**МІНІСТЕРСТВО ОБОРОНИ УКРАЇНИ**
**Військовий інститут телекомунікацій та інформатизації**
**Національного технічного університету України**
**„Київський політехнічний інститут”**

# ВОЄННО-НАУКОВО КОНФЕРЕНЦІЯ КУРСАНТІВ (СТУДЕНТІВ)

**Факультету інформаційних технологій в системах управління**
**27 травня 2009 року**

**(Доповіді та тези доповідей)**

Київ – 2009

**ББК**
Ц4 (4Укр)39
П-768

У збірнику матеріалів воєнно-наукової конференції курсантів (студентів) факультету інформаційних технологій в системах управління опубліковано доповіді та тези доповідей вчених, науково-педагогічних працівників, ад'юнктів, здобувачів, курсантів і студентів Військового інституту телекомунікацій та інформатизації Національного технічного університету України „Київський політехнічний інститут" та інших вищих навчальних закладів, в яких розглядаються пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення.

## ЗМІСТ

1. ОРЖЕШКО Д.В. Вступне слово..... 4
2. ЛЮБАРСЬКИЙ С.В Про роботу наукового гуртка кафедри..... 6

**(Тези доповідей)**

1. **Бугера М.Г., Сілко О.В.** Методика визначення психофізичного стану студента в дистанційній формі навчання..... 7
2. **Бичков А.М., Нестеренко М.М.** Аналіз існуючих підходів щодо захисту даних від несанкціонованого доступу шляхом контролю запитів до записів у масивах баз даних..... 11
3. **Лазар Ю.В., Герасимов Б.М.** Методика побудови системи захищеної передачі поштових повідомлень із використанням криптографічних технологій..... 13
4. **Носовськой Р.О., Горбенко В.І.** Методика розробки структури автоматизованої навчальної системи мові програмування асемблеру.. 15
5. **Панченко А.Ю., Хусаінов П.В.** Автоматизація інформаційної підготовки мережевих програмно-ініційованих атак..... 16
6. **Прохорчук Ю.Ю., Макарчук О.М**. Система для послідовного аналізу статичних випробувань..... 17
7. **Симоненко О.А., Субач І.Ю.** Інтелектуальний аналіз даних в системах підтримки прийняття рішень в інформаційних мережах спеціального призначення..... 18
8. **Фесьоха В.В., Хусаінов П.В.** Мультиагентна система аналізу мережевого трафіку..... 19
9. **Циванюк М.С., Хусаінов П.В.** Тестування web-застосувань на предмет уразливостей типу SQL-ін'єкції..... 20
10. **Шемендюк О.В., Хусаінов П.В.** Пріоритезація надання повідомлень про інцидент безпеки..... 21

## ВСТУПНЕ СЛОВО

Шановні офіцери, працівники ЗСУ, курсанти та студенти. Сьогодні, відповідно до річного плану воєнно-наукової роботи курсантів (студентів) факультету, ми проводимо наукову конференцію воєнно-наукового товариства.

Конференція проводиться з метою підбиття підсумків наукової роботи курсантів (студентів) за навчальний рік, популяризації кращих робіт і широкого обміну думками стосовно них на факультеті.

Робота воєнно-наукового товариства на факультеті була організована і проводилася відповідно до вимог керівних документів:

1. Наказ Міністра оборони України № 9 від 13.01.2007 р.
2. Наказу НІ № 94 від 11.08.2008 р. „Про організацію підготовки та проведення наукової та науково-технічної діяльності в інституті на 2007-2008 навчальний рік”.
3. Методичних вказівок про організацію роботи ВНТ курсантів і студентів.
4. Положення про воєнно-наукове товариство курсантів (студентів) (затверджене Вченою радою інституту. Протокол № 10 від 27.02.2008 р.).

Товариші, кожний із вас у свій час виявив бажання самостійно займатися науковою працею і технічною творчістю, добровільно вступивши до воєнно-наукового товариства ВНТ курсантів (студентів) інституту. На протязі року ви підвищували свою методологічну підготовку, розвивали наукове мислення, набували навички дослідницької роботи, творчого підходу до вирішення задач бойового застосування з питань телекомунікацій та інформатизації, а також вивчали основи організації і проведення наукових досліджень.

Пріоритетними напрямками наукової роботи та науково-технічної діяльності роботи факультету є:

– статистичне оцінювання та його застосування на практиці;
– технології функціонування комунікаційних систем в мережах;
– методологія аналізу, синтезу та управління телекомунікаційними мережами;
– системи автоматизації електронного документообігу;
– інформаційні системи та бази даних;
– управління інформаційними мережами;
– захист інформації в інформаційних мережах;
– маршрутизація в територіальних мережах передачі даних;
– підвищення ефективності технічного обслуговування і ремонту військової техніки зв’язку і автоматизації;
– зменшення працезатрат на технічне обслуговування і ремонт військової техніки зв’язку і автоматизації;
– підвищення якості зберігання засобів зв’язку і автоматизації Збройних Сил України;

– автоматизація процесів управління технічним забезпеченням зв'язку і АУВ на всіх рівнях підпорядкування;

– оптимізація номенклатури засобів вимірювальної техніки з урахуванням їх морального стану, фізичного старіння та можливостей поставок для забезпечення.

Бажаю вам успіхів під час виступів як на пленарному засіданні так і під час роботи наукових секцій та закликаю до плідної творчої праці.

підполковник Любарський С.В. (ВІТІ НТУУ „КПІ”)

## ПРО РОБОТУ НАУКОВОГО ГУРТКА КАФЕДРИ

Наукова робота курсантів (студентів) є окремим видом наукової і науково-технічної діяльності, яка проводиться у вищих військових навчальних закладах та військових навчальних підрозділах вищих навчальних закладів під керівництвом професорсько-викладацького складу (наукових співробітників).

Метою наукової роботи наукового гуртка кафедри № 21 є підвищення методологічної підготовки, розвиток наукового мислення, набуття навичок дослідницької роботи, творчого підходу до вирішення задач бойового застосування і експлуатації сучасних інформаційних технологій, спеціального програмного та апаратного забезпечення ПЕОМ, вивчення основ організації і проведення наукових досліджень у цьому напрямку.

Залучення курсантів (студентів) до наукової роботи дає також змогу використовувати їх творчий потенціал для вирішення актуальних завдань ВВНЗ.

Наукова робота нашого гуртка проводиться у тісному зв’язку з навчальним процесом, як його невід’мне продовження, повинна відповідати завданням навчального процесу та науково-дослідної роботи кафедри.

Пріоритетними напрямками сумісної співпраці професорсько-викладацького складу та курсантів (студентів) є: впровадження та застосування сучасних інформаційних технологій в систему управління військами; методологія аналізу захищеності та забезпечення безпеки комп’ютеризованих систем, моделювання загроз їх безпеці; підтримка прийняття рішень у галузі захисту інформаційних систем; підвищення ефективності підготовки висококваліфікованих кадрів за рахунок оптимізації алгоритмів функціонування сучасних систем навчання; методологія оптимізації шляхів відпрацювання електронних документів; дослідження актуальних проблем і перспектив розвитку військової освіти, удосконалення підготовки та виховання військових фахівців. І у цих напрямках деякі з студентів (курсантів) нашого факультету досягнули певних успіхів. Так за кращу наукову працю серед курсантів та студентів ВІТІ НТУУ “КПІ” заохочені наступні члени наукового гуртка кафедри: курсант Бугера М.Г., Панченко А.Ю., Шемендюк О.В., Лазар Ю.В., Циванюк М.С., Єрмоленко В.М., Фесьоха В.В.

Саме з метою підбиття підсумків наукової роботи курсантів (студентів) за навчальний період, популяризації кращих робіт і широкого обміну думками стосовно них проводиться сьогоднішня наукова конференція.

Бажаю усім присутнім успішного виступу і подальшої творчої наснаги у питаннях розбудови сучасних Збройних Сил України.

Бугера М.Г. (ВІТІ НТУУ „КПІ”)
Сілко О.В. (ВІТІ НТУУ „КПІ”)

# МЕТОДИКА ВИЗНАЧЕННЯ ПСИХОФІЗИЧНОГО СТАНУ СТУДЕНТА В ДИСТАНЦІЙНІЙ ФОРМІ НАВЧАННЯ

Активний розвиток як самого дистанційного навчання, так і впровадження дистанційних технологій в різних областях, пов'язаних певною мірою з передачею знань, даних або будь-якої інформації є об'єктивною тенденцією впровадження інформаційних технологій в усі сфери людської діяльності.

Індивідуально орієнтований підхід в системі дистанційного навчання передбачає постійне спілкування студентів в процесі пізнавальної діяльності їх спільну діяльність, взаємодію між собою і з викладачем. При цьому важливо викладачеві уміти здійснювати диференціацію навчання, рефлексію та на відміну від очних форм навчання, йому необхідно вміти визначати психологічний та психофізичний стан студентів на відстані. Останнє більшою мірою пов'язано з тим, що навчання за дистанційною формою передбачає аналіз студентом текстової та графічної інформації з екрана монітора, а фізичне навантаження на м'язовий апарат є побічним, небажаним ефектом. Крім того, на фізичний стан впливає незмінна статична поза перед екраном монітора, при цьому більшість груп м'язів знаходиться у постійній напрузі, що призводить до швидкої втоми, сприяє розвитку професійних захворювань операторів ЕОМ. Студент має неперервні нервово-психічні перевантаження, які пов'язані з перенавантаженням зорового апарата, що також негативно впливає на його стан.

Визначення складності робіт, які виконує студент в системі дистанційного навчання, є складним завданням. Аналіз існуючих літературних джерел, стосовно даної проблеми, показавши, що існує спеціальне програмне забезпечення, яке дозволяє достатньо просто виявити кількість уведених символів, але неможливо визначити кількість прочитаних символів з екрана монітора [1], відсутній чіткий опис методик забезпечення викладача інформацією про психофізичний стан та його зміну у студента протягом навчання за дистанційною формою [2, 3]. Відомі біометричні методи визначення стану людини, які передбачають підключення спеціальних датчиків безпосередньо до людини або до його робочого місця, але в умовах дистанційного навчання такі методи мають обмежену область застосування.

Для системи дистанційного навчання завдання визначення психофізичного стану студента формулюється наступним чином: визначити психофізичний стан студента шляхом оцінки відхилення потокового психофізичного стану від найкращого.

Для рішення поставленої задачі обраний метод біометрії, який обробляє дані клавіатурного почерку. Цей метод дозволяє визначити психофізичний стан студента з необхідною періодичністю та здійснити постійний котроль за станом протягом навчання. При застосуванні методу відліком для визначення психофізичного стану студента є інтервали натиснення на клавіші та час

утримання клавіші між натисненням. Для виміру обираються послідовності, які студент має спеціально набирати на клавіатурі під час проходження навчального курсу. Максимальна працездатність дорівнює найкращому стану студента, цей стан – еталон, який оцінюється у сто відсотків, мінімальна працездатність – нуль відсотків. На основі отриманої інформації відбувається визначення психофізичного стану студента та формування управляючих впливів.

Для реалізації математичної моделі пропонується застосувати штучну нейронну мережу, яка реалізується багатошаровим персептроном. Персептрон здатний працювати із багатьма вхідними даними, поділяти їх на простори, тобто класифікувати дані за ознаками, які визначає нейронна мережа.

Вхідною інформацією для нейронної мережі є дані клавіатурного почерку, а саме, час утримання клавіш і час між натисненнями. Вихідною інформацією виступає номер нейрона, який спрацював в мережі. Номер нейрона сповіщає про належності вхідних даних клавіатурного почерку до певної області значень багатомірного простору даних моделі.

Математичне подання пропонуємої нейронної мережі:

$$y_k = f\left(\sum_{i=0}^{K} w_{ki}^{(2)}\, v_i\right) = f\left(\sum_{i=0}^{K} w_{ki}^{(2)} f\left(\sum_{j=0}^{N} w_{ij}^{(1)} x_j\right)\right) \quad ,$$

де $y_k$ – значення нейрона вихідного шару, $x_i$ – $i$-тий вхід нейрона, $v$ – вхідне значення нейрону, $K$ – кількість нейронів вихідного шару, $N$ – кількість нейронів прихованого шару, $w_{ij}^{(1)}$ – вага між $j$-тим нейроном вхідного шару та $i$-тим нейроном прихованого шару, $w_{ki}^{(2)}$ – вага між $k$-тим нейроном вихідного шару та $i$-тим нейроном прихованого шару.

Функція активації:

$$f(x) = \frac{1}{1+e^{-\beta x}} \ ,$$

де β – коефіцієнт.

Процес навчання нейронної мережі дозволяє провести класифікацію вхідних значень шляхом розбиття простору даних на п'ять просторів [4]. Для визначення зміни психофізичного стану студента за короткий період часу пропонується застосувати процедуру визначення відхилення станів поточного та наступного нейрону, який спрацював. Процедура реалізує лінгвістичну змінну:

$$\Pi = < \beta, T, X > ,$$

де β – назва змінної, T – множина значень змінної, X – область визначення множини значень змінної.

Для сформульованої задачі маємо:

$$\Pi = < \text{відхилення}, T, [0; 100] > ,$$

де T = {"велике", "мале"}.

Велике значення відхилення психофізичного стану описується:

$$< \text{велике}, [62{,}5\ ;\ 100],\ \widetilde{A}_B >,$$
$$\widetilde{A}_B = \left\{ \mu_{\widetilde{A}_B}(x_i) / x_i \right\},$$

де $\mu_{\widetilde{A}_B}$ – функція залежності:

$$\mu_{\widetilde{A}_B} = \begin{cases} 1, & \textit{якщо} \quad x_2 \geq 0{,}652\, x_1 \\ \dfrac{x_2 - 0{,}5x_1}{0{,}1x_2}, & \textit{якщо} \quad 0{,}5x_1 \langle\, x_2 \,\langle 0{,}652\, x_1 \\ 0, & \textit{якщо} \quad x_2 \leq 0{,}652\, x_1 \end{cases}.$$

Мале значення відхилення психофізичного стану описується:

$$< \text{мале}, [0\ ;\ 40],\ \widetilde{A}_M >,$$
$$\widetilde{A}_M = \left\{ \mu_{\widetilde{A}_M}(x_i) / x_i \right\},$$

де $\mu_{\widetilde{A}_M}$ – функція залежності:

$$\mu_{\widetilde{A}_B} = \begin{cases} 1, & \textit{якщо} \quad x_2 \leq 0{,}4\, x_1 \\ \dfrac{0{,}5x_1 - x_2}{0{,}1x_1}, & \textit{якщо} \quad 0{,}4x_1 \langle\, x_2 \,\langle 0{,}5\, x_1 \\ 0, & \textit{якщо} \quad x_2 \geq 0{,}5\, x_1 \end{cases}.$$

Функція визначення необхідного приросту:

$$y = x_1 + \left( \mu_{\widetilde{A}_B}(x_1) \times \Delta \right) - \left( \mu_{\widetilde{A}_M}(x_2) \times \Delta \right), \qquad (1)$$

де $y$ – відхилення, $x_1$ – попереднє значення стану, $x_2$ – поточне значення стану, $\Delta$ – приріст.

Значення виразу (1) дозволяє зробити висновок про розвиток гальмування моторних функцій організму студента та про поточний психофізичний стан під час дистанційного навчання.

На основі наведених міркувань пропонується розробити універсальну оболонку у вигляді додаткового модуля, який реалізує наведену математичну модель та алгоритм (рис. 1).

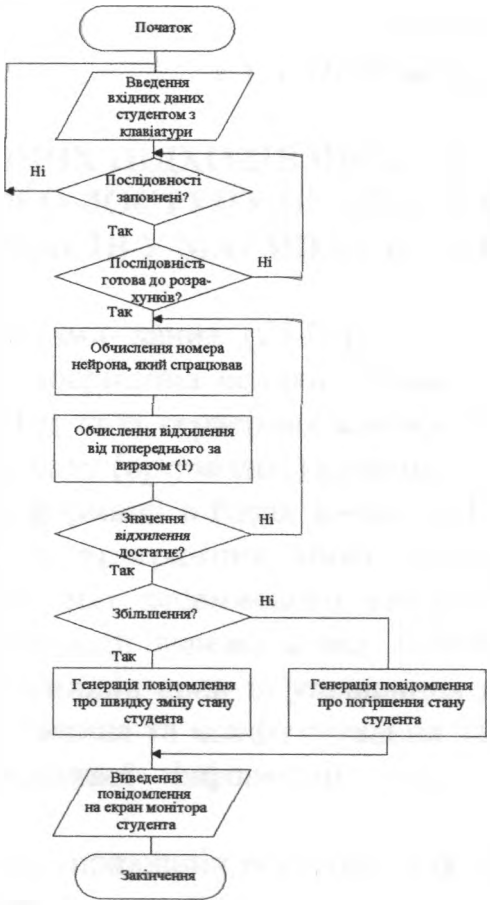


Рис. 1. Алгоритм визначення стану студента за клавіатурним почерком

Програмне забезпечення дозволить викладачу отримати інформацію про психофізичний стан студентів під час дистанційного навчання та приймати рішення про вибір впливу на тих, хто навчається. Розроблене програмне забезпечення передбачається розмістити у об'єктно-орієнтованому середовищі для навчання Moodle.

*Література*

1. *Пономаренко Л.А., Степанова Я.М.* Особливості захисту інформації та ідентифікації користувачів в системах дистанційного навчання // Вісник КНТЕУ, 2003. – № 3. С. 62 – 67.

2. *Пономаренко Л.А., Степанова Я.М.* Определение времени реакции системы обработки данных на сообщения, которые поступают от удаленных абонентов // Кибернетика и вычислительная техника. – 2002. – Вып. 136. – С. 62 – 67.

3. *Гороховський О.І., Трояновська Т.І.* Аспекти створення, моделювання та практики автоматизованих систем дистанційного навчання // Автоматика 2006. – Вінниця, 2006. – С. 453.

4. *Кукушкин Ю.А., Богомолов А.В., Гузий А.Г.* Принципы построения систем обеспечения жизнедеятельности систем обеспечения операторов систем "человек–машина", адаптивных к их функциональному состоянию // Мехатроника, автоматизация, управление. – 2005. № 3. С. 43–47.

Бичков А.М. („ВІТІ НТУУ КПІ”)
к.т.н. Нестеренко М.М. („ВІТІ НТУУ КПІ”)

# АНАЛІЗ ІСНУЮЧИХ ПІДХОДІВ ЩОДО ЗАХИСТУ ДАНИХ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ ШЛЯХОМ КОНТРОЛЮ ЗАПИТІВ ДО ЗАПИСІВ У МАСИВАХ БАЗ ДАНИХ

Системи керування базами даних (СКБД), в особливості реляційні, стали домінуючим інструментом зберігання великих масивів інформації. Забезпечення інформаційної безпеки СКБД та їх серверних компонентів, набуває вирішального значення для безпеки підрозділу (організації) в цілому.

Ступінь збереження інформації в базах даних (БД) підвищується, якщо вона захищена від апаратних та програмних збоїв, катастрофічних, кримінальних ситуацій, некомпетентності або зловмисного використання. Але, насамперед, забезпечення безпеки інформації залежить від адміністраторів БД, основними аспектами роботи яких є розподіл прав та управління доступом до БД, контроль доступу, правильне налагодження та конфігурування захисту БД. При відмові від останнього більшість важливої інформації стане легкою здобиччю для зловмисників.

Ефективність механізму управління доступом для захисту даних залежить від виконання трьох припущень:

1. Правильна ідентифікація користувача;
2. Використання шифрування;
3. Використання категорій секретності для визначення доступу кожної програми до об’єктів системи.

Засоби керування даними в СКБД дозволяють користувачеві управляти доступом інших користувачів до його даних та контролювати недоторканність останніх. Засоби захисту можуть також забезпечувати виконання групових операцій (транзакцій) і здійснювати відновлення БД.

Якщо інформація, що отримується на основі конфіденційних даних, призначена для широкого використання, то вимагають змін правила управління потоком переданих даних. Це стосується, в першу чергу, до статистичних баз і банків даних, які містять конфіденційну інформацію, яка використовується для формування різних статистичних зведень.

Особливість ситуації полягає в тому, що зведення містять „відголоски” вихідної конфіденційної інформації, і досить наполегливий користувач може її відновити. Коли інформація стосується деякої конкретної особистості, процедура відновлення розцінюється як посягання на його особисту таємницю.

Запис вважається скомпрометований, якщо користувач, що формує запит, може визначити значення конфіденційної величини, порівнюючи відповіді на запити і використовуючи будь-яку апріорну інформацію. Компрометація полягає у виявленні запису, що зацікавив на основі перехресних запитів; перекручуванні відповіді шляхом округлення або якоїсь умисної корекції даних; контролю звернення лише до випадкових записів.

Доступ до інформації на основі методу висліджування заснований на використанні групи записів, що перетинаються. Для захисту від висліджування застосовують принцип мінімального взаємозв'язку питань, який полягає в забороні відповідати на запит, в якому міститься більше певного числа співпадаючих записів з попередніх запитів. Такий контроль на практиці нереальний, оскільки програма повинна зробити порівняння останньої групи запитів з усіма попередніми. Але якщо навіть до нього і вдатися, цей контроль можна обійти в базі даних, де кожна конфіденційна величина з'являється лише один раз. Контроль мінімального взаємозв'язку питань може бути усунутий шляхом вирішення системи лінійних рівнянь відносно невідомої величини.

Інший спосіб контролю заснований на внесенні навмисних спотворень у звіти. Зазвичай, реалізується округлення результатів, коли точна відповідь на запит незначно спотворюється, перш ніж сформується відповідь користувачеві на його запит.

Ще один спосіб контролю заснований на тому, що запити адресуються не до всієї бази даних, а до деякої випадково вибраної групи записів. Такий підхід найбільш ефективний, оскільки позбавляє користувача можливості контролювати багато запитів. Функції запитів в більшості комерційних СКБД дозволяють виявити значно більше інформації про конфіденційні записи, ніж уявляється. Без відповідного контролю несанкціонований доступ до бази даних буде швидше за правило, ніж винятком. У комбінації з принципом мінімальної безлічі запитів випадкові запити забезпечують найкращий захист.

Отже, ефективним заходом захисту від нав'язливих зловмисників є спостереження за вторгненнями, що включають перевірку файлів реєстрації та контрольних журналів на наявність незвичайних сполучень запитів або великої кількості запитів до одного і того ж запису. Хоча при цьому і контролюється потік інформації, яка проходить через програми обробки запитів, але спостереження за вторгненнями дозволяє виявити підвищену активність звернень і зробити певні висновки з забезпечення захисту даних.

Лазар Ю.В.(ВІТІ НТУУ „КПІ”)
д.т.н. Герасимов Б.М.(ВІТІ НТУУ „КПІ”)

# МЕТОДИКА ПОБУДОВИ СИСТЕМИ ЗАХИЩЕНОЇ ПЕРЕДАЧІ ПОШТОВИХ ПОВІДОМЛЕНЬ ІЗ ВИКОРИСТАННЯМ КРИПТОГРАФІЧНИХ ТЕХНОЛОГІЙ

В даний час процесу передачі конфіденційної інформації по відкритих каналах зв’язку приділяється велика увага. Особливо, це питання є актуальним для державних установ та підрозділів спеціального призначення.

Конфіденційний зв’язок, регулюється Конституцією України, законами України „Про інформацію”, „Про державну таємницю”, „Про захист інформації в автоматизованих системах”, „Про національну систему конфіденційного зв’язку”, і т. д. Згідно цих законів та вимог щодо управління зв’язком та військами до таємної інформації накладаються такі основні вимоги: своєчасність; достовірність; цілісність; скритність.

Для організації управління підрозділами та частинами у Збройних Силах України, з метою забезпечення вимоги достовірності та цілісності даних, застосовують сучасні криптографічні технології. Такі як:

– симетричні технології шифрування (*DES*, *AES*, ГОСТ 28147-89, *Camellia*, *Twofish*, *Blowfish*, *IDEA*, *RC4* і ін.);

– асиметричні технології шифрування (*RSA* і *Elgamal* (Ель-Гамаль)).

Сучасні рішення передачі конфіденційної інформації по відкритих каналах від компанії *Microsoft* передбачають: реалізацію шифрування; генерацію відкритих і закритих ключів; створення і перевірку електронно-цифрового підпису.

Але відповідні рішення носять комерційний характер і використовувати відповідні технології та програмні модулі для побудови інформаційних систем спеціального призначення не представляється можливим.

Пропонується реалізація завдання побудови інформаційних систем спеціального призначення, для організації захищеного інформаційного обміну даними, використовуючи криптографічні бібліотеки сучасних інструментальних оболонок програмування на мовах високого рівня. Так, пропонується використання бібліотеки *Crypto API*, з базової бібліотеки інструментальної оболонки *Borland Delphi*. Бібліотека *Crypto API* орієнтована на: надійне заховання даних; можливість передачі прихованих даних третім особам; надійну систему перевірки достовірності інформації, що прийшла від третіх осіб; розшифровку отриманих конфіденційних даних; роботу з „ідентифікаційними посвідченнями” третіх осіб; забезпечення роботи з визнаними криптографічними стандартами; можливість розширення і роботи з поки що невідомими алгоритмами.

Основними функціями шифрування/дешифрування в мові високого рівня стали:

– *CryptEncrypt*. Функція шифрування даних. Як параметри використовують раніше отримані контексти криптопровайдера й сесійного ключа;

– *CryptDecrypt*. Функція розшифровування даних. Як параметри використовуються раніше отримані контекст криптопровайдера та параметри сесійного ключа;

– *CryptGenKey*. Дана функція призначена для генерації сесійного ключа (ключ, використовується тільки протягом поточної сесії роботи), а також для генерації пар ключів для обміну (публічний і закритий ключ) і цифрового підпису.

Так вищезазначені функції можна використати для побудови поштових клієнтів спеціального призначення, для організації поштового обміну конфіденційною електронною кореспонденцією із залученням алгоритмів шифрування.

Особливістю програмної реалізації є те, що програмний продукт матиме відкритий код, з гарантованою стійкістю та гібридним алгоритмом шифрування, який підходить для спеціальних систем.

Носовськой Р.О. (ВІТІ НТУУ „КПІ”)
к.т.н. Горбенко В. І. (ВІТІ НТУУ „КПІ”)

# МЕТОДИКА РОЗРОБКИ СТРУКТУРИ АВТОМАТИЗОВАНОЇ НАВЧАЛЬНОЇ СИСТЕМИ МОВІ ПРОГРАМУВАННЯ АСЕМБЛЕРУ

При вивченні мови програмування асемблеру 32 розрядних процесорів архітектури *Intel* виникає проблема, пов'язана з відсутністю інтегрованої оболонки для комплексної розробки, трансляції, компоновки і відлагодження асемблерних програм. Крім того, проблемним є те, що ці етапи не автоматизовані і не розраховані на самостійне навчання.

У рамках процесів контролю навчання, спостереження за тенденціями розвитку тих, кого навчають, ведення електронного журналу викладача не існує програмних засобів автоматизації.

З метою автоматизації процесів отримання, контролю та перевірки знань тих, кого навчають пропонується автоматизована навчальна система мові програмування асемблеру (АНСА). Вона орієнтована на студентів (курсантів) вищих навчальних закладів (ВНЗ), які мають практичні навички при роботі з мовами програмування високого рівня, а також ознайомлені з проблемами безпеки інформаційних систем. АНСА вирішує одну з найактуальніших проблем безпеки при авторизації користувачів шляхом шифрування та дешифрування паролів.

Методика розробки структури АНСА є багатоетапною і базується на декомпозиції за функціональними ознаками складної системи на підсистеми.
В результаті декомпозиції отримані наступні підсистеми:

- підсистема адміністрування;
- підсистема безпеки при авторизації користувачів;
- підсистема навчання;
- підсистема перевірки та контролю;
- підсистема звітування;
- підсистема реєстрації.

Сукупність підсистем АНСА вирішує наступні задачі:

- розмежування доступу користувачів до ресурсів АНСА;
- забезпечення тих, кого навчають необхідною літературою та учбовими матеріалами (аудіо- та відео- даними) тощо;
- створення середовища для написання та відлагодження програм;
- забезпечення можливості дизасемблювання розроблених програм;
- перевірка знань навчаємих шляхом тестування;
- аналіз якості навчання за певними тематиками;
- відслідковування тенденцій професійного росту тих, кого навчають;
- отримання звітів за результатами роботи АНСА.

Ця методика забезпечує вирішення проблеми навчання фахівця мові програмування асемблеру *Intel* – сумісних мікропроцесорів шляхом розробки структури АНСА як інтегрованої оболонки.

Панченко А.Ю.(ВІТІ НТУУ „КПІ”)
к.т.н. Хусаінов П.В.(ВІТІ НТУУ „КПІ”)

# АВТОМАТИЗАЦІЯ ІНФОРМАЦІЙНОЇ ПІДГОТОВКИ МЕРЕЖЕВИХ ПРОГРАМНО-ІНІЦІЙОВАНИХ АТАК

Найближчою перспективою розвитку інформаційних технологій є впровадження концепції електронного уряду, що полягає у активному впровадженні інформаційних технологій для підвищення ефективності надання державних послуг.

Концепція електронного уряду передбачає відкритість та доступність інформації для великих соціальних груп суспільства, організацій, комерційних установ та фірм тощо. При цьому очевидним є наявність в інформаційно-телекомунікаційній інфраструктурі держави вузлів, з якими пов’язано функціонування загальнодоступних програм серверного типу, виведення з ладу яких здійснює безпосередній вплив на якість державного управління.

Виходячи з цього можна констатувати зростання уваги з боку силових відомств до виконання завдань порушення роботи інформаційно-телекомунікаційної інфраструктури держави евентуального противника, як елемента інформаційної боротьби в інформаційно-телекомунікаційних системах у вигляді мережевих атак: порушення доступності, цілісності, достовірності інформаційних ресурсів. Великого значення в цьому випадку відіграє збір даних про об’єкт атаки. Реалізація мережевих атак передбачає наявність достовірної інформації про структуру, стан, якісний склад вузлів інформаційно-телекомунікаційної системи евентуального противника.

Інформаційна підготовка атаки передбачає виконання наступної послідовності дій:

– відслідковування адрес маршрутизаторів, через які проходить пакет від вузла зловмисника до вузлів об’єкта атаки, та отримання інформації про них;

– збирання та обробка інформації про структуру мережі;

– встановлення структури інформаційно-телекомунікаційної системи;

– логічний висновок щодо найбільш важливих цілей для мережевих атак;

Найбільш простим та імовірним типом атаки є порушення доступності вузлів інформаційно-телекомунікаційної мережі. Для успішного проведення такої атаки суб’єкту атаки необхідно порушити доступ до вузлів, що мають відкриті ресурси, шляхом виведенням з ладу об’єкта атаки або прилеглих до нього вузлів таким чином, щоб до об’єкта атаки не було доступу. Отже, великого значення набуває питання дослідження структури мережі, що знаходиться у безпосередній близькості до об’єкта атаки.

В даний момент немає офіційних некомерційних засобів, що виконують завдання інформаційної підготовки атаки у наведеній змістовній постановці. Тому актуальним питанням є розробка програмного забезпечення, що зможе автоматизувати роботу з дослідженя структури мережі.

Прохорчук Ю.Ю. (ВІТІ НТУУ "КПІ")
к.т.н. Макарчук О.М. (ВІТІ НТУУ "КПІ")

# СИСТЕМА ДЛЯ ПОСЛІДОВНОГО АНАЛІЗУ СТАТИЧНИХ ВИПРОБУВАНЬ

В сучасному світі підприємці великого та малого бізнесу, а також окремі посадові особи у військовій сфері, часто зустрічаються з актуальним на сьогоднішній день питанням, саме як при закупці чи отриманні великої кількості, наприклад деталей, була кількість дефектних деталей мінімальною.

З цим питанням зустрічаються в самих різних сферах діяльності. Тісно пересікається у військовій діяльності, коли необхідно оновити озброєння у збройних силах та закупити саме якісну, велику партію зброї(АК-74). Або у сфері промисловості, завод по виготовленню якісних кондиціонерів. Власник заводу повинен мати експертів та спеціальні засоби діагностування товарів, з метою уникнення хибної партії.

Рішення цієї проблеми знайшов видатний математик-статистик, Вальд Абрахам, який запропонував метод послідовної перевірки статичних гіпотез. Цей метод виявляється досить ефективним у різних галузях науки і техніки, наприклад, під час вибіркового контролю масової продукції, при статистичній обробці результатів фізичних експериментів, у загальній теорії зв'язку (при вирішенні задачі виявлення сигналу в шумах).

Користуючись цим методом, пропонується його автоматизувати, для програмної реалізація методу послідовного аналізу пропонується використати мову програмування високого рівня Object Pascal, в інструментальному середовищі Delphi 7, що дозволить:

- аналізувати продукт без втручання людини, та приймати вірне рішення;
- значно підвищити швидкість обробки інформації;
- зекономити час;
- зменшити кількість спеціалістів, що займаються перевіркою продукту на його дефектність;
- підвищити мобільність.

Особливістю цього програмного продукту буде те, що користувач під час випробувань матиме змогу стежити за цим процесом. Та кінцевий результат можна продивлятись графічно, що дозволить більш краще сприйняття результатів. А також система дозволить з мінімальним числом випробувань прийняти правильне рішення, щодо прийняття або усунення партії.

Симоненко О.А. (ВІТІ НТУУ „КПІ”)
к.т.н. Субач І.Ю. (ВІТІ НТУУ „КПІ”)

# ІНТЕЛЕКТУАЛЬНИЙ АНАЛІЗ ДАНИХ В СИСТЕМАХ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ В ІНФОРМАЦІЙНИХ МЕРЕЖАХ СПЕЦІАЛЬНОГО ПРИЗНАЧЕННЯ

Сучасний етап розвитку галузі надання інформаційних послуг все частіше характеризується переходом до поняття „інформаційна мережа”, який обумовлений все більшою інтеграцією транспортних сервісів та інформаційних служб. Інформаційна мережа – мережа, яка утворюється шляхом об’єднання у ієрархічній структурі інформаційних вузлів, активного та пасивного мережевого обладнання, відповідних програмних засобів та призначена для реалізації інформаційних процесів, що відбуваються в органах управління.

Інтелектуальний аналіз даних — виявлення прихованих закономірностей або взаємозв’язків між змінними у великих масивах необроблених даних.

ІАД включає методи і моделі статистичного аналізу і машинного навчання, дистанціюючись від них у бік автоматичного аналізу даних. ІАД дозволяє проводити аналіз даних певними фахівцями (аналітиками), за допомогою відповідних математичних знань, якими вони володіють.

Специфіка сучасних вимог до такої переробки наступна:

- дані мають необмежений об’єм;
- дані є різнорідними (кількісними, якісними, текстовими);
- результати мають бути конкретні і зрозумілі;
- інструменти для обробки „сирих” даних мають бути прості у використанні.

Розробка систем підтримки прийняття рішень (СППР) посадових осіб, які приймають рішення (ОПР) для управління інформаційними мережами, зараз є актуальним питанням. Проведений аналіз предметної області та публікацій дозволив визначити низку особливостей, які акцентують увагу на створенні відповідних систем підтримки прийняття рішень:

- забезпечення високої швидкості обробки запитів користувачів та надання необхідних інформаційних ресурсів і сервісів;
- створення ефективної служби діагностики і своєчасного оповіщення для попередження аварійних ситуацій та підвищення відмовостійкості інформаційної системи;
- забезпечення служби моніторингу, що виконує збір, обробку, зберігання і відображення повної інформації про стан усіх компонентів інформаційної інфраструктури компанії.
- надання миттєвої допомоги користувачу при виникненні нестандартних ситуацій (відмова, збій, зависання).

Реалізація описаних наукових завдань дозволить значною мірою підвищити ефективність функціонування інформаційної мережі, та якість її роботи у режимі реального часу під впливом різнорідних зовнішніх та внутрішніх факторів.

Фесьоха В.В. (ВІТІ НТУУ „КПІ”)
к.т.н. Хусаінов П.В. (ВІТІ НТУУ „КПІ”)

# МУЛЬТИАГЕНТНА СИСТЕМА АНАЛІЗУ МЕРЕЖЕВОГО ТРАФІКА

Аналіз існуючих підходів та умов моніторингу мережевого трафіка інформаційних систем (ІС) показав їх доцільне застосування до запобігання та швидкого виявлення мережевих руйнівних інформаційних впливів – мережевих атак. Яскравими прикладами інтегрування засобів моніторингу мережевого трафіка та систем захисту ІС є можливість виявлення наступних класів мережевих атак:

– розповсюдження зловмисного вірусного трафіка;
– функціонування троянських програм;
– атак типу відмова в обслуговуванні та розподілена відмова в обслуговуванні;
– перехоплення трафіка в ІС;
– несанкціонованих підключень;
– несанкціонованої зміни мережевої конфігурації;
– парольних атак;
– атак на прикладному рівні;
– переадресації портів;
– мережевої розвідки.

За умови деяких обмежень побудова системи моніторингу мережевого трафіка за схемою (менеджер-агент) на сьогоднішній день вважається найбільш прийнятною. При цьому особливості мультиагентної системи в порівнянні із системами моніторингу з жорсткою структурою мають наступні переваги:

– забезпечення моніторингу значно більшої частини мережі інформаційної системи;
– гнучка схема розподілу агентів;
– покладання первинної обробки даних на агентів;
– зменшення завантаженості мережі.

Перспективними напрямками удосконалення мультиагентної системи моніторингу трафіка мережі вважається:

– інтелектуалізація обробки даних менеджером;
– інтелектуалізація обробки даних агентами;
– кросплатформенність програмних агентів.

Інтелектуалізація обробки даних полягає у застосуванні для обробки інформації моделей надання знань: нейронні мережі, семантичні мережі, продукційні правила, фрейми. Забезпечення кросплатформенності програмних агентів полягає у їх розробці для застосування під управлінням різних операційних систем та апаратних платформ.

Циванюк М.С. (ВІТІ НТУУ „КПІ”)
к.т.н. Хусаінов П.В. (ВІТІ НТУУ „КПІ”)

# ТЕСТУВАННЯ WEB-ЗАСТОСУВАНЬ НА ПРЕДМЕТ УРАЗЛИВОСТЕЙ ТИПУ SQL-ІН'ЄКЦІЇ

На сучасному етапі розвитку Web-застосувань їх важливість та надійність з точки зору безпеки інформації значно зросла. Далеко не всі Web-застосування можна вважати захищеними, більшість з них має ті чи інші уразливості, і лише певна частина Web-застосувань (близько 7 %) вважається цілком захищеною.

За результатами проведених досліджень визначено, що однією з найбільш поширених уразливостей з високим ступенем ризику, що притаманна Web-застосуванням, є впровадження SQL-ін'єкцій (SQL – Structured Query Language). Впровадження SQL-ін'єкцій, в залежності від типу СУБД (система управління базами даних) та умов впровадження, надає можливість зловмиснику виконати довільний запит до бази даних (отримати зміст будь-яких таблиць, видалити, додати або змінити дані), також отримати можливість читання та/або запису локальних файлів і виконання довільних команд на скомпрометованому сервері.

Виходячи з цього, досліднику, який займається віддаленим аналізом захищеності Web-застосувань потрібен автоматизований засіб (система) для проведення аналізу Web-застосувань на предмет уразливостей типу SQL-ін'єкції, оскільки ручний (неавтоматизований) аналіз вимагає від виконавця значних затрат часу. Прикладами таких програмних засобів, що мають відкритий код є The Absinthe, SQLiX Injection Scanner, Burp Suite та ін.

В загальному випадку методологія проведення тестування складає, так званий, шаблон текстового сценарію – для опису елементів, що повторюються. Він складається з наступних компонентів:

– вихідні дані (унікальні для кожного тестування);

– спосіб тестування – додавання до очікуваного Web-застосуванням параметрів символів, що не очікуються;

– алгоритм тестування, а саме: оцінка очікуваного значення параметра; додавання набору символів, що призводять до SQL-ін'єкції; оцінка відповіді Web-застосування або повідомлення про помилку;

– набір символів, що використовується для створення тестів (унікальні для кожного тестового сценарію);

– обробка результатів тестування, оцінка їх ефективності та достовірності.

Виходячи з цього можна визначити 5 основних типів тестових сценаріїв спрямованих на: уразливість символьних параметрів, уразливість числових параметрів, уразливість полів пошуку, уразливість полів авторизації, уразливість полів реєстрації. Кожен сценарій містить від 5 до 17 етапів, що значною мірою ускладнює роботу дослідника.

Математичний опис та наукове обґрунтування зазначених тестових сценаріїв значною мірою підвищить ефективність роботи спеціаліста, що займається віддаленим аналізом захищеності Web-застосувань.

Шемендюк О.В. (ВІТІ НТУУ „КПІ”)
к.т.н. Хусаінов П.В. (ВІТІ НТУУ „КПІ”)

# ПРІОРИТЕЗАЦІЯ НАДАННЯ ПОВІДОМЛЕНЬ ПРО ІНЦИДЕНТ БЕЗПЕКИ

Захист серверів, АРМ, контроль з’єднань та аналіз трафіка – це навіть не повний перелік головних завдань адміністратора безпеки. З огляду на те, з якою інтенсивністю можуть з’являтися повідомлення про атаки на комп’ютерну мережу, виникає необхідність встановлення дисципліни обслуговування повідомлень про інциденти безпеки.

Реагування на інциденти безпеки покладаються на відповідальну особу – адміністратора безпеки, який приймає рішення при обробці наданих повідомлень від засобів виявлення вторгнень.

На підставі обмежень щодо діяльності оператора технічної системи, зрозуміло, що адміністратор безпеки не зможе вчасно реагувати на всі повідомлення, що надходять на його робоче місце.

Враховуючи те, що повідомлення про інциденти безпеки розміщуються в черзі на обслуговування та мають різну важливість, необхідно, таким чином, встановити послідовність обробки, щоб адміністратор, в першу чергу, обробляв повідомлення з найвищою важливістю.

Виходячи з аналізу роботи адміністратора безпеки слід зауважити, що своєчасне виконання заходів захисту в значній мірі залежить від пріоритезації обробки повідомлень про інциденти безпеки так, щоб повідомлення від найважливіших елементів комп’ютерної мережі оброблялись в першу чергу.

З огляду на це, можна сказати, що повідомлення від елементів комп’ютерної мережі з низькою важливістю аналізуються менш інтенсивно. Автоматизація процесу пріоритезації повідомлень про інциденти безпеки полягає у розробці алгоритмів надання повідомлень, на основі методів теорії розкладів.

З метою розробки алгоритмів пріоритезації, з урахуванням обмежень діяльності адміністратора безпеки необхідно:

– проаналізувати типові методи теорії розкладів, стосовно роботи адміністратора безпеки;

– розробити можливі алгоритми пріоритезації, стосовно даної предметної області;

– оцінити алгоритми пріорітезації за переліком критеріїв;

– провести моделювання роботи адміністратора безпеки використовуючи методи та алгоритми теорії розкладів;

– зробити висновок та обґрунтування обмежень щодо застосування методів та алгоритмів теорії розкладів при автоматизації процесу пріоритезації повідомлень про інциденти безпеки.