. Й. Програмне забезпечення для розв'язання задачі маршрутизації з різнорідним вантажем 172

Майданик О. О. Особливості генетичних алгоритмів 173

Майданик О. О. Важливість оптимізації коду 175

Манченко Я. В. Спеціалізовані програмні засоби діагностики стану користувача глобальної мережі 177

Мішевський Г. А., Кузнєцов Д. І. Методи та засоби оптимізації пошуку медіа файлів у хмарних сховищах на основі використання Android додатку 178

Пархоменко Д. О. Концептуальні засади забезпечення якості програмних продуктів 180

Патиковський Ю. В. Структурно-функціональні особливості оцінки якості програмних засобів критичного призначення 181

Петренко А. Б., Колпаков М. О. Інтеграція хмарних сховищ Amazon S3 у веб-додатки розроблені засобами мови програмування Java 182

Петренко Д. О. Аналіз методів та розробка прототипу програмної системи для моніторінгу технічного стану автомобіля 185

Половинка О. Л. Використання паралельної реалізації для пошуку асоціацій 186

Ткаченко О. С. Аналітична оцінка трудомісткості процесів реалізації програмних засобів 187

Фесечко Д. В. Принципи роботи з великими даними 188

Фролова М. С., Співак Р. В. Застосування технології доповненої реальності та 3d-моделювання для попередження надзвичайних ситуацій 190

Черніков Д. Д., Конопліцька-Слободенюк О. К. Проблема 2038 - 32bit systems 192

КОМП'ЮТЕРНІ СИСТЕМИ ШТУЧНОГО ІНТЕЛЕКТУ

Бабич Є. Ю. Небезпека штучного інтелекту 193

Берладін В. К., Гермак В. С. Штучний інтелект у сучасному світі 194

Боярський Д. О. Генерація дизайну сайтів на основі використання згорткових генеративних змагальних мереж глибокого навчання 196

Власюк І. В., Сухомлин А. А. Нейронні мережі з розподіленою обробкою даних 197

Гіцеларь Д. В. Штучний інтелект та його залежність від відеоігор 198

Гіцеларь Д. В. Методи утворення штучного інтелекту комп'ютерно-керованим персонажем. Обгрунтування вибору саме нейронної мережі 200

Гриб О. О., Конопліцька-Слободенюк О. К. Штучні нейронні мережі 202

Калюжний Р. І. Симбіоз штучного інтелекту і хмарних технологій 204

Котов І. А. Модель маркування сигнального графа мережі метаправил в онтологіях інтелектуальних систем 205

Логінова С. М. Дослідження методу лейтнера з нейромережею для мобільного додатку вивчення іноземної мови 208

Маценко Р. В. Використання нейромережевої комп'ютерної системи для анімаційних об'єктів 210

Мельник Р. А., Шпортько В. О., Тушницький Р. Б. Програмне забезпечення для екстракції, збереження та опрацювання зображень супутникових карт хмарності 211

Разно В. С. Штучна нейронна мережа. Нейронні мережі проти звичайних комп'ютерів 213

Сидоренко С. В. Прогнозування тенденцій рівня цукру у крові за допомогою нейтронної мережі 215

Сінєгіна А. Д. Передача стилю за допомогою нейронної мережі 216

Сінєгіна Ю. Д. Колоризація зображень за допомогою згорткової нейронної мережі 218

Холоша М. С., Сидорова М. Г. Побудова ансамблю нейронних мереж для тегування зображень 220

Шуліка Я. П. Сучасні можливості штучного інтелекту 221

МЕРЕЖНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Безрук Є. А., Брусеньский В. Р., Козіна Г. Л. Впровадження технологіїї блокчейн в торгівлю цінними паперами 223

Демидов З. Г. Big data: застосування та можливості 225

Дрєєва Г. М. Імітаційне генерування фрактального трафіку за допомогою GERT моделі 226

Коваленко Д. О. Розробка програмного забезпечення для веб-ресурсу "Планувальник навантаження викладачів ХНЕУ імені Семена Кузнеця" 230

Коваль В. О. Переваги та недоліки клієнт-серверної архітектури 231

Коваль В. О., Конопліцька-Слободенюк О. К. Переваги та недоліки мережевих топологій 232

Константинова Л. В., Константинова А. А. Дослідження засобів для кросплатформеної розробки мобільних додатків 234

Константинова Л. В., Константинова А. А. Огляд існуючих засобів для повнотекстового пошуку в веб-проектах 236

Коровaненко В. В. Оптимізація процесу вибору постачальника безкоштовного хостингу 238

Кулік І. С. Система підтримки прийняття рішеня при оцінюванні якості трафіку в NGN 241

Кучерявий М. В. Аналіз алгоритмів взаємодії елементів інтернету речей 244

Мамонтов О. О. Застосування методів сплайнапроксимації для синтезу характеристик нелінійних пристроїв засобів телекомунікації 247

Матвєєнко Ю. В. Сучасні WEB-дизайн і інтернет-технології 248

Оксіюк О. Г., Кротов В. Д. Управління потоками даних в Ad Hoc мережах спеціального призначення 250

Ткаченко Е. В. Огляд сучасних технологій розробки баз даних їх властивостей та функцій 253

Цюпко В. В. Хмарні сервіси SaaS, PaaS, IaaS і їх тренди розвитку 255

Шуліка Я. П. Розробка сайту з урахуванням SEO 257

КОМП'ЮТЕРНА ЕЛЕКТРОНІКА, ЛОГІКА Й СХЕМОТЕХНІКА

Аносов О. В. Аналіз застосування методу AEP для формальної верифікації HDL-опису дизайнів цифрових систем 259

Антонюк М. А., Неласа Г. В. Дослідження арифметики точок еліптичної кривої на пристроях з обмеженим об'ємом пам'яті 261

Кучеренко І. О. Використання темпоральних графів при розробці шаблону опису алгоритмів функціонування скінченних автоматів 262

Майданик О. О. Мови опису апаратури для ПЛІС та їх використання в сучасній обчислювальній техніці 264

Попко С. О. Розробка інтелектуального зарядного пристрою на основі мікроконтролера 266

Семеніхін Д. О. Моделювання МЕМС сенсорів з використанням Matlab/Simulink 267

Сенько А. О., Андрющенко Д. Ю. Дослідження структури статичного ОЗП 269

КОМП'ЮТЕРНА ГРАФІКА

Абель Т. В., Дрєєва Г. М. Дослідження та програмна реалізація системи генерування зображення за допомогою рекурентних повторень 271

Гіцелярь Д. В. Огляд та практичне застосування L-систем 273

Долженко І. О. Дослідження методів сегментації для розпізнавання харчових об'єктів ... 275

Карпов Є. О. Особливості комп'ютерної графіки в контексті Net-Art 277

Ладигіна О. А. Аналіз моделей освітлення для досягнення фотореалізму у віртуальній реальності 279

Сахарова А. В. Цифрове оточення людини 281

Ткаченко А. М. Роль комп'ютерної графіки у підготовці майбутнього фахівця в сучасних умовах працевлаштування 283

Шевченко В. О. Вибір засобів комп'ютерної графіки для вирішення прикладних задач 285

НОРМАТИВНО–ПРАВОВІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Obach V. Current Issues of Cyber Defense in Ukrainian Billing and Payment Systems 286

Гайтота Є. В., Чуницька В. В., Нікуліщев Г. І. Про врахування досвіду Німеччини в Стратегії кібербезпеки України 288

Жогов В. С., Форос Г. В. Особливості нормативно-правового регулювання кібербезпеки в Україні та в законодавстві інших країн 291

Колодяжний І. О. Вдосконалений підхід до протидії пропаганді сепаратизму та антиукраїнській ідеології в соціальних мережах..... 293

Копиця Н. С., Ликов Ю. В. Аналіз документа "Політика конфіденційності" на базі регламенту GDPR в популярних інтернет-ресурсах 295

Обач В. А., Гермак В. С. Аналіз впливу темних патернів на свідомість людини 297

Прокопов В. В., Гермак В. С. Огляд основних вразливостей SCADA-система та засобів їх усунення 298

Романовська М. С. Компаративний аналіз визначення сутності поняття „кібербезпека" 300

Семеній Д. М. Нормативно-правові засади забезпечення кібербезпеки України 303

Толмачов Ю. П. Актуальні питання забезпечення інформаційної безпеки у медіасфері України 306

Хомяк О. О., Шматок О. С. Методологія формування систем захисту інформації сучасних АС 307

ІНФОРМАЦІЙНА БЕЗПЕКА НАЦІОНАЛЬНОГО СЕГМЕНТА КІБЕРПРОСТОРУ

Артюх С. Г., Шевченко А. С. Аналіз методик забезпечення інформаційної безпеки організацій та інформаційних систем 308

Безрук Є. А., Брусеньский В. Р., Нікуліщев Г. І. Використання технології uXTD та методу Timing-атак для деанонімізації користувачів Tor..... 309

Бойко О. С. Протидія несанкціонованому запису мовної інформації 312

Колодяжний І. О. Дослідження алгоритмів аналізу віртуальних соціальних мереж 315

Леонтьєв В. С., Неласа Г. В. Аналіз методів спарювання точок еліптичних кривих 317

Майборода О. П. Демаскуючі ознаки GSM і CDMA радіоакустичних закладних пристроїв..... 318

Нєдєльський Д. С. Інформаційні війни в соціальних мережах 320

Петров М. В. Дослідження технології блокчейн, криптографії та крипто валют..... 321

Прокопов В. В. Нормативно-правові засади протидії маніпуляціям суспільною свідомістю і поширенню спотвореної інформації в Україні..... 322

Савченко О.О. Специфічні властивості скручених кривих Едвардса для криптографічних додатків 324

Трухачов А. В., Козіна Г. Л. Аналіз захищеності ідентифікації клієнта у системі Біткоін..... 326

Шуліка Я. П. Сучасна пропаганда як продукт інформаційного простору 327

Щирова Ю. А. Аналіз впливу атак на традиційні системи автентифікації користувачів..... 329

БОРОТЬБА З КІБЕРЗЛОЧИННІСТЮ

Білоконь Д. С., Форос Г. В. Окремі аспекти протидії кіберзлочинності 331

Вакулинська А. Є. Методи біометричної автентифікації 334

Глазунов Д. М. Важливість забезпечення захисту інформації від загроз соціальної інженерії 336

Донченко П. О., Жума В. М., Савельєва Т. В. Механізм реагування на потенційно небезпечні дії користувача в Linux 339

Кривенко С. С., Шматок О. С. Методи виявлення закладних пристроїв 341

Кульчицький О. С. Вимоги протидії кіберзлочинності в умовах громадської локалізації 344

Макеєв А. В. Огляд особливостей кіберзлочинів в Україні 345

Пашинських В. В. Огляд дистрибутивів GNU/Linux для тестування безпеки 346

Пашинських В. В., Конопліцька-Слободенюк О. К. Двофакторна автентифікація: огляд та недоліки 348

Пашинських В. В. Огляд інструментів для пентестинга 350

Поліщук О. В., Карабут Н. О. Кібертероризм як глобальна проблема 352

Стрілець А. М. Основні технології проти кіберзлочиності 354

Хлистун В. В. Кіберзлочинність як загроза для кожного: види, причини розвитку, поради до протидії загрозам 357

Шостак В. І. Захист інформаційних ресурсів та засобів обробки інформації 359

ЗАХИСТ ПРОГРАМ ТА ДАНИХ В КОМП'ЮТЕРНИХ СИСТЕМАХ І МЕРЕЖАХ

Sokolov V. Y., Korzhenko O. Y. Analysis of Recent Attacks Based on Social Engineering Techniques 361

Аяз Р. Х. Використання конволюції/деконволюції для стегоаналізу зображень в рамках підходу Хармсена и Перл мана 364

Бабюк Є. М. Інновації у сфері кібербезпеки: хмарні ресурси та машинне навчання 366

Байлюк Є. М. Розвідувальна організація з питань загроз Cisco Talos Intelligence Group 368

Байлюк Є. М. Покращений протокол безпеки безпровідних мереж Wi-Fi Protected Access 3 (WPA3) 370

Безносюк І. В. Сучасні методи аутентифікації 372

Безрук Є. А., Брусеньский В. Р., Неласая Г. В. Використання технології ubeacons для тергетингу та методи боротьби з нею 374

Вервейко В. В. Аналіз методів захисту від комп'ютерних вірусів 377

Власов Б. Ф. Модернізація алгоритму гешування MD5 378

Ганечко О. О., Даніленко В. М., Сагун А. В. Підсистема інтелектуальної фільтрації електронних повідомлень на базі алгоритму машинного навчання 380

Гонтарь І. А. Методика виявлення вразливостей мереж стандарту IEEE 802.11 з використанням пакету KALI LINUX 383

Грек О. М., Марчук А. В. Розробка технологій захисту від мережних атак із використанням апарату штучних нейронних мереж 385

Гриб О. О. Особливості роботи брандмауерів 386

Григоров А. Г. Актуальність протидії XSS-атакам та засоби захисту від них 388

Гуреєва А. О., Карабут Н. О. Методи і технології захисту комп'ютерних мереж (фізичний та канальний рівні) 390

Дмитрієва О. А., Горбенко В. Ю. Створення відмовостійких розподілених інформаційних систем 392

Добринін К. І. Засоби забезпечення захисту аккаунтів користувачів при використанні публічних мереж стандарту 802.11 393

Журова П. В. Блочне шифрування з властивостями виправлення помилок 395

Ільєнко А. В., Яковенко О. Л., Данилюк Ю. Р. Аналіз сучасних методів автентифікації з використанням криптографічних перетворень 396

Коваль В. О. Захист персональних даних в Інтернеті 398

Колмик О. О., Грінченко Є. М. Майнінг на чужих ресурсах 399

Кохан Є. Р. Соціальна інженерія як загроза інформаційній безпеці 401

Крапівін В. В. Система виявлення мережевих атак на основі алгоритмів нечіткого виведення 402

Крайтапук К. К. Чи потребує Інтернет Речей інтеграції блокчейну? 405

Кузнєцов О. О., Попова М. В., Шаповал О. В., Чернов К. А., Єрьомин Е. С. Аналіз і дослідження автоматизованих технологій пошуку вразливостей програмного забезпечення 406

Кузьменко Д. С., Луценко В. В., Тарасенко Ю. С. Аспекти експрес аналізу захищеності комп'ютерних даних 409

Лісова В. П. Аналіз методів пошуку прихованих мереж в корпоративній мережі з розгорнутими ролями Active Directory 411

Мартиненко О. О., Телющенко В. А. Оцінка надійності програмних засобів захисту 413

Марченко А. Ю. Мінімізація факторів суб'єктивності в тестуванні на проникнення 414

Машталер Д. О. Динамічне використання групи ключів в асиметричному Шифруванні 415

Михайловский Р. Л., Шматок О. С. Система стеганоаналізу на основі розпізнавання образів 416

Нєдєльський Д. С., Конопліцька-Слободенюк О. К. Grey Wizard – нові технології захисту веб-ресурсів 418

Оксіюк О. Г., Руденко А. С. Захист інформації у корпоративних мережах на основі моделі OSI 419

Павлов І. І. Методи підвищення надійності та захищеності корпоративних комп'ютерних мереж 421

Покотило О. А. Аналіз моделі Cyber Kill Chain та її використання для забезпечення захисту мережі 423

Романько С. В., Астраханцев А. А. Методи вбудовування цифрових водяних знаків у відеофайли, що стиснені за стандартами MPEG 425

Сандаков О. О., Гермак В. С. Огляд сучасних криптографічних алгоритмів 427

Сердюк О. Ю. Підхід щодо оцінки вразливостей інформаційних систем з використанням метрик стандарту NIST CVSS v3 429

Трапезнікова В. П., Телющенко В. А. Алгоритм вибору альтернативних засобів захисту для автоматизованої системи 432

Удовиченко А. В. Вибір методу аутентифікації у бездротових мережах 434

Федорко М. А., Маслова Н. О. Застосування вітчизняних стандартів шифрування для захисту даних великих обсягів 435

Нікуліщев Г. І., Хвостенко А. І. Дослідження та аналіз сучасних методів та засобів захисту хмарних обчислень 437

Хемішінець Є. В., Куцак С. В. Аналіз механізмів захисту даних в бездротових мережах 439

Целуйко В. В., Никодюк Д. В. Важливість використання SIEM в системах захисту банківської таємниці 442

Чекурда О. М., Пономарьов О. А. Формування моделі загроз для інформації, що циркулює в телекомунікаційних системах військового призначення 443

Черняк Т. О., Глушко В. В. Вдосконалення методів безпечного хешування при забезпеченні автентичності та цілісності даних у автоматизованих банківських системах 444

Ярош І. В., Черняк Т. О. Розробка системи виявлення вторгнень у web-додатки 446

УДК 004.056.53

Колмик О. О., Грінченко Є. М.
Харківський національний університет внутрішніх справ

Майнінг на чужих ресурсах

В даний час значно зросла популярність криптовалют. Різке зростання їх вартості привело до появи великої кількості людей які на цьому заробляють. Для багатьох це стає основним джерелом доходу, а для деяких майнінг перетворився на повноцінний бізнес. Частина добропорядних користувачів отримують свої біткоіни, збираючи свої майнінг-ферми, не завдаючи при цьому шкоди іншим людям. Але деякі майнять біткоіни на чужих комп'ютерах. Прихований майнінг - це процес видобутку криптовалюти зловмисником на чужому комп'ютері. При цьому жертва ні про що не підозрює, а шахраї добувають кріптовалу, не витрачаючи власні кошти і ресурси. Для майнінга криптовалюти на чужих потужностях шахраї проводять зараження комп'ютера вірусом. Це зараження відбувається при відкритті шкідливих повідомлень, скачування невідомих файлів і перегляду спам-розсилки. Ця програма активується, автоматично підключається до заданого розробником пулу і починає видобуток криптовалюти. Цей спосіб називається прихованим майнінгом з використанням вірус-майнера. Однак для того, щоб почати майніти за рахунок користувача зовсім необов'язково встановлювати на його комп'ютер троян або іншу вірусну програму. Досить ввести в код сайту спеціальний скрипт, який дозволяє непомітно підключитися до гостьової системі сайту. Такий спосіб називається браузерним майнінгом. Найчастіше приховано майнять піратські популярні сайти, сайти з фільмами і серіалами, торрент-трекери, форуми.

У початковому етапі розвитку шкідливих програм частину їх вдавалося вирахувати і видалити, так як вони активізували всі невикористовувані ресурси ПК, що призводило до перегрівів і неможливості роботи комп'ютера. У цих умовах для маскування своїх дій, і забезпечення отримання прибутку шахраї пішли на зниження обсягів використовуваних ресурсів, припускаючи, що при цьому вірус пропрацює довше, так як якщо він не заважає, то і виявити його буде складніше. Якщо на першому етапі віруси майнери могли використовували 90-100%, потужностей ПК, то далі вони різко знизили завантаження ПК і довели його до 2 до 5% вільних ресурсів, фактично не заважаючи користувачеві спокійно працювати.

Виявлення та захист від прихованого браузерного майнінгу не викликає великих труднощів. Якщо при відвідуванні сторінки комп'ютер почне працювати повільно і при цьому диспетчер задач відображає збільшене навантаження, то потрібно просто вийти з такої сторінки. Крім того, необхідно встановити найсучасніші антивірусні програми і постійно оновлювати їх бази до останніх версій. Також можна скористатися розширеннями для браузерів «No Coin» і «minerBlock». Ще один спосіб - використання блокувальників типу «AdBlock» і йому подібних. Ці програми здатні з успіхом блокувати більшість спливаючих банерів, особливо завдають шкоди вашому центральному процесору CPU шляхом підвищеного використання потужностей. Також потрібно відзначити, що в комп'ютерну та мобільну версії браузера Opera тепер вбудований захист від майнінгу.

Ситуація з прихованим вірус майнінгом трохи складніша. Як зазначалося, багато сучасних вірусів-майнерів використовують невелику частину потужності ПК. Тому їх важко виявити. Якщо виникли підозри, що ПК заражений, необхідно за допомогою антивірусної програми провести глибоку перевірку з метою підтвердження наявності

вірус-майнера на комп'ютері. Це дозволить підтвердити присутність, але можливо антивірусна програма визначить конкретне місце розміщення вірусу. Видалити шкідливий софт з жорсткого диска буде набагато складніше, тому що частина програм можуть відновлюватися з bat файлу в разі, якщо вбудований сканер не знаходить виконавчий файл. Після видалення всіх підозрілих програм з жорсткого диска потрібно відкрити диспетчер задач і закрити всі не знайомі процеси, або ті, які займають більше 10% потужності. Необхідно звернути увагу на завантаженість CPU (процесор) і GPU (відеокарта) понад норму і закрити їх по черзі. Як правило цього вистачає для того щоб вірус-майнер, який не має можливості відновлюватися або автозапускатися, після перезавантаження був знищений. Однак це стосується відносно «слабких» вірус-майнерів. Складні програми прихованого майнінгу можуть приховувати свою присутність в системі, можуть відключаються перед відкриттям диспетчера задач або самі його закривати. Є версії, які відстежують запуск антивірусної програми і видаляють виконавчу частину, а після перезавантаження відновлюються. Алгоритм пошуку і видалення вірус майнера з ПК наступний:

- запустити повну перевірку антивірусною програмою, яка оновлена до останньої версії;
- проаналізувати результати перевірки і видалити всі підозрілі програми, що виявлені антивірусом;
- перезавантажити ПК. Під час перезавантаження увійти в меню BIOS, і вибрати завантаження операційної системи з розширеними настройками Advanced Boot Options;
- запустити безпечний режим з мережевою підтримкою (Safe Mode w Networking);
- запустити систему і авторизуватись під своїми обліковими даними;
- знайти в мережі і завантажити якісне ПО для роботи із шпигунськими програмами, наприклад, Malwarebytes Anti-Malware;
- в обраному режимі, пошукове ПО буде знаходити все підозріле ПО, що не входить в базові настройки Windows і автоматично видаляти. Також, будуть видалені дані з системного реєстру і довантажуючи базові файли для відновлення працездатності ряду програм, частина файлів яких здалася підозрілою.

У більшості випадків цього вистачає для того щоб впоратися навіть з досить сильними вірус-майнерами. Якщо достовірно відомо про присутність вірус-майнера на ПК, то кращим рішенням в ситуації залишається традиційне повне форматування диска і переустановлення операційної системи. Саме в такому порядку, оскільки файли майнера, що виконувані не зберігається в тих папках, де їх будуть шукати і не прив'язані до конкретної ОС, тобто можуть активуватися і після її переустановлення.

Висновки:

1. щоб превентивно захиститися від атак прихованих майнерів, слід обмежити відвідування неперевірених сайтів і відразу ж закривати будь-які інформаційні портали, на які лається антивірус або захист браузера.
2. не відкривати листи від незнайомих кореспондентів, а також рекламні листи.
3. встановити якісне антивірусне ПЗ і постійно його оновлювати.
4. періодично проводити глибокі перевірки, наприклад, щоночі або раз на три дні, щоб видаляти будь-яке вірусне сміття.
5. в ідеальній ситуації відбирати ряд надійних ресурсів для перегляду кіно, прослуховування музики та інше, а також обмежте скачування контенту з піратських порталів.