# Навчання з IT-аудиту
# День 3

*Київ, грудень 2017*

Манфред ван Кестерен
Яспер Венеман

National Academy for Finance and Economics
*Ministry of Finance*


- Початок - 10.00
- Перерва на каву 11:20-11:40
- Продовження роботи 11:40-12:15
- Підведення підсумків і остаточні запитання 12:15-12:30
- Вручення сертифікатів і закриття 12:30-13:00
- Перерва на обід 13:00 – 13:30

# Порядок денний  - Автоматизовані інструменти аудиту (CAATS)

- Інструменти для аналізу даних
  - Витягування інформації про процеси
  - Аналіз автоматизованих даних за допомогою Splunk
    - Інформація про мережу та сервер в режимі реального часу з панеллю приладів Splunk
    - Аналіз журналів
- Інструменти для IT-безпеки
  - Центр для інтернет-безпеки
  - Оцінити якість цифрових сертифікатів
  - Перевірити комп'ютери на предмет спільних неправильних конфігурацій безпеки
  - Бонус

# Інструменти IT-аудиту

- Навіщо потрібні інструменти?

- Ефективність
  - Можна дуже швидко зробити аналіз великих даних
  - Більше тестів можна провести за мінімальний час

- Результативність
  - Легше розпізнавати (потенційні) ризики
  - Використовувати як один з інструментів аудиту, поряд зі збором даних з інтерв'ю та документів.

# Модель мислення для IT-систем

(Веб) застосунок (файли)

Проміжне програмне забезпечення (PHP, ASP, Python)

Веб-сервер (Apache, IIS)

Сервер бази даних(MySQL)

Операційна система (Linux, Unix, Windows)

Мережа (Міжмережевий екран, вирівнювач навантаження, проксі)

Комп'ютерне обладнання (прошивка, процесор, пам'ять і жорсткий диск)

# Інструменти IT-аудиту

- Аналіз даних
  - Інструменти: Excel, IDEA, ACL, Splunk і Disco





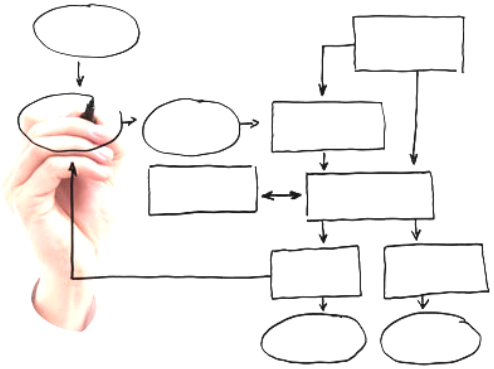
- Постійне проведення аудиту і моніторинг

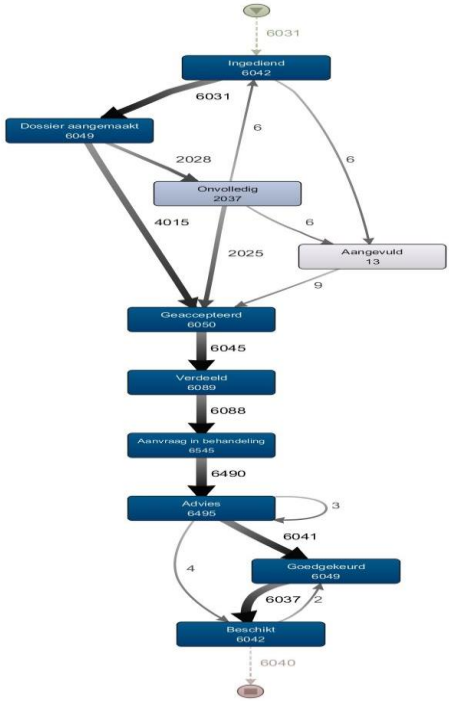
# Порядок денний

- **Інструменти для аналізу даних**
  - Витягування інформації про процеси
  - Аналіз автоматизованих даних за допомогою Splunk
    - Інформація про мережу та сервер в режимі реального часу з панеллю приладів Splunk
    - Аналіз журналів
- Інструменти для IT-безпеки
  - Центр для інтернет-безпеки
  - Оцінити якість цифрових сертифікатів
  - Перевірити комп'ютери на предмет спільних неправильних конфігурацій безпеки
  - Бонус

# Інструменти для аналізу даних: Витягування інформації про процес

- Витягування інформації про процес – це прийом управління процесом, що дозволяє аналіз бізнес-процесів на основі журналу подій
(джерело: вікіпедія)





# Витягування інформації про процес

- Вам потрібні дані про події з однієї прикладної програми із щонайменше:
  - Унікальним ідентифікатором
  - Позначкою часу
  - Назвою дії

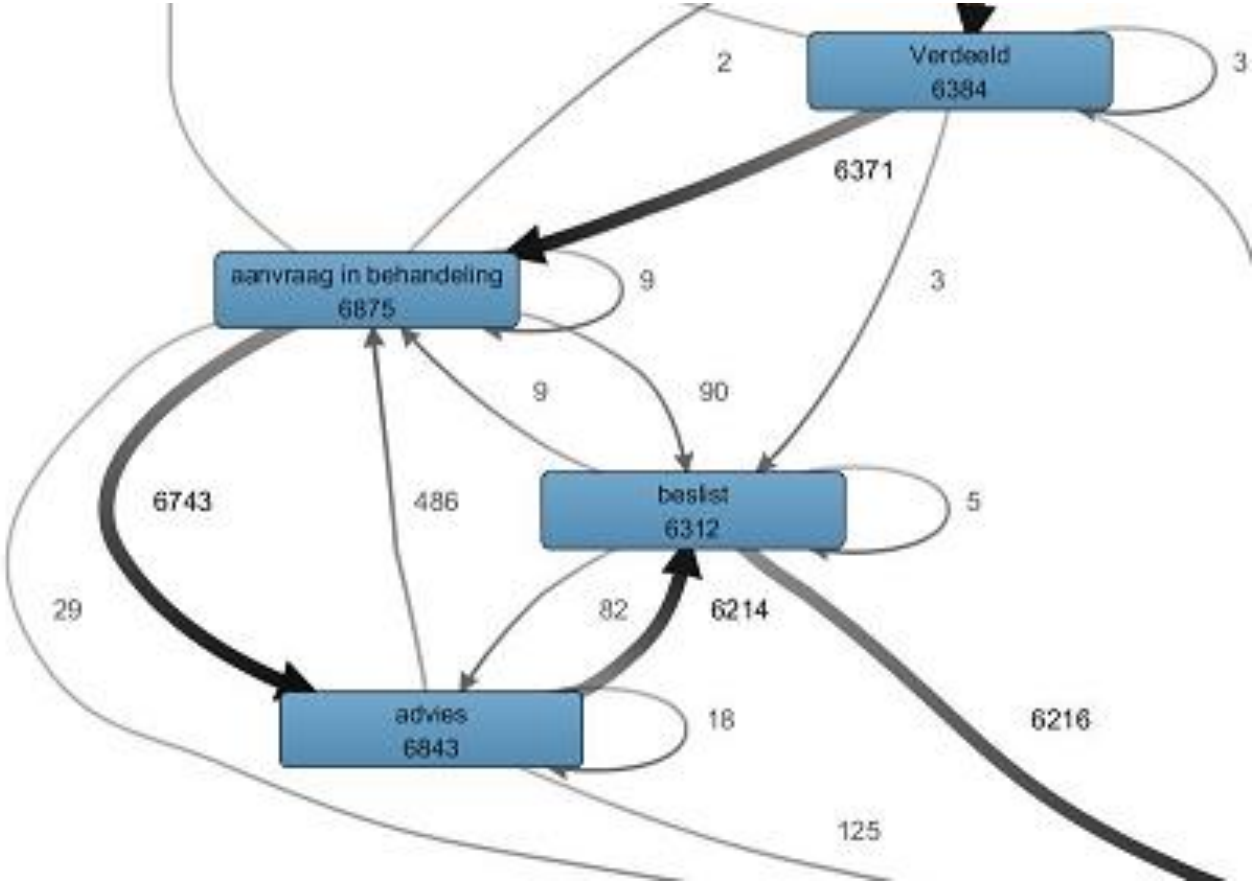
- Два приклади інструментів витягування інформації про процеси:
  - ProM: безкоштовне і відкрите джерело.
  - Disco: графічний і легкий для розуміння.
- Підказка: почитайте Coursera (технологічна компанія) з цього питання: Наука даних в дії

Disco

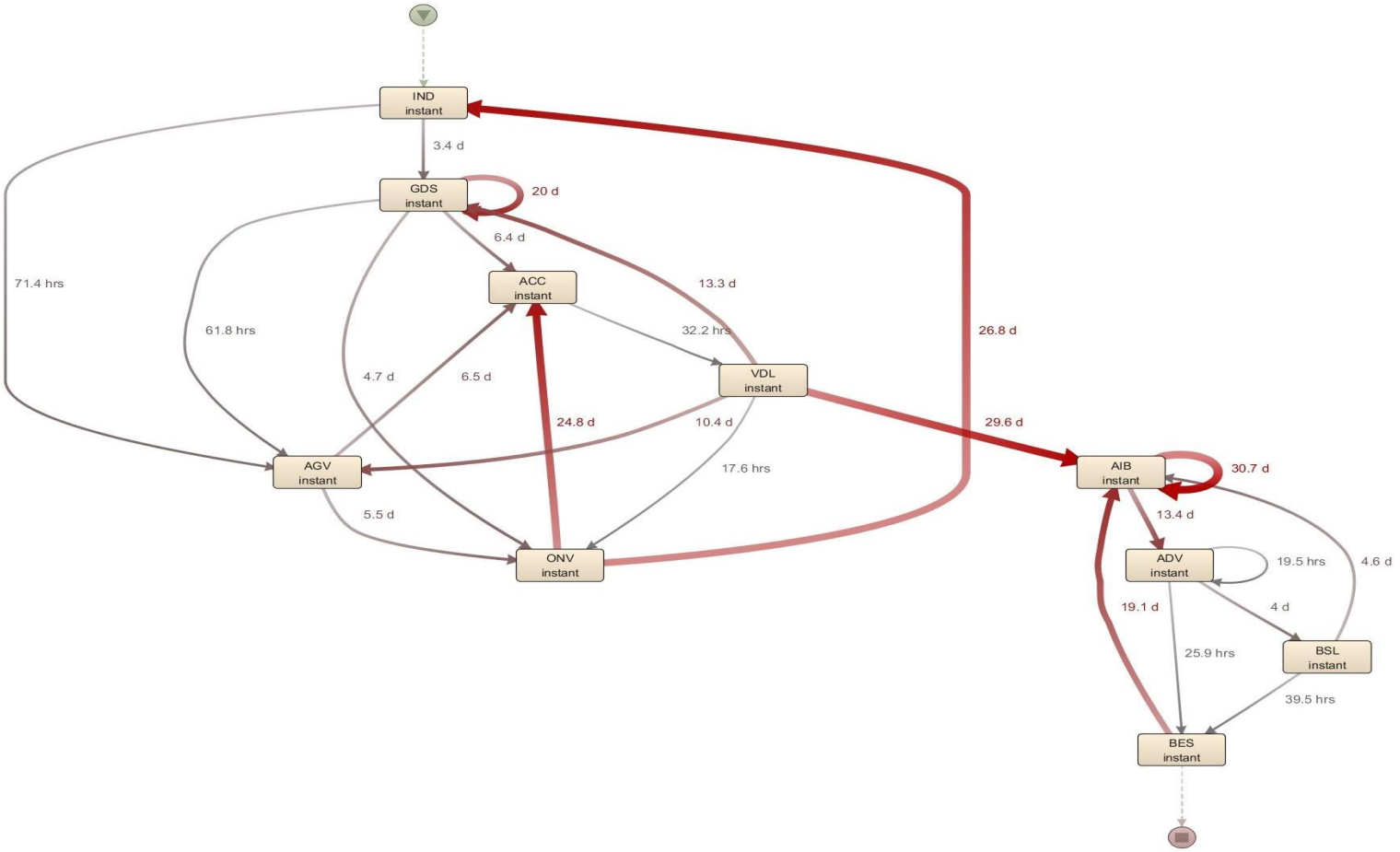
# Внесок у витягування даних про процес


| file ID | Operation | Date | Naam | Team | amount |
|---|---|---|---|---|---|
| 3022344 | ingediend | 19-10-2010 11:44 | KLANT | Klant | |
| 3022344 | aanvraag in behandeling | 6-1-2011 8:38 | Medewerker A | Team A | |
| 3022344 | advies | 24-1-2011 15:17 | Medewerker A | Team A | |
| 3022344 | geaccepteerd | 8-11-2010 13:35 | Medewerker B | Team B | |
| 3022344 | Verdeeld | 6-12-2010 8:45 | Medewerker B | Team B | |
| 3022344 | beslist | 28-1-2011 13:16 | Medewerker C | Team A | 25.000.000 |
| 3022344 | beschikt | 31-1-2011 10:14 | Medewerker D | Team B | |
| 3022344 | geen dossier status | 25-10-2010 11:02 | Medewerker E | Team B | |
| 3022345 | ingediend | 19-10-2010 16:15 | KLANT | Klant | |
| 3022345 | beschikt | 9-11-2010 9:25 | Medewerker F | Team B | |
| 3022345 | geen dossier status | 25-10-2010 11:02 | Medewerker G | Team B | |
| 3022346 | ingediend | 19-10-2010 18:25 | KLANT | Klant | |
| 3022346 | aanvra g in behandeling | 27-12-2010 14:42 | Med werker D | Team C | |
| 3022346 | advies | 15-2-2011 8:48 | Med werker D | Team C | |
| 3022346 | beslist | 15-2-2011 13:27 | Med erker C | Team C | 15.000.000 |
| 3022346 | onvolle | 29-11-2010 17:07 | Med erker A | Team B | |
| 3022346 | geacc erd | 21-12-2010 14:24 | Med rker A | Team B | |
| 3022346 | Ve | 22-12-2010 18:19 | M | m B | |
| 3022346 | bes | 16-2-2011 10:10 | r | m B | |
| 3022346 | gee | 25-10-2010 11:02 | M | m B | |

# Приклад витягування даних про процес (кількість)



# Приклад витягування даних про процес (опрацювання)



# Порядок денний

- Інструменти для аналізу даних
  - Витягування інформації про процеси
  - **Аналіз автоматизованих даних за допомогою Splunk**
    - Інформація про мережу та сервер в режимі реального часу з панеллю приладів Splunk
    - Аналіз журналів
- Інструменти для IT-безпеки
  - Центр для інтернет-безпеки
  - Оцінити якість цифрових сертифікатів
  - Перевірити комп'ютери на предмет спільних неправильних конфігурацій безпеки
  - Бонус

# Що таке Splunk?

• Splunk – це американська мультинаціональна корпорація з базою у Сан-Франциско (Каліфорнія), яка виробляє програмне забезпечення для пошуку, моніторингу і аналізу автоматично згенерованих Великих Даних через інтерфейс у веб-стилі.

•Особливим щодо Splunk  є той факт, що можна опрацювати майже всі можливі види ввідних даних.

•Плата за ліцензію розраховується за кількістю гігабайт, яку ви хочете опрацювати на щомісячній основі, але для непрофесійного використання (<500 безкоштовно).

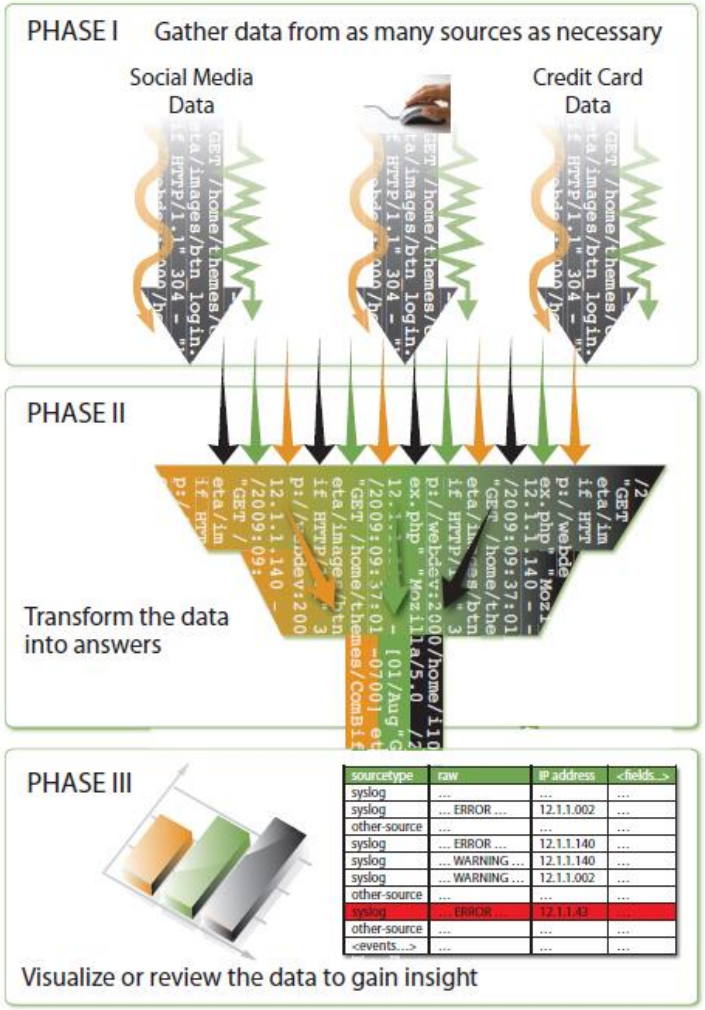
# Які функціональні можливості Splunk?

- Безпека і шахрайство
  - Просунуте виявлення і реагування на загрози
  - Відповідність
- Управління журналами
  - Індексування, пошук та кореляція будь-яких даних для повного розуміння вашої інфраструктури
  - Прогортання донизу і догори та по горизонталі усіх даних, щоб швидко знайти голку в стозі сіна
  - Побудова звітів та панелей управління
- Спрощення IT-операцій
  - Співвідношення подій по усіх прошарках інфраструктури для видимості рівня обслуговування
  - Розв'язування проблем швидше, скорочення часу простою

# Мета Splunk

- Автоматизовані дані з центру даних
- Від даних до відповідей
- Зв’язок між автоматизованими даними

і бізнес-даними, як вхідна інформація для звітів керівництву

# Порядок денний

- Інструменти для аналізу даних
  - Витягування інформації про процеси
  - Аналіз автоматизованих даних за допомогою Splunk
    - Інформація про мережу та сервер в режимі реального часу з панеллю приладів Splunk
    - Аналіз журналів
- Інструменти для IT-безпеки
  - **Центр для Інтернет-безпеки**
  - Оцінити якість цифрових сертифікатів - SSL лабораторії
  - Перевірити комп'ютери на предмет спільних неправильних конфігурацій безпеки
  - Бонус

# Інструменти для IT-безпеки

**Безпека комп'ютерів**

**Безпека мережі**

**Інтернет-безпека**

Приклади інструментів для тестування:




# Центр для Інтернет-безпеки (ЦІБ)

- Центр для Інтернет-безпеки (ЦІБ) – це 501c3 неприбуткова організація, яка зосереджується на посиленні готовності і реагування державних та приватних установ в частині кібербезпеки
- Програма ЦІБ щодо тестування безпеки забезпечує чіткими, однозначними та узгодженими найкращими практиками в цій галузі, щоб допомогти організаціям оцінити та покращити свою безпеку. Ресурси включають тестування конфігурації безпеки, автоматизовані інструменти оцінки конфігурації та змісту, метрики безпеки та сертифікати програмного забезпечення безпеки.
- Найкращі практики для конфігурації: Windows, Linux, Unix, Віртуалізація, мережа і сервери
- https://www.cisecurity.org/cis-benchma

Center for Internet Security®

# Порядок денний

- Інструменти для аналізу даних
  - Витягування інформації про процеси
  - Аналіз автоматизованих даних за допомогою Splunk
    - Інформація про мережу та сервер в режимі реального часу з панеллю приладів Splunk
    - Аналіз журналів
- Інструменти для IT-безпеки
  - Центр для Інтернет-безпеки
  - **Оцінити якість цифрових сертифікатів - SSL лабораторії**
  - Перевірити комп'ютери на предмет спільних неправильних конфігурацій безпеки
  - Бонус

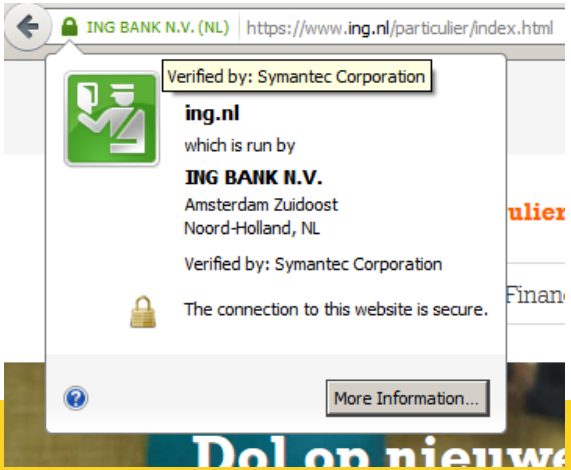
# Оцінити якість цифрових сертифікатів

- Дані, що передаються, можуть бути перехоплені на шляху до місця призначення третьою стороною.

# Оцінити якість цифрових сертифікатів

- Ризик: Дані, що передаються, можуть бути перехоплені на шляху до місця призначення третьою стороною.
- Захід контролю: використовувати інфраструктуру відкритих ключів для кодування зв'язку з кінцевим користувачем.

- Цифрові сертифікати можуть використовуватися для ідентифікації особи. Наприклад, при підписанні цифрових документів.



# Оцінити якість цифрових сертифікатів

# Порядок денний

- Інструменти для аналізу даних
  - Витягування інформації про процеси
  - Аналіз автоматизованих даних за допомогою Splunk
    - Інформація про мережу та сервер в режимі реального часу з панеллю приладів Splunk
    - Аналіз журналів
- Інструменти для IT-безпеки
  - Центр для Інтернет-безпеки
  - Оцінити якість цифрових сертифікатів - SSL лабораторії
  - **Перевірити комп'ютери на предмет спільних неправильних конфігурацій безпеки**
  - Бонус

# Перевірити комп'ютери на предмет спільних неправильних конфігурацій безпеки

- Ризики і заходи контролю: система не скоригована і містить неправильну конфігурацію безпеки.

- Аналізатор Microsoft стану безпеки (Microsoft Baseline Security Analyzer) – це програмний інструмент, розроблений Microsoft для визначення стану безпеки шляхом оцінки, чи не бракує оновлень з безпеки і чи немає менш захищених налаштувань безпеки в самому Microsoft Windows, чи таких компонентах Windows як Internet Explorer, IIS веб-сервер, і в продуктах Microsoft SQL сервер, і Microsoft Office макро-налаштуваннях.


- Обмеження: тільки для продуктів Microsoft

- https://www.microsoft.com/en-us/download/details.aspx?id=7558

# Порядок денний

- Інструменти для аналізу даних
  - Витягування інформації про процеси
  - Аналіз автоматизованих даних за допомогою Splunk
    - Інформація про мережу та сервер в режимі реального часу з панеллю приладів Splunk
    - Аналіз журналів
- Інструменти для IT-безпеки
  - Центр для Інтернет-безпеки
  - Оцінити якість цифрових сертифікатів - SSL лабораторії
  - Перевірити комп'ютери на предмет спільних неправильних конфігурацій безпеки
  - **Бонус**

# Бонус: Питання безпеки персональних даних

- **Можна**

- Браузер
  - Додатки
  - Ghostery
  - Addblock
  - Https тільки
- Паролі (Keepass / lastpass)
- 2 фактори автентифікації
- Сканування вірусів
- Виправлення комп'ютера
  - Виправлення комп'ютера
  - Оновлення Windows
- Обізнаність!

- **Не можна**

- Фішинговий електронний лист з гіперпосиланнями на шкідливе програмне забезпечення
- Програмне забезпечення для вимагання
- Інструмент віддаленого доступу
- Ненадійні паролі
- Незахищені з'єднання через Wifi
- постійна загроза підвищеної складності

National Academy for Finance and Economics
*Ministry of Finance*

# Заключні запитання і відповіді

Дякуємо за увагу!