УДК 338.246:339.543

А. Д. Войцещук, кандидат економічних наук,
директор Центру підвищення кваліфікації,
перепідготовки працівників та кінології
Міністерства доходів і зборів України

ЗАХИСТ ІНФОРМАЦІЇ В КОМПЛЕКСНІЙ СИСТЕМІ "ЕЛЕКТРОННА МИТНИЦЯ" ЯК ОДНА ЗІ СКЛАДОВИХ ЕКОНОМІЧНОЇ БЕЗПЕКИ ДЕРЖАВИ

Розглянуто механізм захисту інформації в багатофункціональній комплексній системі "Електронна митниця".

Рассмотрен механизм защиты информации в многофункциональной комплексной системе "Электронная таможня".

The mechanism of information protection in the multifunctional complex system "Electronic Customs" is considered in the article.

Ключові слова. Інформаційні технології, захист інформації, багатофункціональна комплексна система, економічна безпека держави, митна безпека держави, "Електронна митниця".

Вступ. Стратегія розвитку суспільства у світі однозначно показує, що перемоги досягають ті структури, які накопичують наявну інформацію та вміло розпоряджаються нею. Збирання й обробка великих обсягів інформації можливі тільки із застосуванням інформаційних технологій, які реалізуються шляхом створення комплексних систем.

Митні відомства зарубіжних країн (Німеччина, Франція, Росія, Японія, Китай, США, Канада та ін.) також активно переходять на сучасні електронні технології. Зокрема, в Японії для електронного декларування використовується автоматизована система NACCS (Nippon Automated Cargo and Port Consolidated System), що об'єднує учасників зовнішньоекономічної діяльності з учасниками митних служб держави. Для оформлення вантажів з використанням такої системи декларантові потрібно лише заповнити зі свого персонального комп'ютера необхідні дані про товар, його найменування, країну походження, контрактну вартість товару, а також вартість транспортування.

У США діє аналогічна система. Американська система АКС (автоматизована комерційна система) є прототипом японської. У країнах ЄС для передачі даних в електронному вигляді використовується система NCTS (New Computerized Transit System). В ЄС електронне декларування товарів обов'язкове. Така система дає можливість декларантам подавати декларації в електронному вигляді до прибуття вантажу, проводити аналіз ризиків та прискорювати обробку даних.

Департамент митної справи Міністерства доходів і зборів України розпочав утілення новітніх технологій у митну справу ще в 1992 р. У 2005 р. почався новий етап розробки принципів побудови системи "Електронна митниця" та її часткової реалізації. Однак організація і проведення цієї роботи потребує єдиного підходу та комплексного вирішення.

Питання щодо впровадження проекту "Електронна митниця" розглядалися Комісією Європейського Союзу [1]. Провідні фахівці О. Г. Жерехов [2], О. В. Слобожанов [3] з'ясували та показали напрямки розвитку застосування інформаційних технологій під час реалізації проекту "Електронна митниця" у митній службі Російської Федерації.

© А. Д. Войцещук, 2013

Вітчизняні дослідники К. О. Євсєєва [4], С. О. Колобов [5], М. Ланг [6], О. О. Ніколайчук [7], М. М. Савостін [8], П. В. Пашко [9, 15–17] розглядають проблеми, що виникають під час упровадження інформаційних технологій, питання побудови Національної системи конфіденційного зв'язку, аналізується європейський досвід у цій сфері.

Постановка завдання. Мета – розглянути механізм захисту інформації в комплексній системі "Електронна митниця" як складову економічної безпеки держави.

Результати дослідження. Для початку з'ясуємо, що таке "Електронна митниця". Електронна митниця (англ. e-Customs) – це багатофункціональна комплексна система, яка існує в митних органах країни й поєднує інформаційно-комунікативні технології та сукупність механізмів їх застосування й дає можливість підвищити якість митного регулювання та вдосконалити митне адміністрування [2].

Автоматизована система "Електронна митниця" має за мету забезпечення митної безпеки держави, тобто її економічної безпеки. Це реалізовується завдяки постійному двосторонньому потоку інформації від суб'єктів ЗЕД, органів державної влади, а також митних адміністрацій інших держав; автоматизації всіх процесів митних процедур – від митного контролю та оформлення вантажів до їх супроводження; інформаційному забезпеченню правоохоронної діяльності та контролю за переміщенням товарів [2].

Крім того, створення такої багатофункціональної комплексної системи спрямовано на адаптацію Єдиної автоматизованої інформаційної системи Департаменту митної справи Міністерства доходів і зборів України та нової комп'ютеризованої транзитної системи ЄС, оперативне отримання актуальної і достовірної інформації про наміри щодо здійснення зовнішньоекономічних операцій, створення умов для прискорення процедур митного контролю й митного оформлення, поліпшення соціального та інформаційного обслуговування населення, удосконалення інформаційної інфраструктури Департаменту митної справи.

Багатофункціональна комплексна система "Електронна митниця" поєднує інформаційно-телекомунікаційні технології та сукупність механізмів їх застосування. Створення зазначеної системи дасть можливість підвищити якість митного регулювання і вдосконалити митне адміністрування.

Основні стратегічні цілі впровадження "Електронної митниці": збирання та захист надходжень до бюджету, захист економіки, захист суспільства, збирання торговельної інформації, кваліфіковане консультування, зміцнення кордонів.

Усього цього можна досягти шляхом удосконалення митного законодавства, політики і процедур, а також прийняття управлінських рішень, які враховують існуючі ризики, спираються на результати дослідження й аналізу цільової інформації і включають фактор підготовки компетентного персоналу.

Застосування інформаційних технологій у митній службі України, створення інформаційного середовища розпочалося, як уже зазначалося вище, в 1992 р. Хронологічно впровадження поділяється на п'ять етапів.

Спочатку це було формування бази даних електронних копій вантажних митних декларацій з паперових примірників та подальшою обробкою і наданням керівництву держави статистичних даних зовнішньоекономічної діяльності.

Протягом 1994–2005 рр. застосовували новітні інформаційні технології, удосконалювалися вже побудовані автоматизовані системи, розвивалися власні інформаційні ресурси. У результаті створено центральну базу даних електронних копій вантажних митних декларацій, автоматизовано процеси контролю доставки вантажів і митного оформлення, формування електронних копій вантажних митних декларацій здійснюється суб'єктами зовнішньоекономічної діяльності, впроваджено відомчу електронну пошту і транспортну мережу супутникового зв'язку, розпочато побудову відомчої телекомунікаційної мережі та комплексної системи захисту інформації.

Розпорядженням Кабінету Міністрів України схвалено Концепцію створення багатофункціональної комплексної системи "Електронна митниця" [10].

Етапи реалізації Концепції:

I – 2009 р. Створення законодавчої основи для застосування інформаційно-телекомунікаційних технологій у роботі контрольних органів, суб'єктів зовнішньоекономічної діяльності; вдосконалення автоматизованих систем, що функціонують у митній службі та базуються на сучасних інформаційно-телекомунікаційних технологіях, які спрямовані на технологічне забезпечення безперервності потоку, накопичення та обробки електронної митної інформації в електронному вигляді, впровадження механізму електронного декларування; забезпечення взаємодії відомчої телекомунікаційної мережі, призначеної для передачі даних, голосу, відеозображення, з іншими аналогічними мережами органів державної влади; забезпечення захисту інформації в інформаційно-телекомунікаційних системах митних органів;

II – 2009–2010 рр. Створення систем:

- адміністрування (в тому числі міжвідомчого) процесів, які відбуваються під час підготовки, прийняття, доведення рішень та контролю за їх виконанням, що є необхідною умовою для мінімізації часу проходження митних процедур (для суб'єктів зовнішньоекономічної діяльності) та раціоналізації дій контрольних органів;
- оперативного виконання рішень, які потребують певних дій щодо товарів і транспортних засобів (огляду, затримання, обмеження руху тощо), що є необхідною умовою для недопущення несанкціонованого поводження з ними;
- електронного цифрового підпису та захисту інформації;
- подальшого вдосконалення програмного забезпечення функціонування механізму електронного декларування (розробка програмного забезпечення, що дасть змогу приймати повідомлення від суб'єктів зовнішньоекономічної діяльності як на рівні центральної бази даних (з подальшим інформуванням відповідного митного органу), так і безпосередньо на рівні митного органу);
- виконання робіт щодо гармонізації документів з вимогами ЄС та забезпечення сумісності системи контролю за переміщенням вантажів з новою комп'ютеризованою транзитною системою ЄС;
- III – 2010–2013 рр. Завершення побудови системи аналізу ризиків як складової частини автоматизованої системи митного оформлення товарів і транспортних засобів на всіх рівнях митної системи; впровадження системи електронного документообігу в усій системі управління митними органами.

Наріжним каменем, на якому базується вищенаведена система, є "Електронна митниця", складовими елементами якої повинні бути такі підсистеми, як: електронне декларування; електронний документообіг; аналіз ризиків і керування ними; контроль за транзитом; єдина міжвідомча автоматизована система збирання, збереження й обробки інформації, в тому числі від різних відомств; автоматизоване здійснення усіх видів державного контролю; уніфікована база нормативних та довідкових документів, які використовуються в митних цілях; інформаційне забезпечення постаудиту та правоохоронної діяльності. Тобто замість придатка до митних процедур вона повинна стати ядром, стрижнем не тільки митних технологій, але ще й інструментом керування та контролю митної діяльності, тобто головним механізмом забезпечення митної справи (рис. 1).

Необхідно змінювати підходи роботи Департаменту митної справи: усі нормативні документи, технології повинні базуватися та будуватися в межах визначеної інформаційної електронної стратегії, а не навпаки.

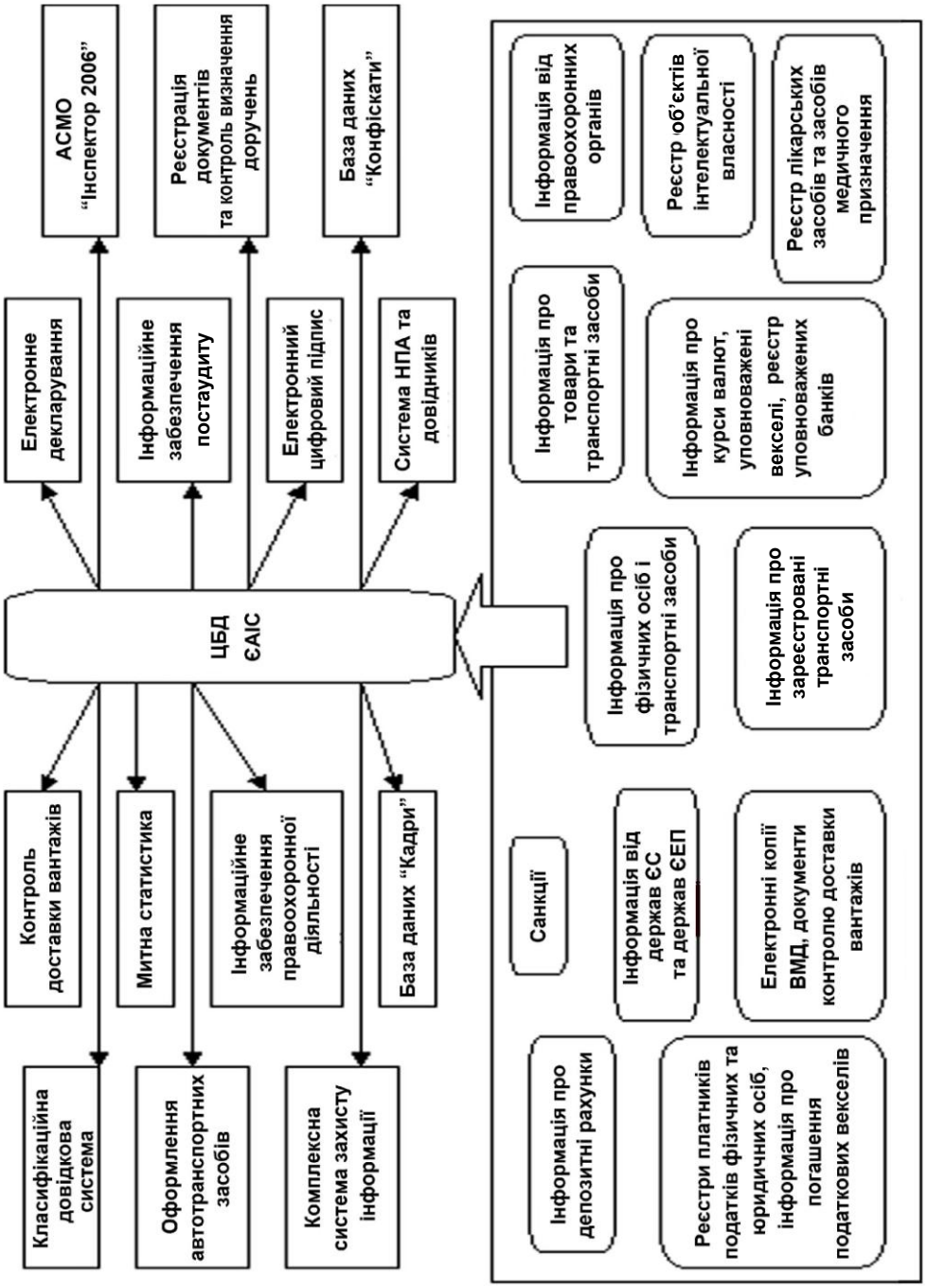

Рис. 1. Інформаційна взаємодія в рамках системи "Електронна митниця"

Об'єднавчий стрижень митниці в подальшому – це інформаційні механізми, тобто запорука посилення авторитету та потужності митниці. Інші шляхи – це крок назад.

Фактично створення та організацію електронного інформаційного середовища в Міністерстві доходів і зборів можна уявити як перехід від інформаційного сховища до інформаційно-довідкової системи, яка, у свою чергу, потребує перетворення на автоматизовану виконавчо-контрольну.

Цю систему має бути створено на нових інформаційних технологіях та відповідній матеріальній базі, яка дозволить побудувати модернізовану багаторівневу систему з відомчою телекомунікаційною мережею, забезпеченою комплексною системою захисту інформації, що потребує тривалого часу та значних капіталовкладень.

З розвитком митної інформаційної інфраструктури зростає актуальність підвищення рівня безпеки всіх її складових. Тому іншою проблемою є захист інформаційних ресурсів від несанкціонованого доступу, забезпечення безпеки інформаційно-телекомунікаційних систем, що активно використовуються у різних сферах суспільного життя й діяльності держави. В умовах глобалізації інформаційна сфера стає як ареною міжнародної співпраці, так і суперництва. Повномасштабне залучення Міністерства доходів і зборів України до процесу формування глобального інформаційного суспільства супроводжується забезпеченням її інформаційної безпеки як одного з найважливіших стратегічних завдань безпеки національної. Актуальність даної проблеми багато в чому обумовлено зростанням "кіберзлочинності" і розширенням можливостей міжнародного тероризму з використанням сучасних інформаційних технологій для здійснення терористичних актів.

В умовах глобалізації інформаційних технологій об'єктом інформаційної злочинності стає весь світовий інформаційний простір у цілому і кожний його елемент зокрема. Нейтралізувати наслідки протиправних дій в інформаційній сфері, наприклад, інформаційного тероризму, надзвичайно важко, а іноді взагалі неможливо. Усвідомивши небезпеку, породжену глобалізацією інформаційних технологій, і розуміючи, що прогрес суспільства не можна зупинити, слід зосередитися на підтримці позитивних і нейтралізації негативних особливостей розвитку інформаційних технологій.

Проблема захисту інформації виникла давно, ще в умовах централізованої обробки інформації із застосуванням великих ЕОМ, але свого критичного стану вона досягла разом з "комп'ютерним бумом". Потреба захисту інформації зумовлена децентралізацією її обробки, полегшенням доступу до неї завдяки комп'ютерним мережам, необхідністю збереження комерційної таємниці. Захист інформації в комп'ютерному середовищі – проблема складна і багатогранна.

Мотиви у зловмисників можуть бути різні: нажива, хуліганство, бажання слави, проте всі зловмисники діють приблизно однаково. Існує ряд основних загроз, кожна з яких може мати нескінченну кількість варіацій.

Підробка. Існує кілька різновидів цієї загрози. Підробка IP-адрес передбачає створення пакетів, що мають адресу відправника, відмінну від справжньої. Даний метод використовується в основному для односторонніх атак (наприклад, атак типу "відмова в обслуговуванні"). Якщо пакети надходять від комп'ютера в локальній мережі, вони проходять повз брандмауер (який призначений для захисту від зовнішніх загроз). Атаки з підміною IP-адрес складно виявити. Це потребує знань і засобів, необхідних для відстеження й аналізу пакетів даних. Підробка повідомлень електронної пошти – це зміна адреси в полі "Від" повідомлення. Наприклад, у кінці 2003 р. в мережі циркулювали листи-містифікації, що містили повідомлення про офіційні оновлення системи безпеки, що нібито розсилалося корпорацією Майкрософт (зловмисники використовували підроблену адресу електронної пошти).

Викривлення. Викривленням називається зміна вмісту пакетів, що передаються через Інтернет, або зміна даних на дисках комп'ютерів після проникнення зловмисника в локальну мережу. Наприклад, зловмисник може зламати мережний канал для перехоплення пакетів, що надходять від організації. Це дозволить йому перехоплювати або змінювати відомості, передані з локальної мережі.

Невизнання. Невизнанням називається здатність користувача заперечувати факт здійснення будь-якої дії, яку він насправді вчинив. Користувач, що видалив файл, може цього не визнати, якщо не існує механізму для доказу (наприклад, записи аудиту).

Розкриття інформації. Розкриттям інформації називається надання інформації особам, що у звичайних умовах не мають до неї доступу.

Відмова в обслуговуванні. Атакою типу "відмова в обслуговуванні" називається комп'ютерна атака, проведена з метою перевантаження або зупинки мережної служби, наприклад, файлового або веб-сервера. Атака може викликати таке перевантаження сервера, що він припинить обробляти звичайні запити на підключення. У 2003 р. відбулися масштабні атаки типу "відмова в обслуговуванні" на сервери декількох великих корпоративних вебвузлів, у тому числі Yahoo та Microsoft.

Підвищення привілеїв. Підвищенням привілеїв називається процес незаконного отримання повноважень шляхом "обману" системи, зазвичай з метою компрометації або руйнування цієї системи. Наприклад, зловмисник може виконати вхід у мережу під обліковим записом гостя, а потім використати вразливість у програмному забезпеченні для отримання повноважень адміністратора.

Обчислювальну потужність комп'ютерів більшість зловмисників використовують як зброю. Наприклад, за допомогою вірусу вони можуть поширити програму для атак типу "відмова в обслуговуванні" на сотні тисяч комп'ютерів. Вони можуть скористатися програмою автоматичного підбору пароля за словником. Звичайно, спочатку вони перевірять варіанти "password", "sezam" тощо, а також ім'я користувача, введене у функції пароля. Зловмисники мають у своєму розпорядженні програми, що випадково перевіряють IP-адреси в Інтернеті для виявлення незахищених систем. Виявивши таку систему, зловмисник може скористатися сканером портів для визначення портів, відкритих для атаки. Потім він спробує одержати доступ до системи за допомогою бібліотеки відомих вразливостей. Для витонченіших атак (таких, як промислове шпигунство) максимально ефективним засобом може виявитися комбінація технічних засобів і "соціальної інженерії". Такі атаки можуть включати отримання конфіденційних відомостей у співробітників, перегляд утиліт у пошуках потрібної інформації або застосування паролів, написаних на папірцях, прикріплених до моніторів.

Висновки. Отже, на сучасному етапі на всіх рівнях державного управління потрібно глибоко усвідомити, що формування, поширення, використання й захист інформаційних ресурсів Департаменту митної справи Міністерства доходів і зборів України є основою забезпечення її національних інтересів в інформаційній сфері, становлення й розвитку інформаційного простору та його інтегрування у світовий інформаційний простір.

Для запобігання інформаційним загрозам має бути розроблено чіткий план, який відображатиме персональну відповідальність кожного працівника, починаючи з технічного персоналу й закінчуючи вищою керівною ланкою. У плані мають визначатися також заходи щодо відновлення інформаційних ресурсів після їх ураження. Ці процедури слід постійно перевіряти. Розробці плану мусить передувати аналіз усіх інформаційних масивів та потоків інформації (як внутрішніх, так і зовнішніх). Практика свідчить, що ефективний комплексний аудит можливий лише за участі сторонньої спеціалізованої організації, яка має відповідну

ліцензію на проведення такої діяльності. Останнім етапом щодо захисту інформації є страхування інформаційних ресурсів як від традиційних, так і від кіберзагроз.

Таким чином, надійність програмного забезпечення пов'язана не тільки із засобами його створення, але й із виникненням різних аварійних і позаштатних ситуацій під час експлуатації, які викликані зовнішніми обставинами: перепади напруги в мережі, збій у роботі вузлів комп'ютерної системи (наприклад, вихід із ладу центрального процесора, обривання мережного кабеля, механічне пошкодження носіїв інформації).

Література

1. Многолетний Стратегический План [Электронный ресурс] TAXUD/477/2004 – Версия 7 – EN, Інтернет-видання, сайт митної організації Європейського Союзу. – Режим доступа : http://www.revenue.ie.

2. Жерихов О. Е. О состоянии и задачах таможенных органов Российской Федерации на ближайшую перспективу с учетом их ресурсного обеспечения [Електронний ресурс] : доповідь керівника Федеральної митної служби Росії, 2006. Інтернет-видання, сайт Федеральної митної служби Росії. – Режим доступу : http://www.customs.ru.

3. Слобожанок В. А. На пути к электронной таможне / В. А. Слобожанок // Таможня. – 2006. – № 7 (150). – С. 8–11.

4. Євсєєва К. О. Електронна митниця як один із напрямів удосконалення митної логістики на підприємстві [Електронний ресурс]. – Режим доступу : http: //www. rusnauka. com/ 18_DNI_2010/Economics/69555.doc.htm.

5. Колобов С. О. Інфраструктура захисту інформаційних ресурсів на основі Національної системи конфіденційного зв'язку [Електронний ресурс] : доповідь на другій науково-практичній конференції "Безпека сучасних інформаційних та телекомунікаційних систем", 2005. – Інтернет-видання, сайт Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. – Режим доступу : http://www.dstszi.gov.ua.

6. Ланг М. Обзор подходов Европейского Союза к вопросу построения инфраструктуры открытых ключей [Електронний ресурс] / М. Ланг : доповідь на другій науково-практичній конференції "Безпека сучасних інформаційних та телекомунікаційних систем", 2005. – Інтернет-видання, сайт Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. – Режим доступу : http://www.dstszi.gov.ua.

7. Ніколайчук О. О. Електронне декларування, шляхи вирішення / О. О. Ніколайчук // Митниця. – 2006. – № 5 [19]. – С. 13–15.

8. Савостін М. М. Електронне декларування – шлях до вдосконалення та реформування митної справи в Україні [Електронний ресурс] / М. М. Савостін. – Режим доступу : http://www.nbuv.gov.ua/portal/soc_gum/vsunu/2012_14_1/ Savostin.pdf.

9. Митні інформаційні технології : навч. посіб. ; за ред. П. В. Пашка. – К., 2011. – 391 с.

10. Про схвалення Концепції створення багатофункціональної комплексної системи "Електронна митниця" : розпорядження Кабінету Міністрів України від 17 вересня 2008 р. № 1236-р.