

**МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ
КРЕМЕНЧУЦЬКИЙ ЛЬОТНИЙ КОЛЕДЖ**

Циклова комісія економіки та управління

ТЕКСТ ЛЕКЦІЙ

навчальної дисципліни «Логістичний інжиніринг»
вибіркових компонент
освітньо-професійної програми
першого (бакалаврського) рівня вищої освіти

Логістика

за темою - Системна інформаційна підтримка життєвого циклу виробів

Харків 2022

ЗАТВЕРДЖЕНО

Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 30.08.2022 № 8

СХВАЛЕНО

Методичною радою
Кременчуцького льотного
коледжу
Протокол від 22.08.2022 № 1

ПОГОДЖЕНО

Секцією науково-методичної ради
ХНУВС з гуманітарних та соціально-
економічних дисциплін
Протокол від 29.08.2022 № 8

Розглянуто на засіданні циклової комісії економіки та управління,
протокол від 15.08.2022 № 1

Розробник: викладач циклової комісії економіки та управління, спеціаліст другої категорії, Черніхова О.С.

Рецензенти:

1. Старший викладач циклової комісії економіки та управління КЛК ХНУВС, к.е.н., спеціаліст вищої категорії, викладач – методист, Цимбалістова О.А.
2. Професор кафедри логістики НАУ, доктор економічних наук, професор, експерт Українського логістичного альянсу (УЛА) Смерічевська С.В.

План лекцій:

1. Захист інформації.
2. Заходи безпеки.
3. Безпаперове представлення інформації та використання електронно-цифрового підпису.
4. Вимоги законів України щодо використання електронно-цифрового підпису.

Ключові терміни: безпека інформаційних систем, загроза безпеки інформації, програмні, апаратні засоби, комплексна система управління, системний підхід, засоби безпеки, сертифікат відкритого ключа, цифровий підпис

Рекомендована література:

Основна

1. Григорак М. Ю. Логістичний інжиніринг : навч. посіб. для студ. ВНЗ, які навчаються за напрямом підготовки "Менеджмент" та "Транспортні технології" / М. Ю. Григорак, В. Є. Марчук, О. Й. Косарєв, Ю. С. Ремига, В. І. Калініченко; Нац. авіац. ун-т. - К. : НАУ, 2011. - 322 с.
2. Blanchard, B. S. Logistics Engineering and Management / Blanchard, B. S. : 4th Edition, Prentice-Hall, Inc., Englewood Cliffs, NJ, 1992.
3. Глогусь О. Логістика: Навч. посіб. - Тернопіль: Екон. думка, 2006. - 332с.
4. Грищенко І.М. Маркетингові основи комерційного посередництва: Навч. посібник. К.: КНУТД, 2006. – 304 с.
5. Дудар Т.Г., Волошин Р.В., Основи логістики, Центр навчальної літератури, 2012. - 176 с.
6. Забуранна Л.В. Логістичне управління підприємством: сутність та передумови розвитку /Л.В. Забуранна // Сталій розвиток економіки. – 2010. – № 7. – С. 120–123
7. О. Хромов Логістика, Видавництво – Бурун Книга, 2012 – 224 с.
8. Пономаренко В.С. Логістичний менеджмент: підручник / В.С. Пономаренко, К.М. Таньков, Т.І. Лепейко. - Харків : Інжек, 2010.-440 с.
9. Пономарьов Ю.В. Логістика: Навчальний посібник. / Ю.В. Пономарьов - К.: Центр навчальної літератури, 2008.- 478с.

Допоміжна

10. Ремонт повітряних суден та авіаційних двигунів [Кудрін А.П., Зайвенко Г.М., Волосович Г.А., Хижко В.Д.] : Підручник. – К.: НАУ, 2002. – 492 с.

Інформаційні ресурси в Інтернеті

11. <http://barhan.poll/ava.ua/marek> – розділ маркетинг і реклама: теорія практичні поради;
12. <http://www.customs.gov.ua> - Державна митна служба України.
13. <http://www.dssu.gov.ua> - Державний комітет України з питань технічного регулювання та споживчої політики.
14. <http://www.obriy-marketing.kiev.ua> – маркетинг для ефективного просування на ринку товарів і організацій (Обрій-маркетинг).
15. <http://udc.com.ua/> – проект про бізнес-технології, головні теми: кооперація, системи управління якістю, маркетинг і Internet, дисконтна програма.
16. <http://www.i2.com.ua> – Бібліотека інтелектуальні системи прогнозування: фінанси, валюта, економіка, маркетинг, менеджмент, цінні папери, біржі.

Текст лекції

1. Захист інформації

Захист інформації на потрібному рівні можливий лише за умови комплексного вжиття взаємодоповнюючих заходів, а саме:

- нормативно-правових;
- адміністративних;
- спеціального обладнання та програмного забезпечення.

Використання систем захисту інформації не приносить прибутку, але її відсутність може стати причиною значних збитків за рахунок:

- втрати конфіденційності;
- втрати даних;
- відмови системи в обслуговуванні користувачів;
- втрати репутації.

Виконувати функції відносно заходів безпеки на підприємствах можуть:

- керівники підприємств;
- відділи інформаційної безпеки;
- ІТ-менеджери;
- системні адміністратори.

Незважаючи на те, що політика безпеки повинна розроблятися індивідуально для кожної системи, є низка рекомендацій щодо організації захисту в довільній системі.

Ці рекомендації наведені в документі RFC 2196 "Site Security Book" (інструкція з безпеки систем), що є частиною документів RFC (Request for Comment), в яких визначаються стандарти і процедури для Інтернет.

Політика безпеки - це формальний виклад правил, яких повинні дотримуватись особи, що отримують доступ до корпоративних технологій та

інформації.

У відповідності до RFC 2196 виділяють чотири етапи формування політики безпеки:

1. Реєстрація всіх ресурсів, які повинні бути захищені
2. Аналіз та створення списків можливих загроз для кожного ресурсу
3. Оцінка ймовірності появи кожної загрози
4. Прийняття рішень, які дозволять економічно ефективно захистити інформаційну систему.

Інформаційні системи наражені на такі загрози:

- несанкціонований доступ;
- ненавмисне розкриття інформації;
- різні види атак, що дозволяють проникнути в мережу або перехопити управління нею;
- комп'ютерні віруси;
- логічні бомби;
- засоби пригальмовування передавання даних;
- природні катаклізми та стихійні лиха.

Вартість засобів захисту не повинна перевищувати втрат, до яких може спричинити ця загроза, зокрема витрат на відновлення інформації.

2. Заходи безпеки

Сервіс безпеки - це сукупність механізмів, процедур та інших заходів управління для зменшення ризиків, пов'язаних із загрозою втрати або розкриття даних.

Одні сервіси забезпечують захист від загроз, інші - виявляють слабкі місця в системі безпеки.

Основними сервісами безпеки є:

- сервіс аутентифікації;
- сервіс конфіденційності;
- сервіс цілісності;
- сервіс дотримання зобов'язань.

Аутентифікація користувача передбачає два кроки:

- 1) ідентифікацію - уведення імені, під яким користувач зареєстрований в системі;
- 2) верифікацію - уведення пароля, присвоєного даному користувачу.

Останнім часом великого розповсюдження набули системи біометричної аутентифікації.

Конфіденційність означає, що доступ до інформації може бути наданий лише тим користувачам, які мають на це право.

Сервіс цілісності даних забезпечує захист від навмисної чи випадкової зміни даних. Він дозволяє виявити факт зміни, часткового вилучення або доповнення даних.

Сервіс дотримання зобов'язань гарантує, що учасники інформаційного обміну не можуть заперечити факт своєї участі в ньому.

Виділяють чотири основних механізми порушень безпеки даних:

- роз'єднання, коли порушується доступність даних;
- перехоплення, що спричиняє порушення конфіденційності даних;
- модифікація, що призводить до порушення цілісності;
- фальсифікація.

Ускладнити чи унеможливити читання даних сторонніми особами дозволяє шифрування даних.

Шифрування - це перетворення даних у форму, яка не дає можливості безпосереднього сприйняття зашифрованої інформації.

Шифрування здійснюється з використанням криптографічного ключа.

З використанням ключа здійснюється і зворотна процедура - дешифрування (повернення інформації до первинного вигляду).

Методи криптографії (шифрування) даних - симетричний та асиметричний. Якщо відправник і отримувач користуються одним і тим же ключем, то говорять про симетричну криптографію. Асиметрична криптографія передбачає використання двох різних ключів.

Розрізняють відкриті і таємні ключі. При цьому таємний ключ використовується або на стороні отримувача, або на стороні відправника.

Якщо таємний ключ використовується для шифрування інформації (на стороні відправника), то говорять про цифровий підпис.

Ключ - це набір символів, сформований довільним чином з доступних у системі шифрування символів. Довжина такого ключа може коливатись від 16 до 128 біт.

3. Безпаперове представлення інформації та використання електронно-цифрового підпису

Всі процеси інформаційного обміну за допомогою ІВС мають своєю кінцевою метою максимально можливе виключення з ділової практики традиційних паперових документів і перехід до прямого безпаперового обміну даними.

На перехідному періоді потрібно забезпечити співіснування і спільне використання як *паперової*, так і *електронної форм представлення інформації* і гармонізувати застосовуються поняття.

Термін	Визначення
БД про виріб	сховище інформації, необхідної для випуску конструкторської документації, необхідної на всіх стадіях життєвого циклу виробу [Р50.1.031-2001]
Електронний конструкторський документ (ЕКД)	структурований набір даних, необхідних для розробки, виготовлення, контролю, приймання, експлуатації і ремонту, забезпечений заголовком і підписаний електронно-цифровим підписом (ЕЦП)

Екранне уявлення даних	відображення конструкторської інформації на екрані комп'ютера у формі, яка сприймається людиною
Паперовий конструкторський документ	графічний і (або) текстовий документ, що містить дані, необхідні для розробки-ки, виготовлення, контролю, приймання, експлуатації і ремонту [ГОСТ 2.102-93]

Інформація може бути представлена:

- у формі бази даних;
- в формі електронного конструкторського документа;
- в формі, придатній для сприйняття людиною - паперовій або екранній.

Подання інформації в формі бази даних використовується при необхідності логічного структурування великих обсягів інформації. При цьому дані певним чином розподіляються між таблицями бази даних, записами в таблицях, полями в записах (при використанні реляційної СУБД) і (або) окремими файлами і таблицями (при використанні об'єктно-орієнтованої СУБД). Використовувані структури даних орієнтовані на специфіку вирішуваних завдань.

Іншою формою подання інформації ***є електронний документ*** - структурований набір даних, що включає в себе заголовок, змістовну частину і електронно-цифровий підпис.

Електронний документ використовується в якості форми представлення результатів роботи, призначеної для передачі з однієї автоматизованої системи в іншу або подальшої візуалізації.

Обидві форми подання інформації - ***у формі бази даних*** (внутрішнє подання інформації в комп'ютерній системі) і ***у формі електронного документа*** - не придатні для сприйняття людиною і вимагають для спеціальних програмних засобів візуалізації, тобто перетворення даних в паперовий документ або в екранну форму.

Існуючі стандарти, що регламентують конструкторсько-технологічну діяльність, такі як ЕСКД, ЕСТД, СРПП і їм подібні, стосуються тільки візуальної форми подання інформації. Тому одним із першочергових практичних завдань впровадження CALS є розвиток стандартів ЕСКД і вироблення нових стандартів і специфікацій, що регламентують електронну форму подання та обігу даних.

Процедура електронно-цифрового підпису (ЕЦП) заснована на математичних принципах так званих "систем з відкритим ключем".

У формування підпису використовується індивідуальне число (закритий ключ) користувача, яке породжується за допомогою генератора випадкових чисел і зберігається користувачем в секреті весь час його дії.

Для перевірки справжності цифрового підпису застосовується інше число, так званий "відкритий ключ перевірки цифрового підпису" (або коротко - "відкритий ключ"), який за відомим алгоритмом обчислюється з індивідуального закритого ключа і надається всім, кому це необхідно для перевірки справжності цифрового підпису.

ЕЦП є математичну функцію (hash) від вмісту підписуються даних (data) і

секретного ключа автора (*secret_key*), яка обчислюється за стандартизованого алгоритму:

Sign = h (data, secret_key)

В результаті обчислення хеш-функції формується пара чисел - префікс і суфікс електронно-цифрового підпису. Байтові уявлення отриманих чисел, записані один за одним, оголошуються цифровим підписом.

Для перевірки справжності підписів повинні використовуватися відкриті ключі, якими учасники процесу спільної роботи з даними повинні обмінятися один з одним. Однак при великій кількості учасників така процедура може виявитися організаційно і технічно складною. Одним з можливих рішень є використання *сертифікатів* ключа.

Довірена особа приймає на себе функції *центру сертифікації ключів*, тобто формує для кожного відкритого ключа пакет даних, що містить власне відкритий ключ і дані про його власника (ім'я, посада і т.д.) і підписує його власним ЕЦП.

Такий пакет даних називається *сертифікатом ключа*.

В результаті утворюється *ланцюжок сертифікатів* від ключа перевірки підпису кінцевого користувача до самого верхнього (головного) *центру сертифікації* (ЦС), в якій авторство підпису на попередньому сертифікаті засвідчується наступним сертифікатом.

Сертифікати не містять в собі ніякої конфіденційної інформації, можуть поширюватися у відкритому вигляді по мережах передачі даних або приєднуватися до підписаних даними.

Процедура перевірки справжності підпису включає в себе наступну послідовність кроків.

1. ЕЦП підпису виділяються її префікс і суфікс.
2. З використанням процедури хешування і відкритого ключа обчислюється значення, яке має бути префіксом ЕЦП.
3. Обидва отриманих значення порівнюються.

Якщо вони збігаються, то дані вважаються справжніми. Якщо отримані значення не збігаються, підпис вважається недійсною.

Таким чином, для перевірки підпису необхідний відкритий ключ або його сертифікат. Використання сертифіката краще, оскільки він містить не тільки відкритий ключ, але і дані про автора.

4. Вимоги законів України щодо використання електронно-цифрового підпису

Закон України "Про електронні довірчі послуги" ВВР, 2017, № 45.

Цей Закон визначає правові та організаційні засади надання електронних довірчих послуг, у тому числі транскордонних, права та обов'язки суб'єктів правових відносин у сфері електронних довірчих послуг, порядок здійснення державного нагляду (контролю) за дотриманням вимог законодавства у сфері електронних довірчих послуг, а також правові та організаційні засади

здійснення електронної ідентифікації.

Метою Закону є врегулювання відносин у сферах надання електронних довірчих послуг та електронної ідентифікації.

Відносини, пов'язані з наданням електронних довірчих послуг та електронною ідентифікацією, регулюються:

- Конституцією України,
- Цивільним кодексом України,
- Законом України "Про інформацію",
- Законом України "Про захист інформації в інформаційно-телекомунікаційних системах",
- Законом України "Про електронні документи та електронний документообіг",
- Законом України "Про захист персональних даних",
- іншими нормативно-правовими акти.

Суб'єктами правових відносин у сфері послуг електронного цифрового підпису є:

- 1) підписувач;
- 2) користувач;
- 3) центр сертифікації ключів;
- 4) акредитований центр сертифікації ключів;
- 5) центральний засвідчувальний орган;
- 6) засвідчувальний центр органу виконавчої влади або іншого державного органу (далі - засвідчувальний центр);
- 7) контролюючий орган.

Електронний цифровий підпис за правовим статусом прирівнюється до власноручного підпису (печатки) у разі, якщо:

- електронний цифровий підпис підтверджено з використанням посиленого сертифіката ключа за допомогою надійних засобів цифрового підпису;
- під час перевірки використовувався посилений сертифікат ключа, чинний на момент накладення електронного цифрового підпису;
- особистий ключ підписувача відповідає відкритому ключу, зазначеному у сертифікаті.

Електронний цифровий підпис призначений для забезпечення діяльності фізичних та юридичних осіб, яка здійснюється з використанням електронних документів.

Електронний цифровий підпис використовується фізичними та юридичними особами - суб'єктами електронного документообігу для ідентифікації підписувача та підтвердження цілісності даних в електронній формі.

Використання електронного цифрового підпису не змінює порядку підписання договорів та інших документів, встановленого законом для вчинення правочинів у письмовій формі.

Нотаріальні дії із засвідчення справжності електронного цифрового підпису на електронних документах вчиняються відповідно до порядку, встановленого законом.

Сертифікат ключа містить такі обов'язкові дані:

- найменування та реквізити центру сертифікації ключів (центрального засвідчувального органу, засвідчувального центру);
- зазначення, що сертифікат виданий в Україні;
- унікальний реєстраційний номер сертифіката ключа;
- основні дані (реквізити) підписувача - власника особистого ключа;
- дату і час початку та закінчення строку чинності сертифіката;
- відкритий ключ;
- найменування криптографічного алгоритму, що використовується власником особистого ключа;
- інформацію про обмеження використання підпису.

Питання для самоконтролю:

1. Вітчизняні засоби захисту інформації.
2. Рівні захисту інформаційної безпеки.
3. Типи методів забезпечення інформаційної безпеки.
4. Характеристика електронного підпису.