3. Bonden B. Website / B.Bonden // Wikipedia, the free encyclopedia. - 2010. - Access mode: http://en.wikipedia.org/wiki/Website
4. Pasichnyk N.R. Formalism in the formulation of the problem of creating a quality site / N.P. Pasechnik, M.P. Divak // Scientific works of DonNTU. - 2011. - Vip. 14 (188). - P. 325-329.
5. Performance_indicator // Wikipedia, the free encyclopedia. - 2019. - Access mode: https://en.wikipedia.org/wiki/Performance_indicator
6. Taktashkin D.V., Islyaev R.S. Criteria used to assess the quality of web resources // Modern scientific research and innovation. 2017. № 3 [Electronic resource]. URL: http://web.snauka.ru/issues/2017/03/80002

---

УДК 004.9

## ВИКОРИСТАННЯ МОДЕЛІ IDS У ФОРМУВАННІ ОСВІТНЬОЇ ПРОГРАМИ ДЛЯ СПЕЦІАЛЬНОСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

**Баришполь В.В.,** студент гр. МПІн-171
Науковий керівник: **Скітер І.С.**, к.т.н., доцент

Розвиток інформаційних технологій спричинив зростання важливості інформації у всесвітньому масштабі, що призвело до становлення проблеми захисту інформації. Створення спеціалізованих освітніх програм для підготовки висококваліфікованих кадрів у сфері кіберзахисту набуває популярності з кожним днем та сприяє відмежуванню цього напрямку від інших інформаційних дисциплін в окремий навчальний процес.

На практиці, галузь інформаційної безпеки в навчальному плані має схожі предмети та кваліфікації з іншими напрямками інформаційних технологій. На цій основі можуть виникати деякі суперечності у обраному студентом напрямку навчання. Більш ефективне представлення галузі інформаційної безпеки та захисту інформації можна презентувати студентам у вигляді системи IDS як компіляцією чітко-виокремлених підсистем з різними функціями та особливостями.

Під час роботи над магістерською кваліфікаційною роботою на тему моделювання IDS системи в мене сформувалось власне бачення функціональних складових та їх призначення у загальній системі. Таке бачення я продемонстрував на рисунку 1.

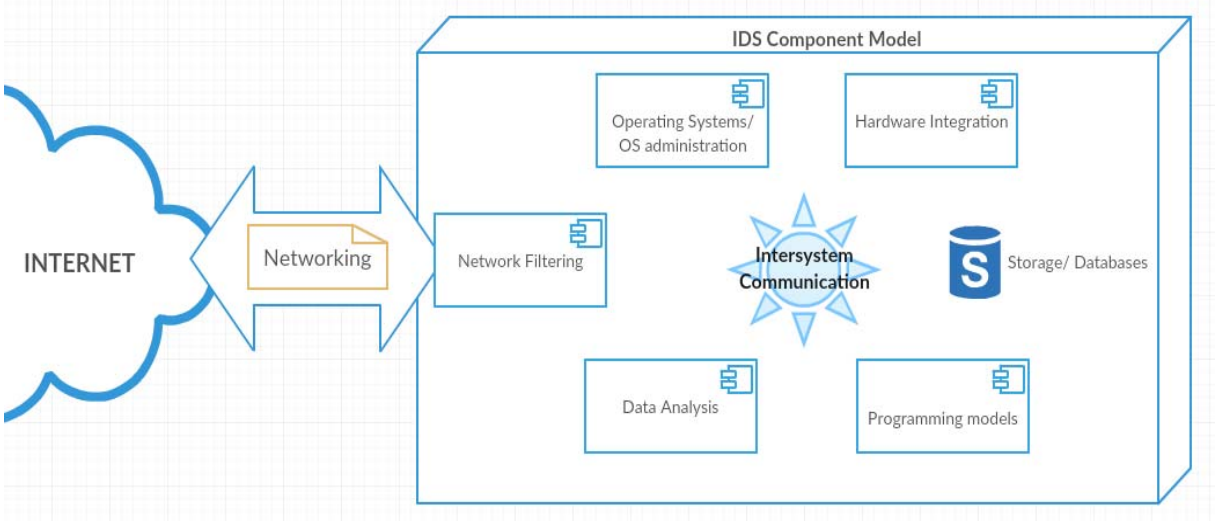


*Рис. 1. Компонентна модель системи виявлення вторгнень.*

Така системна модель охоплює більшість основних кваліфікацій та предметів вивчення по напрямку інформаційних технологій. Модель є динамічною та може бути розширена або підлаштована під вимоги які для неї ставлять.

До основних компонентів системи входять:

- **Мережі та інтернет комунікації - о**хоплення мережевого планування, налаштування локальної мережі, основні ризики та захист корпоративних мереж, і т.д.
- **Операційні системи - с**истемні налаштування, файлові системи, ядро операційної системи, процеси, апаратне управління, і т.д.
- **Бази даних та системи зберігання інформації –** види баз даних, зберігання та доступ до інформації, налаштування БД та реплікації, і т.д.
- **Методи аналізу даних -** види аналізу даних (кореляційний аналіз, дисперсійний аналіз, регресійний аналіз,…), статистичні методи обробки даних, data mining…
- **Програмування та парадигми програмування - о**б’єктно-орієнтовне програмування, функціональне програмування, мови програмування…

• **Апаратна інтеграція - п**рограмування мікроконтролерів, апаратні засоби
• **Внутрішньосистемний зв'язок –** система сигналізації, передача та прийом повідомлень, міжпрограмний/міжкомпонентний зв'язок.

Список компонентів можна доповнювати та вносити зміни згідно плану навчання та розвитку технологій.

Позитивні аспекти формування навчального плану на основі компонентного аналізу системи виявлення атак наступні:

- формування чіткого представлення поняття «система» та взаємозв'язок окремих компонентів;
- уніфікація загального навчального плану та наглядна необхідність даного предмету в повному курсі навчання;
- гнучкість побудування навчального плану;
- можливість інтегрування командної роботи над спільним проектом ids із розподіленням обов'язків між учасниками;
- постановка задачі розробки при закінченні курсу навчання з урахуванням всіх предметів, що були вивчені;
- актуальність теми кіберзахисту.

Загалом така модель навчання надає студентам повне бачення мети курсу та дасть можливість викладачам використовувати актуальну інформацію в зв'язку з розвитком даного напрямку.

---

УДК 004.93'1

## МОБІЛЬНИЙ ЗАСТОСУНОК ДЛЯ ІДЕНТИФІКАЦІЇ ОСОБИ

**Бендик А.В., Прохоренко А.А.,** студ. гр. ПІ-151
**Войтенко В.П.,** к.т.н., доцент
*Чернігівський національний технологічний університет*

Безпека власних громадян – найважливіша функція держави, без якої неможливий економічний і соціальний розвиток країни та її інституцій. Для України, яка перебуває в стані війни, доводиться мати справу з численними спробами внутрішньої дестабілізації, до яких належать теракти, підготовлені спецслужбами країни-агресора [1, 2]. Також не треба забувати про кримінальні елементи, які, користуючись моментом, незаконно заволодівають зброєю, яку намагаються використати у своїх протиправних діях проти інших громадян та державних органів, чи вчиняють інші злочини [3].

Попередження соціально-небезпечної поведінки певних суб'єктів можливе у випадку їхнього своєчасного виявлення та знешкодження. Сучасний стан розвитку інформаційних технологій (комп'ютерні мережі, смартфони) відкриває шляхи ефективного вирішення задачі ідентифікації особи на базі спеціалізованої розподіленої комп'ютерної системи.

Метою роботи є створення мобільного застосунку для ідентифікації особи, який має стати важливим компонентом спеціалізованої комп'ютерної розподіленої системи безпеки. Для цього потрібно вирішити такі задачі:

– проаналізувати існуючі аналоги і визначити архітектуру створюваної системи;
– обґрунтувати вибір і застосування окремих компонентів системи;
– розробити програмне забезпечення системи;
– провести інтеграцію окремих компонентів і випробувати систему в комплексі.

Створювана система складається з кількох апаратних та програмних компонентів. Фронтенд-модуль в смартфоні містить інтерфейс користувача, за допомогою якого запускається відеокамера. Отримане зображення піддається попередній обробці (фільтрація, підвищення контрасту, виділення границь об'єктів та ін.). Далі здійснюється попередня ідентифікація сфотографованої особи з використанням локальної бази даних. У випадку збігу з параметрами особи, яка є предметом інтересу (наприклад, перебуває у розшуку), спрацьовує обрана сигналізація (звукова або візуальна) та на екран смартфону виводиться попередження й інші потрібні дані. У будь-якому випадку формується запит на доступ до віддаленої бази даних (наприклад, у територіальному підрозділі поліції), який передається у вигляді пакету, що містить час запиту, ідентифікаційні дані запитувача, попередні гіпотези щодо встановленої особи або автотранспортного засобу тощо.

На місці розташування віддаленої бази даних здійснюється прийом пакету, його аналіз, визначення запиту та подальше опрацювання: уточнення гіпотези, виклик оперативної групи, передавання зворотного пакету на смартфон, з якого був здійсненим первинний запит тощо.

Програмне забезпечення розроблюваної системи територіальної безпеки повинно мати модульну структуру та передбачати можливість вибору різних методів обробки відеоінформації. В рамках роботи виконано попередній аналіз інформації за темою проекту, з'ясовано особливості та перевірено можливості