МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Одеська національна академія харчових технологій
Навчально-науковий інститут комп`ютерних систем і технологій
"Індустрія 4.0" ім. П.М. Платонова
Факультет Комп`ютерної інженерії, програмування та кіберзахисту

XX Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

“СТАН, ДОСЯГНЕННЯ І ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ”

Матеріали конференції. Частина І.

Одеса

21-22 квітня 2020 р.

Стан, досягнення і перспективи інформаційних систем і технологій / Матеріали XX Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Частина І. Одеса, 21-22 квітня 2020 р. - Одеса, Видавництво ОНАХТ, 2020 р. - 240 с.

Збірник включає матеріали доповідей учасників конференції, які об'єднані по секціях кафедри інформаційних технологій та кібербезпеки (ІТтаКБ).

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Голова - д.т.н., проф., **Єгоров Б.В.**, ректор ОНАХТ.

Співголови:

Поварова Н.М. – к.т.н., доц., проректор з наукової роботи ОНАХТ,
Котлик С.В. – к.т.н., доц., директор ННІКСіТ "Індустрія 4.0" ОНАХТ,
Даріуш Долива, д.математичн.наук, уповноважений декана факультету Інформатики УІтаПЗ, м. Лодзь, Польща,
Ковалюк Т.В. - к.т.н., доц. кафедри АСОІтаУ НТУУ «Київський політехнічний інститут».

Члени оргкомітету:

Плотніков В. М. – д.т.н., проф., завідувач кафедри ІТтаКБ ОНАХТ,
Артеменко С.В. – д.т.н., проф., завідувач кафедри КІ ОНАХТ,
Князєва Н.О. – д.т.н., проф. кафедри КІ ОНАХТ,
Хобін В.А. – д.т.н., проф., завідувач кафедри АТПтаРС ОНАХТ,
Тарасенко В.П. – д.т.н., проф., завідувач кафедри СКС НТУУ «Київський політехнічний інститут»,
Невлюдов І.Ш. – д.т.н., проф., завідувач кафедри КІТАМ ХНУРЕ,
Мельник А.О. – д.т.н., проф., завідувач кафедри ЕОМ НУ "Львівська політехніка",
Жуков І. А. – д.т.н., проф., завідувач кафедри КСтаМ НАУ.

Матеріали подано українською, російською та англійською мовами.
Редактор збірника Котлик С.В.

СЕКЦІЯ № 1

Комп'ютерні науки

Тематичні напрями:

МАТЕМАТИЧНЕ І КОМП'ЮТЕРНЕ МОДЕЛЮВАННЯ СКЛАДНИХ ПРОЦЕСІВ

УПРАВЛІННЯ, ОБРОБКА ТА ЗАХИСТ ІНФОРМАЦІЇ

НОВІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В ОСВІТІ

ПРОЕКТУВАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ ТА ПРОГРАМНИХ КОМПЛЕКСІВ

КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА КІБЕРБЕЗПЕКИ

ОДЕСЬКОЇ НАЦІОНАЛЬНОЇ АКАДЕМІЇ ХАРЧОВИХ ТЕХНОЛОГІЙ

Список
скорочень організацій, представники яких взяли участь у конференції

Таблиця 1

Скорочення	Повна назва організації
АУПРБ	Академия управления при Президенте Республики Беларусь
БГЄУ	Белорусский государственный экономический университет
ВНТУ	Вінницький національний технічний університет
ДДПУ	ДВНЗ «Донбаський державний педагогічний університет»
УДХТУ	ДВНЗ «Український державний хіміко-технологічний університет»
ДДТУ	Дніпровський державний технічний університет
ДДМА	Донбаська державна машинобудівна академія
ДНТУ	Донецький національний технічний університет
ДНУ	Донецький національний університет ім. Василя Стуса
ІФНТУНГ	Івано-Франківський національний технічний університет нафти і газу
ІІТЗН	Інститут інформаційних технологій і засобів навчання НАПН України
ІТТНАН	Інститут технічної теплофізики НАН України
КНУ	Київський національний університет імені Тараса Шевченка
НТУУ "КПІ"	Національний технічний університет «Київський політехнічний інститут»
КПАІТ	Коледж промислової автоматики та інформаційних технологій ОНАХТ
КДПУ	Криворізький державний педагогічний університет
НУ"ПП"	Національний університет «Полтавська політехніка імені Юрія Кондратюка»
НТУ «ХПІ»	Национальный технический университет "Харьковский политехнический институт"
ОНПУ	Одеський національний педагогічний університет ім.Ушінского
ОНАХТ	Одеська національна академія харчових технологій
ОНПУ	Одеський національний політехнічний університет
ОНУ	Одеський національний університет імені І. І. Мечникова
ПДАТУ	Подільський державний аграрно-технічний університет
РДГУ	Рівненський державний гуманітарний університет
СКХП	Сумський коледж харчової промисловості НУХТ
ТЛіАЛ	Технічний ліцей імені Анатолія Лигуна, Національний технічний університет «Дніпровська політехніка»
УАД	Українська академія друкарства
УДПУ	Уманський державний педагогічний університет імені Павла Тичини
ХНУ	Хмельницький Національний Університет
ХНУРЕ	Харківський національний університет радіоелектроніки
ЦУНТУ	Центральноукраїнський національний технічний університет
ЧНУ	Чорноморський національний університет ім. Петра Могили
IAE	Institute of Automation and Electrometry of the Siberian Branch Russian Academy
VNTU	Vinnytsia National Technical University

РОЗРОБКА ВЕБ-СКАНЕРУ ДЛЯ ВИЯВЛЕННЯ ПРОРІХ У ЗАХИСТІ ХОСТУ

Смирнов В.Г., студент IV курсу, керівник: Стоянова Р.В., викладач
Коледж промислової автоматики та інформаційних технологій ОНАХТ

Перші спроби злому сайту з'явилися практично одночасно з їх широким розповсюдженням. Зломом займалися професійні хакери, які володіли спеціальним набором компетенцій й відповідним технологічним інвентарем, заради фінансової вигоди або зі спортивного інтересу.

Поступово злом сайту перестав носити виключно цільовий характер, перетворившись у масове явище, коли хакери, використовуючи відомі вразливості в CMS(Content management system), за раз стали атакувати десятки тисяч сайтів з ідентичними критичними вразливостями і пізніше використовувати своїх жертв для заробітку: розповсюдження спаму, шкідливого програмного забезпечення, крадіжки трафіка тощо.

Зростаюча кількість утиліт для злому і способів монетизації скомпрометованих веб-ресурсів не може не позначатися на збільшенні зростання числа атак. Щорічно в звітах антивірусних компаній публікується тривожна цифра, що сигналізує про підвищений інтерес хакерів до отримання контролю над веб-сайтами з метою їх подальшої експлуатації. При цьому потрібно розуміти, що сам по собі процес злому для хакера майже нічого не коштує: досить звичайного виходу в інтернет і певних знань, які можна легко отримати на спеціальних хакерських форумах у пабліках.

На тлі загальної «діджіталізації» суспільства й очевидного зміщення інтересів зловмисників з офлайна в онлайн, який виглядає більш безкарним, питання безпеки сайтів організацій та приватних осіб стає актуальним як ніколи. Ситуація ускладнюється і загальною фінансово-економічною нестабільністю в країні: швидкий заробіток нечесним і простим способом привертає увагу багатьох.

Опинитися під прицілом хакера може будь-який веб-ресурс, який відкривається в браузері і індексується пошуковими системами Яндекс, Google та ін. Кандидати для атак знаходяться досить-таки просто. Наприклад, хакери можуть використовувати Google Hacking Database - базу даних «Дорків» (dorks) - пошукових запитів на метамові Google. Дана інформація зберігається у відкритому доступі і, використовуючи її, зловмисник може знайти десятки тисяч сайтів з потрібними йому критичними уразливостями, а потім провести масову атаку в автоматизованому режимі.

Для забезпечення безпеки власних сайтів необхідно знати їх слабкі місця та, за можливості, прикривати їх. Найбільш популярними інструментами для пошуку уразливостей на сьогодні є:

- Nmap ("Network Mapper") - це утиліта з відкритим вихідним кодом для дослідження мережі та перевірки безпеки. Вона була розроблена для швидкого сканування великих мереж, хоча прекрасно справляється і з одиничними цілями. Nmap використовує сирі IP пакети оригінальними способами, щоб визначити які хости доступні в мережі, які служби (назва програми та версія) вони пропонують, які операційні системи (і версії ОС) вони використовують, які типи пакетних фільтрів / брандмауерів використовуються і ще багато інших характеристик. У той час як Nmap зазвичай використовується для перевірки безпеки, багато мережних і системних адміністраторів знаходять її корисною для звичайних завдань, таких як контроль структури мережі, управління розкладами запуску служб і облік часу роботи хоста або служби.

- Nikto - це сканер з відкритим вихідним кодом (GPL) для веб-серверів, він виконує комплексні тести щодо серверів за кількома напрямками, включаючи понад 6700 потенційно небезпечних файлів / програм, перевірка на застарілі версії більше 1250 серверів і проблеми, специфічні для версій більш ніж 270 серверів. Сканер також перевіряє елементи конфігурації сервера, такі як присутність декількох індексних файлів, серверні опції HTTP і намагається визначити ім'я і версії веб-сервера і програмного забезпечення.

- WPScan - це сканер вразливостей WordPress, що працює за принципом «чорного ящика», тобто без доступу до вихідного коду. Він може бути використаний для сканування віддалених сайтів WordPress в пошуках проблем безпеки.

Сайти, що використовують популярні системи управління контентом, такі як WordPress, мають у своїй основі однаковий вихідний код, скрипти. Цей код вже багаторазово перевірений.

Тобто використання сканерів загального призначення для пошуку, наприклад, SQL-ін'єкцій, XSS та інших популярних вразливостей в WordPress, навряд дасть результати, оскільки це вже багато разів було зроблено до нас.

Проте, дослідники безпеки регулярно знаходять уразливості як в основному коді WordPress, так і в його численних плагінах, темах оформлення. Це означає, що сканувати WordPress потрібно не програмами загального призначення для пошуку вразливостей, а спеціалізованою програмою. Приклад такої спеціалізованого сканеру представлено в роботі.

Для створення веб-сканеру був використаний Flask. Flask - фреймворк для створення веб-додатків мовою програмування Python, що використовує набір інструментів Werkzeug, а також шаблонізатор Jinja2. Відноситься до категорії так званих мікрофреймворков - мінімалістичний каркасів веб-додатків, що свідомо надають лише базові функції.Для розробки вибрана мова Python, так як ця мова набирає обороти в різних сферах, наприклад створення програмного забезпечення в розробці веб –ресурсів також має велику різноманітність модулів для написання різних продуктів.

Список використаних джерел:
1. https://habr.com
2. https://hackware.ru
3. http://www.spy-soft.net
4. https://www.chaitin.cn

ІНФОРМАЦІЙНА СТРУКТУРА ТЕХНОЛОГІЧНОГО ПРОЦЕСУ ЕЛЕКТРОДУГОВОГО НАПИЛЕННЯ

Смірнова Т.В., к.т.н., Дрєєв О.М., к.т.н.,
Смірнов О.А., д.т.н., проф., Солових Є.К. д.т.н., проф.,
Центральноукраїнський національний технічний університет

Актуальність теми дослідження. В даний час будь яка галузь виробництва потребує застосування інформаційних технологій. У даній роботі розглядається інформаційна формалізація структури технологічного процесу електродугового напилення (ЕДН)) для оптимізаційної експертної системи.

Постановка проблеми. Комбінаторна складність технологічного процесу налічує чотири можливих варіанти. Для такої кількості варіантів, є доцільним проведення оптимізації для чотирьох ланцюгів технологічних операцій, з обранням результату, що матиме кращий результат згідно ваговій функції. Проведений аналіз руху інформації при проведені оптимізації технологічного процесу на основі ланцюга технологічних операцій [1-3], виявив потребу в забезпеченні інформаційною системою, що є актуальною задачею.

Метою є формалізація інформаційної структури технологічного процесу електродугового напилення для оптимізаційної експертної системи.

Технологічний процес електродугового напилення в процесі створення виробів із покриттям, а також при відновленні або зміцненні поверхонь деталей, складається з поетапної обробки: струменево-абразивної обробки (САО); при потребі нанесення підшару; основний процес нанесення покриття; доведення утвореної поверхні з покриттям до необхідних розмірів і якості (параметри R_z або R_a) методами механічної обробки (МО), найчастіше чорновим або чистовим шліфуванням та методами поверхнево-пластичної обробки (ППД), а саме обкаткою кульками і роликами, електроконтактною обробкою та інше.

Перший етап призначений для збільшення шорсткості поверхні деталі, на яку наноситься покриття, для отримання необхідної адгезійної міцності (міцності зчеплення) системи «основа-покриття». Підшар має функцію усунення несумісності властивостей основного матеріалу (матеріалу поверхні деталі, на яку наноситься покриття) та матеріалу покриття. Для забезпечення міцності зчеплення системи «основа-покриття» використовують підшар із

XX Всеукраїнська науково-технічна конференція молодих вчених, аспірантів та студентів

“СТАН, ДОСЯГНЕННЯ І ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ”

ОДЕСА
21-22 квітня 2020 р.

Збірник включає доповіді учасників конференції. Тези доповідей публікуються у вигляді, в якому вони подані авторами.

Відповідальність за зміст і форму подачі матеріалу несуть автори статей.

Редакційна колегія: Котлик С.В., Артеменко С.В., Ольшевська О.В.

Комп'ютерний набір і верстка: Соколова О.П.

Відповідальний за випуск: Котлик С.В.