УДК 378.147:004 (043.3) **Зубик Л.В.**

УДОСКОНАЛЕННЯ ФОРМУВАННЯ ПРОФЕСІЙНОЇ КОМПЕТЕНТНОСТІ ІТ-ФАХІВЦІВ

У статті розглянуто можливість удосконалення формування професійної компетентності ІТ-фахівців за рахунок використання проблемного методу навчання. Деталізовано специфічні підходи до забезпечення таких складових професійної компетентності ІТ-фахівця як організація захисту сучасного програмного забезпечення від несанкціонованого доступу. Проілюстровано вразливість таких систем захисту ПЗ, як зовнішнє шифрування, перевірка цілісності, методів заборони відлагодження файлів та заборони трасування, що потребує коригування змісту навчання та залучення інноваційних підходів до викладання спеціальних дисциплін.

***Ключові слова*:** проблемний метод навчання, професійна компетентність ІТ-фахівця, методи захисту програмного забезпечення, інноваційні підходи до навчання

Вступ. Україна стрімко розбудовує інформаційне суспільство, висуваючи на перший план вирішення таких питань, як кібербезпека та боротьба з кіберзлочинністю. Нормативно-правову базу становлять Конвенція Ради Європи про кіберзлочинність, ратифікована Законом України від 07.09.2005 р. № 2824-IV, відповідні закони України та Укази Президента України, положення Кримінального кодексу України, окремі постанови Кабінету Міністрів та рішення РНБО України. У 2007 р. було створено Центр реагування на комп'ютерні інциденти, що ввійшов до складу Державної служби спеціального зв'язку та захисту інформації України. У 2010 р. Указом Президента України «Про виклики та загрози національній безпеці України у 2011 році» ухвалено рішення про започаткування Єдиної загальнодержавної системи протидії кіберзлочинності. Україна поступово нагромаджує досвід у захисті власної ІТ-інфраструктури від сучасних кіберзагроз.

Складнощі у протистоянні фізичному руйнуванню технічних засобів, дезорганізації роботи систем і мереж, порушенню функціонування об'єктів, протиправній діяльності окремих суб'єктів тісно пов'язані з недостатньою кількістю висококваліфікованих фахівців, що відмічено у [1, с. 29], а також необхідністю забезпечення постійного підвищення рівня їх професіоналізму.

Найбільшу загрозу вітчизняним установам і відомствам становить нестача фахівців з інформаційної та кібербезпеки, здатних:

– відшукувати та узагальнювати інформацію про ІТ-системи й мережі, а також про технології та засоби їх впливу на власну інформаційну сферу;

– виявляти ознаки стороннього кібервпливу й моделювати можливі ситуації такого впливу, прогнозуючи відповідні наслідки та підбираючи засоби захисту;

– протидіяти несанкціонованому проникненню сторонніх користувачів у власні ІТ-системи й мережі, забезпечувати стійкість їх роботи, а також відновлення нормального функціонування після здійснення кібератак тощо.

Помітно вища активність звичайних користувачів, професійних шпигунів і/або хакерів (порушників), поряд із зростаючою кількістю способів і методів, до яких вони вдаються з метою пошуку й збору інформації з відкритих і закритих електронних джерел, потужний сплеск розвитку соціальних мереж – це ті чинники, що активізують кіберзлочинність, особливо з огляду на тенденції розвитку інтернету в напрямку інтеграції та об'єднання наявних можливостей у рамках єдиних багатокористувацьких веб-платформ. Саме тому глобальна мережа перетворюється на засіб організації різного роду кібернетичних атак, несанкціонованого доступу (НСД) до сайтів, створення сайтів-двійників тощо. За темпами зростання кіберзлочинність неухильно випереджає інші види організованої злочинності. Чинити дієвий опір таким діям стає дедалі важче, адже заходи з ефективного запобігання небажаним витокам інформації крім технічних механізмів спираються на методи й засоби соціального інжинірингу.

Постановка проблеми. Однією з найбільш актуальних проблем, які виникають у процесі розробки, поширення та використання сучасного програмного забезпечення (ПЗ) є його захист від несанкціонованого доступу. Існують спеціальні засоби для вирішення подібних завдань, найбільш відомими серед яких можна вважати CD-COPS, Star Force, LaserLock, SafeDisk, SecuRom, TAGES, Aladdin, VMProtect, WinLic, Denuvo та ін. Проте більшість програм все-таки потрапляють до категорії "зламаних". Таким чином, проблема несанкціонованого доступу вирішується за рахунок наявності високого кваліфікаційного рівня у відповідних фахівців. Аналогічно повинна вирішуватися не менш актуальна проблема його захисту.

Мета – виявити наявні прогалини у формуванні професійної компетентності майбутніх фахівців з інформаційних технологій та запропонувати доцільне коригування змісту окремих спеціальних дисциплін у поєднанні з інноваційними технологіями навчання.

Методи, організація досліджень. Для виконання поставленої мети нами були використані методи аналізу (системний, проблемно-цільовий, структурний), теоретичного й функціонально-структурного моделювання.

Виклад основної частини дослідження. Майбутня професія студентів ВНЗ, що навчаються на ІТ-спеціальностях, є комплексом значної кількості взаємопов'язаних компонентів, добре володіння якими є показником професіоналізму. Методи навчання, які не активізують пізнавальну діяльність студентів, стають перепоною для формування їх професійної компетентності [2, с. 62]. Одним із способів подолання суперечності між вимогами професії до ІТ-фахівців та стандартною практикою викладання у ВНЗ є широке впровадження проблемних методів навчання. Науково-педагогічні працівники повинні організувати процес професійної підготовки таким чином, щоб постійно створювалися ситуації, які спонукають студентів до роздумів і діяльності за фахом. Наближення процесу навчання до реальних виробничих умов покликане створювати ситуації фахової екстремальності, спрямовані на формування у студентів вміння самостійно приймати рішення і діяти. За таких обставин навчання інтелект студента буде знаходитися у постійному пошуку, що є суттєвим для професійного зростання.

Спробуємо виявити деякі прогалини у формуванні професійної компетентності майбутніх ІТ-фахівців та запропонувати доцільне коригування змісту окремих спеціальних дисциплін, насамперед тих, що вміщують розділи, які стосуються захисту інформації в комп'ютерних системах.

Однією з причин "зламу" захищених програм є відкритість апаратної архітектури ЕОМ. Інструменти, що використовуються при розробці програмного забезпечення, а саме: трейсери, відлагоджувачі, дизасемблери, – використовуються і при його "зламі". Усі наведені у статті приклади відповідають ПЗ, що створювалося для операційної системи Windows. Вразливість таких відомих систем захисту ПЗ, як зовнішнє шифрування, перевірка цілісності тощо є достатньо очевидною. Продемонструємо застосування відлагоджувача для підміни ключа ліцензування на прикладі, що наведений на рис. 1:

```
68 00 01 00 00          push 100
68 84 30 40 00          push crackme4.403084                    403084:"NUWM"
68 E8 03 00 00          push 3E8
FF 75 08                push dword ptr ss:[ebp+8]
E8 62 01 00 00          call <crackme4.GetDlgItemTextA>
68 00 01 00 00          push 100
68 84 31 40 00          push crackme4.403184                    403184:"TEST_SERIAL"
68 E9 03 00 00          push 3E9
FF 75 08                push dword ptr ss:[ebp+8]
E8 4B 01 00 00          call <crackme4.GetDlgItemTextA>
FF 75 08                push dword ptr ss:[ebp+8]
E8 BE 00 00 00          call crackme4.4012F9
83 F8 00                cmp eax,0
74 15                   je crackme4.401255
6A 40                   push 40
68 29 30 40 00          push crackme4.403029                    403029:"Check Serial"
68 60 30 40 00          push crackme4.403060                    403060:"You got it! Congrats! :)"
6A 00                   push 0
E8 49 01 00 00          call <crackme4.MessageBoxA>
EB 13                   jmp crackme4.401268
6A 30                   push 30
68 29 30 40 00          push crackme4.403029                    403029:"Check Serial"
68 36 30 40 00          push crackme4.403036                    403036:"Wrong Serial! Keep trying
6A 00                   push 0
E8 34 01 00 00          call <crackme4.MessageBoxA>
```

Рис. 1. Застосування відлагоджувача для підміни ключа ліцензування

Розглянемо більш детально деякі методи та способи їх зневадження:

– AntiDebug – заборона відлагодження файлу. Подібні ситуації обходяться програмними модулями ScyllaHide та TitanHide.

– AntiDump – заборона зняття MemoryDump. Ситуація обходиться Ollydump.

– AntiTrace – заборона трасування коду. Вона неможлива при використанні IntelPin.

– CodeVirtualize – найбільш складний із методів захисту. Відновлення неможливе, для атак на подібний захист використовують Inline Path.

– FileHashCheck – перевірка цілісності виконуваного файлу.

Існує ще досить багато методів, але всі вони є основними для захисту виконуваних файлів.

Наступним випадком може слугувати сама система ліцензування. Класичний приклад системи ліцензування на основі зашифрованої версії ПЗ полягає у тому, що користувачу видають унікальний ідентифікатор системи; він передає ідентифікатор розробнику та отримує ключ до ПЗ; користувач підтверджує ліцензію і тим самим дешифрує основну частину ПЗ. У подібних алгоритмах є один суттєвий недолік: після підтвердження ліцензії програма знаходиться у пам’яті в незахищеному стані, що дозволяє зняти дамп та використати уже розпаковану версію без будь-яких перевірок ліцензії. Таким чином, існуючий на даний момент часу захист ПЗ не є абсолютно повноцінним та ефективним.

Альтернативою класичному захисту виступає технологія SaaS - **програ́ма як по́слуга** (з *англ. Software as a Service, SaaS*) – модель поширення програм споживачам, за якою постачальник розробляє веб-програму, розміщує й управляє нею (самостійно або через третіх осіб) з метою її використання замовниками через інтернет. Замовники оплачують не факт володіння програмним продуктом, а факт його використання (через API, що доступне через веб і яке часто використовують веб-служби). Проте не все ПЗ може так поширюватися, саме тому ми й розглянемо детально кожен із вище перелічених методів.

Захист від відлагоджувачів Anti-Debugger

Функції:

```
IsDebuggerPresen:
if (IsDebuggerPresent())
   {
      std::cout << "Stop debugging program!" << std::endl;
      exit(-1);
   }
CheckRemoteDebuggerPresent:
Bool DbgDetect;
CheckRemoteDebuggerPresent(OpenProcess(GetCurrentProcessId(), ALL), & DbgDetect);
if(DbgDetect) exit(-1);
```

Структура Windows-процесу Peb

При створенні процесу операційна система заповнює структуру Peb по зміщенню 68h. Вигляд структури наведено на рис. 2.

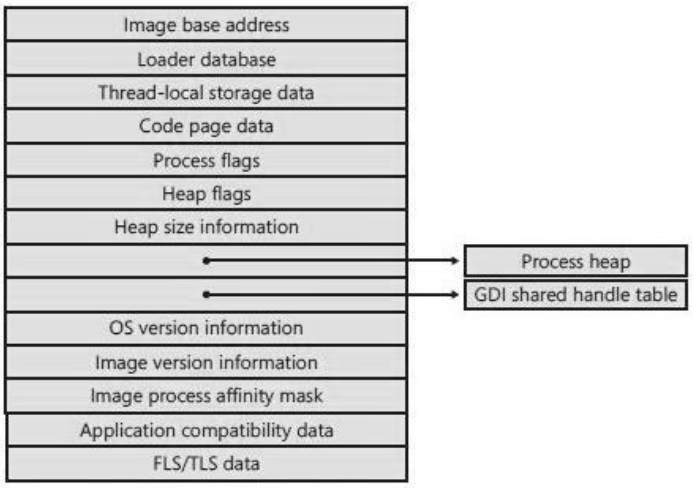

Рис. 2. Вигляд структури

Відповідно, у секції Process Flags деякі елементи маюсь змінне значення при наявності відлагоджувача.

Автоматичне зняття захисту AntiDump

На рис. 3 наведена структура, що встановлює параметри секцій.

```
IMAGE_SECTION_HEADER STRUCT
    Name1                   BYTE        IMAGE_SIZEOF_SHORT_NAME dup(?)
    union Misc
        PhysicalAddress     DWORD       ?
        VirtualSize         DWORD       ?
    ends
    VirtualAddress          DWORD       ?
    SizeOfRawData           DWORD       ?
    PointerToRawData        DWORD       ?
    PointerToRelocations    DWORD       ?
    PointerToLinenumbers    DWORD       ?
    NumberOfRelocations     WORD        ?
    NumberOfLinenumbers     WORD        ?
    Characteristics         DWORD       ?
IMAGE_SECTION_HEADER ENDS
```

Рис. 3. Структура, що встановлює параметри секцій

Захист відбувається через установку SizeOfRawData реальний розмір + FFFFh на останню секцію, що збільшує кількість пам’яті та призводить до зависання програмного забезпечення для peDump.

Перевірка цілісності виконуваного файлу FileHashCheck

Перевірка працює за схемою: CreateFileA->CreateFile Mapping->MapView OfFile->CalcHash. В якості CalcHash можуть використовувати алгоритм CRC32.

Короткий огляд наведених вище методів захисту ПЗ та різних схем їх “зламу” приводить до висновку щодо надзвичайної актуальності концепції проблемного навчання. Адже саме в ній закладено підґрунтя майбутнього творчого розвитку, що зможе слугувати основою професіоналізму, а не звичайного накопичування вже відібраних і запропонованих для опрацювання студентам знань. Не менш важливою для майбутніх фахівців з ІТ є ідея

підвищення міцності знань за умови їх самостійного напрацювання студентами. Кожна педагогічна технологія по-своєму розставляє акценти в ієрархії цілей навчання, хоч би про що саме йшла мова: формування знань, умінь і навичок, особистісний розвиток студентів тощо. Теорія проблемного навчання на сучасному етапі вже має досить стрункий вигляд. Практикою не виявлено суттєвих вад у процесі проблемного навчання.

Все це дозволяє зробити такі висновки:

– про незадовільність діючої системи навчання та зростання потреб у проблемному навчанні;

– виходячи зі специфіки методики, проблемне навчання дійсно теоретично є більш перспективним і складає конкуренцію традиційному навчанню [3].

Оцінювати ефективність тієї чи іншої педагогічної технології надзвичайно важко. Реально результативність методики проблемного навчання значно залежить від того, наскільки адекватно вона була реалізована. Відмітимо, що методики дослідження ефективності педагогічних концепцій повною мірою відображають дійсність, якщо застосовувати комплексну оцінку. Дані проведених досліджень підтверджують, що проблемне навчання забезпечує значне посилення пізнавальної активності, міцне засвоєння знань і їх високу інтеграцію у переважної більшості студентів.

Базуючись на результатах анкетування студентів спеціальності "Комп'ютерні науки та інформаційні технології" Національного університету водного господарства та природокористування, які навчалися на кафедрі комп'ютерних наук за методикою проблемно-орієнтованого навчання впродовж осіннього семестру 2017/2018 н.р. у рамках авторського дослідження з оцінювання ефективності різних методів навчання, зауважимо, що з точки зору студентів позитивні сторони проблемного навчання полягали у ступені заглиблення в процес (61,1% респондентів), можливості прийняття самостійних рішень (38,9% респондентів), усвідомленні наслідків прийнятих рішень (72,2% респондентів) і зростанні мотивації до опанування нового матеріалу (44,4% респондентів). Тому вважаємо доцільним створювати таку систему проблемного навчання, яка б діяла протягом усіх років навчання у вузі.

Щодо зарубіжного досвіду використання методу: у студентів, які пройшли курс проблемного навчання, підтверджено наявність більш досконалого володіння практичними навичками; здатність до самостійного вирішення проблем; краще розвинену самооцінку; більш сформовані навички збору та аналітичного опрацювання інформації тощо [4].

Висновки. Зважаючи на особливості проблемного навчання, відмітимо, що воно виявляється найбільш ефективним саме в тих галузях, де важливі пізнавальна активність, спрямована на постійне розширення теоретичних і практичних пластів знань, а також швидкість вирішення проблем, впевненість у власних силах і самостійність у прийнятті рішень. Відзначимо, що найвищу ефективність проблемного навчання забезпечує не повна відмова від таких традиційних методів, як пояснювально-ілюстративний і репродуктивний, а їх зважене поєднання.

Список використаних джерел:

1. Дубов Д. В. Аналітична доповідь Національного інституту стратегічних досліджень при Президентові України «Кібербезпека: світові тенденції та виклики для України» / Дубов Д. В., Ожеван М. А. // Матеріали міжнародної конференції 26 травня 2011 р. – Київ, 2011. – 31 с.

2. Актуальні проблеми вищої професійної освіти України // Матеріали V Міжнародної науково-практичної конференції 23 березня 2017 р. / За заг. ред. Е. В. Лузік, О. М. Акмалдінової. – К.: НАУ, 2017. – 188 с.

3. Дичківська І. М. Інноваційні педагогічні технології: практикум: навч. посіб. [для студ. вищ. навч. закл.] / І. М. Дичківська; Мін. освіти і науки, молоді та спорту України. – К. : Слово, 2013. – 447 с.

4. Сайт Education USA [Електронний ресурс] – Режим доступу: https://edusa.org.ua (25.11.2017).

Надійшла: 25.03.2018 Рецензент: к.т.н. Довбешко С.В.