АКАДЕМІЯ МИТНОЇ СЛУЖБИ УКРАЇНИ

МІЖНАРОДНА АКАДЕМІЯ КОМП'ЮТЕРНИХ НАУК І СИСТЕМ (ВІДДІЛЕННЯ МАТЕМАТИЧНОГО МОДЕЛЮВАННЯ, ІНФОРМАЦІЙНИХ ТА ТРАНСПОРТНИХ СИСТЕМ І ТЕХНОЛОГІЙ)

ТРАНСПОРТНА АКАДЕМІЯ НАУК УКРАЇНИ (ВІДДІЛЕННЯ ПРОМИСЛОВОГО, МІСЬКОГО, ТРУБОПРОВІДНОГО, НОВИХ ТА НЕТРАДИЦІЙНИХ ВИДІВ ТРАНСПОРТУ)

Семінар "Актуальні проблеми інформаційних та транспортних систем і технологій" під керівництвом академіка Міжнародної академії комп'ютерних наук і систем, академіка Транспортної академії наук України, професора А. М. Пасічника

20.05.2013. **Кравчук С. С.** (Академія митної служби України, Дніпропетровськ). Удосконалення транспортного забезпечення експортно-імпортних вантажопотоків : кандидатська дисертація.

Загострення конкуренції на ринку транспортних послуг обумовлює необхідність пошуку нових форм інтеграції перевізників, митних органів, експедиторів, вантажовласників та інших учасників логістичного ланцюга доставки вантажів для мінімізації витрат часу та ресурсів за одночасного підвищення якості транспортного обслуговування.

У результаті проведеного аналізу досліджень розвитку транспортних вузлів та технічного оснащення залізничних станцій визначено, що в них не враховано: специфіку обробки експортно-імпортного вантажопотоку; особливості роботи та розвиток елементів транспортно-митної інфраструктури; не обговорено питання взаємодії зі співучасниками логістичної системи переміщення вантажопотоку, які виконують контрольні функції.

Центр транспортного сервісу – це система масового обслуговування, переваги якої у тому, що вона складається з окремих підсистем очікування, де утворюється складна мережа причинно-наслідкових технологічних взаємозв'язків з одним або декількома паралельними каналами.

Складність системи в тому, що під час виконання операцій, пов'язаних із прийманням, навантаженням, зберіганням, вивантаженням та видачею вантажів, виникає значна кількість технологічних дій та їх очікування (технічні, комерційні операції, інформаційне супроводження), а міжнародні перевезення зумовлюють взаємозв'язок з іншими системами – митницею та іншими органами державного контролю, термін перебування в яких суттєво впливає на час обслуговування відправки.

Для дослідження функціонування даної системи розроблено імітаційну модель, яка дає можливість проаналізувати стан системи у визначений проміжок часу.

Результатом імітаційного моделювання праці є статистична інформація про: час роботи та простою виконавців (ресурсів), наявність та довжину черги до кожного виду виконавців, час непродуктивного простою заявки в очікуванні виконання операцій, час на обслуговування заявки кожною з передбачених транспортно-технологічною схемою операцій, завантаження системи зберігання та переробки вантажів.

Отримані дані дозволять дослідити систему та проаналізувати основні якісні характеристики її діяльності, знайти шляхи підвищення ефективності роботи окремих виконавців, раціоналізувати логістичні процеси.

23.05.2013. **Кутирєв В. В.** (Східна митниця, Донецьк). Оптимізація місць розміщення ЛТМК на основі факторно-рейтингового аналізу : кандидатська дисертація.

Перший етап завдання визначення оптимальних місць для розміщення логістичних транспортно-митних комплексів (ЛТМК) передбачає проведення розрахунків на основі поєднання двох методик: побудови мережевої моделі, яка враховує обсяги споживання імпортної продукції 250 містами України та відстань між ними для мінімізації транспортної роботи з урахуванням даних факторно-рейтингового аналізу цих міст за такими групами чинників:

– транспортні (наявність автомобільних доріг міжнародного або європейського значення; наявність залізничного сполучення, морського порту, належність міста до системи МТК, наявність у місті вантажного пункту пропуску);

– економічні (середня вартість 1 $м^2$ землі в населеному пункті, інвестиційна привабливість регіону);

– адміністративні (екологічна ситуація, наявність митних постів та відділів митного оформлення).

Проведено факторно-рейтинговий аналіз та визначено найпривабливіші для створення транспортно-логістичних об'єктів міста України з огляду на зазначені фактори, але без урахування взаємного розташування цих міст та вантажопотоків, що через них проходять.

Для виконання поставленого завдання здійснюється розрахунок витрат на утримання та обслуговування ЛТМК за визначений термін для кожного отриманого варіанта, також визначається оптимальний варіант кількості ЛТМК (відповідно, місць їх розташування) шляхом досягнення компромісу між значеннями витрат на утримання і обслуговування та показником сукупної транспортної роботи за однаковий проміжок часу. Виконання цього завдання у повному обсязі дозволить сформувати варіанти оптимального розміщення ЛТМК на території України залежно від їх кількості.

✧ ✧ ✧ ✧ ✧ ✧ ✧

Б. І. Мороз, О. Н. Молотков, С. А. Разгонов

Актуальні завдання підготовки фахівців за напрямом "Управління інформаційною безпекою"

Сучасна концепція забезпечення інформаційної безпеки в митних органах України включає декілька основних напрямків з інформаційної безпеки та технічного захисту інформації (далі – ТЗІ). Зокрема, концепція передбачає організацію технічного захисту інформації, що містить відомості, що є державною або іншою таємницею, яку охороняє закон; забезпечення безпеки інформації за міжнародної та міжвідомчої інформаційної взаємодії, а також інформаційної взаємодії з учасниками зовнішньоекономічної діяльності; експлуатацію сертифікованих засобів криптографічного захисту інформації (далі – КЗІ) та електронного цифрового підпису (далі – ЕЦП), засобів захисту інформації від несанкціонованого доступу (далі – НСД), мережевих екранів, засобів антивірусного захисту інформації, виявлення атак та аналізу рівня захисту, технічних і організаційних заходів щодо захисту персональних даних тощо. Також концепція розвитку митних органів України "Чистий бізнес – чесні податки", оприлюднена у листопаді 2012 р., встановлює новий пріоритет для митниці: починаючи з 2013 р. – це легальний бізнес. У 2012 р. відомство отримало нове митне законодавство (Митний кодекс) і має всі належні повноваження та можливості для того, щоб модернізувати митну систему. Нова концепція розвитку відомства на 2013 р. "Чистий бізнес – чесні податки" забезпечить цивілізований конкурентний ринок та збільшення надходжень до бюджету. Спільна місія бізнесу та митниці – підвищити рівень прозорості ведення підприємництва. Партнерські взаємовідносини платників податків і фіскальних органів – це рушійна сила досягнення балансу інтересів держави та бізнесу.

Нині особливого значення під час реалізації розглянутої концепції набувають питання розвитку інформаційної безпеки, ТЗІ та КЗІ і захисту персональних даних в інформаційно-комп'ютерних системах митних органів. Захист інформації став невід'ємною частиною роботи митних органів України.

Уже зараз українська митниця досягла певних результатів у напрямку побудови електронної митниці, зокрема, введення процедури електронного декларування та захисту інформації. Відповідно до програми розвитку митниці до 2015 р. в усіх митних органах (митницях та постах) має бути впроваджено електронний документообіг (далі – ЕДО) та декларування товарів в електронній формі із застосуванням ЕЦП.

Таким чином, захист даних в інформаційно-комп'ютерних системах та комп'ютерних мережах митних органів України – одна з актуальних і найбільш відкритих проблем.

На сьогоднішній день сформульовано три базові принципи інформаційної безпеки, що забезпечують виконання таких завдань:

1) цілісність даних (захист від збоїв, що призводять до втрати інформації або її знищення);

2) конфіденційність інформації;

3) доступність інформації для авторизованих користувачів.

З огляду на проблеми захисту даних в інформаційно-комп'ютерних системах порушується питання щодо кваліфікації обслуговуючого персоналу та його здатності ідентифікувати категорію комп'ютерного збою та/або ступінь несанкціонованого доступу, а також рівень втрати або зміни даних.

Кваліфіковані користувачі інформаційно-комп'ютерних систем митних органів України повинні вміти оперативно й правильно кваліфікувати порушення доступу до даних, а також визначати збої обладнання (кабельної системи, дискових систем, серверів, робочих станцій тощо), втрати інформації (через інфікування комп'ютерними вірусами, неправильне зберігання архівних даних, порушення прав доступу до даних), збої через некоректну роботу користувачів та обслуговуючого персоналу.

Підвищення ролі захисту інформації в Україні останнім часом пов'язано, зокрема, зі створенням Державного реєстру фізичних осіб – платників податків, об'єднанням Державної митної служби України та Державної податкової служби України в рамках утвореного Міністерства доходів і зборів України, зі зростанням побоювань окремих громадян щодо можливості витоку або втрати інформації, що може призвести до значних фінансових та матеріальних втрат фізичних і юридичних осіб.

Протягом 2012–2013 рр. в Академії митної служби України ведеться активна робота з підготовки до відкриття спеціальності за напрямом "Управління інформаційною безпекою". Необхідність підготовки фахівців зазначеного напряму зумовлена першочерговими завданнями української митниці. Широка інформатизація усіх сторін життєдіяльності суспільства, що передбачає використання комп'ютерних інформаційних технологій, новітніх телекомунікаційних систем, систем зв'язку, входження до світового інформаційного простору, а також розуміння інформаційної незалежності України, спонукає по-новому розглянути проблему захисту інформації про політичний, економічний, науково-технічний, технологічний, військовий та інший потенціали держави від НСД з метою розкрадання, руйнування та цілеспрямованого спотворення, а також від витоку інформації через технічні канали, тому доступ до цієї інформації обмежений.

Інформаційні ресурси держави чи загалом суспільства, а також окремих організацій і фізичних осіб становить певну цінність, мають відповідне матеріальне вираження та потребують захисту від різних впливів, які можуть призвести до зниження цінності інформаційних ресурсів.

Таким чином, розпочата підготовка до відкриття спеціальності за напрямом "Управління інформаційною безпекою" за освітньо-кваліфікаційним рівнем бакалавр є відповіддю на потреби суспільства у виконанні завдань захисту інформації.

Згідно з освітньо-кваліфікаційною характеристикою бакалавра за напрямом підготовки "Управління інформаційною безпекою" спеціаліст повинен уміти: аналізувати інформаційні потоки в комп'ютерних системах та мережах; оцінювати рівень захисту інформації від несанкціонованого доступу і витоку через технічні канали; формулювати й обґрунтовувати вимоги комплексного захисту інформації у таких системах; експлуатувати захищені засоби електронної обчислювальної техніки та технічні засоби захисту, програмно-апаратні та криптографічні засоби захисту інформації у комп'ютерних системах та мережах; розробляти технічні вимоги комплексної системи захисту інформації у комп'ютерних системах та мережах; використовувати та організаційно оформлювати локальні системи комплексного захисту інформації у комп'ютерних системах та мережах; розробляти програмно-апаратні та криптографічні засоби захисту інформації у комп'ютерних системах та мережах; розробляти техніко-економічне обґрунтування комплексного захисту інформації у різноманітних системах та мережах; розробляти технічну документацію на засоби комплексного захисту інформації; здійснювати контроль ефективності захисту інформації у різноманітних системах та мережах від витоку через канали побічних електромагнітних випромінювань і наведень; опановувати наукові дослідження щодо створення сучасних ефективних засобів комплексного захисту інформації у різноманітних системах та мережах; освоювати науково-технічну документацію сучасних засобів комплексного захисту інформації в різноманітних системах та мережах, оцінювати їхню ефективність і реалізовувати в практичній діяльності.

Вирішення проблем захисту інформації потребує системного підходу, освіти з активним використанням у галузях прикладної математики, комп'ютерних наук та прикладної фізики, дослідженнях теоретичних і методологічних проблем формування комплексу знань з питань захисту інформації. Фахівці цього профілю готуються до професійної діяльності зі створення та експлуатації засобів захисту інформації в телекомунікаційних системах різних рівнів, а також захисту мовної інформації від витоку через технічні канали. Спеціаліста слід готувати до професійної діяльності у галузі комплексного захисту інформації від НСД до засобів електронної обчислювальної техніки, автоматизованих систем різного рівня та призначення, банків даних і знань, мереж електронних обчислювальних машин шляхом використання апаратних, програмних, програмно-апаратних, програмно-математичних, криптографічних засобів захисту, а також захисту інформації від витоку через канали побічних електромагнітних випромінювань та наведень за допомогою інженерно-технічних та програмних засобів захисту.

Автори будуть вдячні всім працівникам-практикам, хто, можливо, після знайомства з викладеними матеріалами подасть будь-які пропозиції щодо покращання ефективності підготовки за напрямом "Управління інформаційною безпекою".