На правах рукопису

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Одеська національна академія харчових технологій
Навчально-науковий інститут холоду,
кріотехнологій та екоенергетики
Факультет інформаційних технологій та кібербезпеки

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

“СТАН, ДОСЯГНЕННЯ І ПЕРСПЕКТИВИ ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ”

Матеріали конференції

Одеса
25–26 квітня 2016 р.

Стан, досягнення і перспективи інформаційних систем і технологій / Матеріали XVI Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Одеса, 25–26 квітня 2016 р. - Одеса, Видавництво ОНАХТ, 2016 р. - 176 с.

Збірник включає матеріали доповідей її учасників, які об'єднані по секціях кафедр: комп'ютерної інженерії (КІ), інформаційних технологій та кібербезпеки (ІТтаКБ).

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

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

Співголови :
Капрельянц Л.В. – д.т.н., проф., проректор з наукової роботи та міжнародних зв′язків,
Косой Б.В. – д.т.н., проф., в.о. директора ННІХКтаЕ ОНАХТ,
Котлик С.В. – к.т.н., доц., декан ФІТта КБ ОНАХТ,
Волков В.Е. – д.т.н., доц., директор ННІМАтаКС ОНАХТ,
Хобін В.А. – д.т.н., проф., завідувач кафедри автоматизації виробничих процесів ОНАХТ,
Невлюдов І.Ш. – д.т.н., проф., завідувач кафедри технології і автоматизації виробництва радіоелектронних і електронно-обчислювальних засобів ХНУРЕ,
Мельник А.О. – д.т.н., проф., завідувач кафедри ЕОМ НУ "Львівська політехніка",
Тарасенко В. П. – д.т.н., проф., завідувач кафедри СПіСКС НТУУ «Київський політехнічний інститут»,
Жуков І. А. – д.т.н., проф., директор інституту комп'ютерних технологій Національного авіаційного університету.

<u>Члени оргкомітету:</u>
Плотніков В. М. – д.т.н., проф., завідувач кафедри інформаційних технологій та кібербезпеки ОНАХТ.
Артеменко С.В. – д.т.н., проф., в.о. завідувача кафедри комп'ютерної інженерії ОНАХТ.
Князєва Н.О. – д.т.н., проф. кафедри комп'ютерної інженерії ОНАХТ.
Грищенко І.В. – к.т.н., заступник декана ФІТта КБ ОНАХТ.
Шамрай О.А. – к.т.н., доц. кафедри ТДтаВЕ ОНАХТ.

Матеріали подано українською, російською та англійською мовами.
Редактор збірника Шамрай О.А.

3. Посилення захисту і контролю над головними розподіляють комп'ютерними базами і електронними центрами.

Необхідна форма проведення дистанційної підготовки до здачі тесту:

1-я фаза. Загальний цикл теоретичної підготовки по заданому предмету.

2-я фаза. Відео інструктаж щодо документального оформлення при здачі тесту.

3-тя фаза. Система тренувальних тестувань на основі попередніх матеріалів із застосуванням балловой системи оцінки.

4-й блок. Психолого-педагогічне консультування учнів осіб та їхніх батьків.

5-й блок. Варіант пробного іспиту за поточним предмету.

Пріоритети розвитку:

1. підвищення рівня освіти;
2. допомога в отриманні вищої освіти;
3. розширення клієнтської бази за рахунок важкодоступних районів;
4. зручність в отриманні необхідної підготовки до здачі іспиту;
5. збільшення інтенсивності підготовки до здачі іспиту.

Важливо: З огляду на все вищевикладене, можна з легкістю сказати про те, що дистанційне навчання, безсумнівно, займе одну з лідируючих позицій серед сучасних освітніх технологій, якщо буде дотримуватися більшості перерахованих пунктів, виходячи з яких, можливо домогтися об'єктивно нового рівня розвитку нинішнього освіти.

Список літератури

1. Бугаков П.Ю. Вибір програмного забезпечення для проведення тестування знань студентів / П.Ю. Бугаков // Актуальні питання освіти. – 2014. – № 1. – С. 124-128.
2. Сорочинський М.А. Реалізація технологій електронного навчання на основі системи iSpring / М.А. Сорочинський // Матеріали Міжнародного молодіжного наукового форуму «ЛОМОНОСОВ-2015» [Електронний ресурс] — М.: МАКС Пресс, 2015. — 1 электрон. опт. диск (DVD-ROM); 12 см. - Систем. вимоги: ПК с процесором 486+; Windows 95; дисковод DVD-ROM; Adobe Acrobat Reader.
3. iSpring. iSpring QuizMaker [Електронний ресурс] – Режим доступу: http://www.ispring.ru/ispring-quizmaker (дата звернення 20.03.16).

РЕКОМЕНДАЦІЇ ЩОДО БЕЗПЕКИ ПРИ КОРИСТУВАННІ ГРОМАДСЬКОЮ WI-FI МЕРЕЖЕЮ

Сом Н.С., студентка ОКР „бакалавр” факультету ІТ та КБ ОНАХТ
Керівник – ст. викл. каф. КІ Бондаренко В.Г.

Інтернет сьогодні є невід'ємною частиною сучасного життя. Неможливо собі уявити, як можна жити без доступу до інтернету. З розвитком бездротових технологій найбільш використовуваним способом доступу в інтернет є техно-

логія Wi-Fi і тепер в мережу можна потрапити з ноутбуків або смартфонів. З точки зору інформаційної безпеки, в бездротових мережах отримати доступ до інформації простіше, ніж в провідних мережах. Практично всі точки доступу Wi-Fi на даний момент підтримують останній стандарт безпеки WPA2. WPA2 - це потужні алгоритми шифрування, надійні механізми цілісності інформації, але часто, громадські мережі не мають пароля для доступу до неї. Такі мережі особливо небезпечні, так як підключитися до неї і переглядати трафік може будь-хто. Найнебезпечнішою загрозою є сніффінг трафіку. Зловмисник стає сполучною ланкою між користувачем і точкою доступу, тобто «встає посередині». Коли користувач відкриває бажану сторінку в інтернеті, правопорушник «перехоплює» дані і відправляє їх далі по мережі. Таким чином, якщо пакет даних буде мати дані до профілю на інтернет-сайті, то людина на стороні їх отримає. Раніше вирішували дану проблему введенням протоколу HTTPS, так як дані, що передаються через нього, шифруються. Але в даний момент, так як технології злому теж не стоять на місці, то можливо їх перехопити і навіть розшифрувати. На жаль, технології шифрування HTTPS не змінювалися, тому на допомогу приходить VPN. Технологія віртуальних приватних мереж Virtual Private Network (VPN) - комплекс технологій, який дозволяє створити віртуальне з'єднання поверх мережі Інтернет. За допомогою мережі нової віртуальної мережі, формується захищений канал, через який передаються всі дані в зашифрованому вигляді. Перехопити ці дані все-таки можливо, але на розшифровку піде досить багато часу. Не кожен хакер буде витрачати його на рядового користувача в соціальній мережі Wi-Fi. З боку користувача в соціальній мережі рекомендується дотримуватися наступних рекомендацій: Відключити загальний доступ до файлів і папок. При використанні публічної мережі Wi-Fi ваші файли і папки, які мають статус загального доступу можуть бути видні всім користувачам, підключеним до даної мережі. Використовувати тільки захищений протокол HTTPS, інакше є ризик перехоплення пакетів даних, в яких міститься сесія, паролі та інша важлива інформація. Даний протокол діє на безлічі сайтів, де можливе введення пароля для доступу до персонального профілю, але не скрізь він є обов'язковим до виконання. Але шанс перехоплення все ж є. Можливе використання VPN, тоді перехоплення пакетів даних повністю виключається. Включити міжмережевий екран. Багато операційних систем оснащені вбудованими міжмережевими екранами (наприклад, Брандмауер Windows). Він підвищить шанс безпеки в мережі за рахунок блокування вхідних і вихідних запитів від додатків. Мати антивірус. Це обов'язковий засіб для захисту комп'ютера. Він допоможе виявити, якщо хтось отримав доступ до системи або здійснює підозрілі дії. Також деякі антивіруси оснащені своїм фаєрволом, що підвищує захист операційної системи. Проблема безпеки в мережах Wi-Fi буде актуальна ще довгий час, так як даний тип бездротового зв'язку все більше входить в наше життя. Постійно з'являються нові точки доступу в кафе, кінотеатрах, університетах, виставках і навіть в районах міста. Якщо немає можливості використовувати протокол HTTPS або технологію VPN, то єдиним виходом буде використання стандартного доступу в Інтернет від стільникового оператора. Для цього

потрібно, щоб смартфон підтримував функцію «Точка доступу», тоді він зможе «роздати» інтернет по Wi-Fi. Таким чином, ви захистите свої дані і будете спокійні за те, що за вами не «підглядають».

Список літератури:

1. Таненбаум Е., Уезеролл Д. Комп'ютерні мережі, 5-е видання, 2012. - 960с.
2. HTTPS // Вікіпедія [Електронний ресурс] – Режим доступу: https://ru.wikipedia.org/wiki/HTTPS (дата звернення 20.03.16).
3. Сніффінг HTTPS трафіку в Wi-Fi і локальних мережах [Електронний ресурс] - Режим доступу: http://forum.antichat.ru/threads/345266/ (дата звернення 20.03.16)
4. Wi-fi sniffing [Електронний ресурс] - Режим доступу: http://help.ubuntu.ru/wiki/wi-fi_sniffing (дата звернення 20.03.16)

ИЗУЧЕНИЕ УПРУГИХ ДЕФОРМАЦИЙ ЗАГОТОВКИ ПО УРОВНЮ ВИБРОАКУСТИЧЕСКИХ КОЛЕБАНИЙ

Спильная Е.А., Соколюк А.В.
Одесский национальный политехнический университет

Поисковые исследования показали, что на уровень виброакустических колебаний существенное влияние оказывают упругие деформации обрабатываемых заготовок. Для учета влияния возможных комбинаций геометрических форм заготовок предложена конструкция заготовки (рис.1) с переменной жесткостью [1].

Рис. 1 Конструкция заготовки с переменной жесткостью (справа) и наладка станка перед обработкой этой заготовки (слева).

В ходе экспериментальных исследований решены следующие задачи:

- установлено влияние режимов фрезерования на виброколебания шпинделя и заготовки;
- установлено влияние переменной жесткости в различных направлениях заготовки на виброколебания элементов технологической системы;
- разработаны предпосылки для создания способа управления колебаниями с учетом индивидуальной жесткости заготовки.

Условия эксперимента: обрабатывающий центр мод. 500V/5 (ЧПУ SIEMENS SINUMERIC 840 D (номинальная и максимальная частоты вращения шпинделя 1500 и 8000 мин$^{-1}$); фреза концевая Ø 18 мм; число зубьев 6 (Р9К5);