УДК 378.147

**В. С. Катаєв**

# ПРОБЛЕМИ ПІДГОТОВКИ ФАХІВЦІВ У СФЕРІ КІБЕРБЕЗПЕКИ

Вінницький національний технічний університет

**Анотація**

Активний розвиток інформаційних систем і, як наслідок, значне зростання об’ємів передачі інформації та електронного документообігу, призводить до того, що захист інформації у всіх її проявах, стає однією із важливих сфер людської діяльності, а загострення специфічних проблем для даної галузі, вимагає досвідчених фахівців для їх вирішення. У даній роботі розглядаються основні проблеми, що виникають при підготовці здобувачів спеціальності «Кібербезпека» та пропонуються підходи до їх вирішення, реалізація яких дозволить підвищити якість підготовки студентів.

**Ключові слова:** кібербезпека, загрози для інформації, технічний захист інформації.

**Abstract**

Active development of information systems and significant growth of data transmission and electronic document flow are makes information protection an important area of human activity, aggravation of specific problems for this industry, are requires experienced professionals to solve them. This paper examines the main problems that arise in the preparation of cybersecurity majors and proposes approaches to their solution, the implementation of which will improve the quality of student preparation.

**Keywords:** cybersecurity, threats to information, technical protection of information.

Очевидним є той факт, що сьогодні інформаційні технології захоплюють все більше сфер людської діяльності. Активний розвиток телекомунікаційних, інформаційних і комп’ютерних систем та їхня інтеграція в інформаційне суспільство, обумовлюють життєво важливі ролі, які вони відіграють у медицині, фінансах, виробництві та національній безпеці. Обробка та зберігання інформації у цифровій формі надають особливого значення питанню інформаційної безпеки і захисту інформації та, відповідно, підготовки спеціалістів у даній сфері.

Захист інформації являє собою цілеспрямовану діяльність, спрямовану на виключення або суттєве обмеження неконтрольованого та несанкціонованого поширення (витоку) відомостей, що захищаються, а також різних видів впливів на функціональні інформаційні процеси, що реалізуються. Велику роль, при цьому, відіграє захист інформації від витоку, через технічні канали витоку. Під технічним каналом розуміють сукупність об'єкта розвідки, технічного засобу розвідки, за допомогою якого отримують інформацію про цей об'єкт, та фізичного середовища, в якому поширюється інформаційний сигнал. При вивченні основних принципів технічного захисту інформації питання експериментальних та лабораторних досліджень мають не менше значення ніж лекційні матеріали, а при вивченні окремих питань є, навіть, більш значущими, оскільки опанувати їх лише теоретично, просто неможливо. Таким чином, постає перша проблема підготовки спеціалістів у сфері кібербезпеки – це матеріально-технічне забезпечення навчального процесу. Звичайно, сьогодні ця проблема актуальна для будь-якої спеціальності у будь-якій сфері в країні, але для «Кібербезпеки» вона є більш гострою з багатьох причин.

По перше, це велика номенклатура устаткування та обладнання необхідного для достатнього опанування важливих питань із захисту інформації. Наприклад, при вивченні, зазначених вище, технічних каналів витоку інформації, студент повинен зрозуміти принципи функціонування, як засобів розвідки, що використовують даний канал, так і пристроїв захисту від них. Звичайно, що краще за все, він опанує дане питання, коли буде безпосереднім учасником процесу витоку та захисту інформації, що можна реалізувати у вигляді лабораторної роботи. Відповідно в навчальній лабораторії повинні бути, як модель засобу розвідки, так і модель засобу захисту. Проблема у тому, що технічних каналів існує велика кількість: акустичні, віброакустичні, акустоелектричні, лазерні акустичні і т.д., і кожен має свої особливості, у кожному використовуються свої методи та засоби зняття інформації та свої методи та засоби її захисту [1]. Поряд з технічними каналами йдуть закладні пристрої або апаратні закладки. Це мініатюрні пристрої, які слугують для перехоплення інформації, прикладом є портативні диктофони, провідні та радіо мікрофони та мініатюрні відеокамери. Захист від таких пристроїв здійснюється з допомогою окремої спеціальної пошукової апарату-

ри. Причому, в даному випадку, необхідно так само враховувати всі технічні характеристики та особливості роботи конкретних закладок, адже від принципу їх роботи буде залежати і метод, яким можна буде їх виявити. І все це лише невелика частинна питань з інформаційної безпеки з якими необхідно розібратись майбутньому спеціалісту.

По друге, засоби та устаткування, що використовуються на практиці у даній сфері є досить специфічними і вузько направленими. Так, наприклад для пошуку мініатюрних відеокамер використовуються тепловізори [2] або спеціальні оптичні пристрої, а для пошуку диктофонів – нелінійні локатори [3]. Для зняття, інформації через лазерні канали використовуються лазерні мікрофони, у випадку віброакустичних каналів – електроні стетоскопи, а для протидії їм використовуються спеціалізовані комплекси. Зазначене обладнання, звичайно є дуже дороговартісним, і забезпечити ним навчальний процес не є можливим, але, як зазначалось раніше, без відповідного обладнання, неможливо підготовити реального спеціаліста у даній сфері.

Вирішити дану проблему можна шляхом використання аналогів відповідного обладнання або лабораторних моделей, які функціонують за тими ж базовими принципами. Яскравий приклад, такого підходу наведений у статті [4], де автори досліджують питання реалізації лазерного мікрофону. Такі пристрої дозволяють отримувати акустичну інформацію з приміщення на значних відстанях і взагалі без необхідності проникнення всередину. Зняття інформації здійснюється наступним чином, лазерним променем опромінюється певна поверхня чи конструкція приміщення, яка вібрує в акустичному полі, лазерний промінь модулюється по закону вібрації поверхні і відбивається у зворотному напрямку, після він перехоплюється приймачем, демодулюється і з нього виділяється мовна інформація. Для реалізації демонстраційного пристрою автори використали наступні елементи: гелій-неоновий лазер, кремнієва сонячна панель, аудіопідсилювач та навушники, портативна стереосистема (радіо) та звичайне віконне скло. Зібрана установка мала наступну конфігурацію. Віконне скло встановлене на стіл, а за ним розміщувалось радіо з якого лунала музика. Лазерний промінь спрямовувався на вікно, під таким кутом, щоб відбитий якої подавались дротом на підсилювач, а потім на навушники. В результаті в навушниках було чути музику, що лунає з радіо. Тобто, авторам вдалось, за допомогою такої простої системи, фактично відтворити базовий принцип передачі звукової інформації по лазерному променю, що використовується у професійних лазерних мікрофонах. Звичайно, така система буде мати величезну кількість недоліків в порівнянні з серйозними пристроями. Але при цьому буде одна і дуже важлива перевага, вартість професійного лазерного мікрофону може становити десятки тисяч доларів, що на порядки більше вартості подібної установки. А з точки зору навчання студентів, вона буде мати не меншу цінність, оскільки дозволить зрозуміти базові принципи функціонування таких пристроїв в цілому.

Однак, не для кожної задачі можливо реалізувати макет чи практичну модель, і в такому випадку слід використовувати електронні та програмні засоби навчального призначення, а також системи автоматизованого проектування та програмні засоби комп'ютерної математики. Доволі, ґрунтовний аналіз деяких з них наведено у роботі [4], де автори розглядають можливість розробки принципів класифікації та аналіз систем комп'ютерної математики , як середовища розробки програмних засобів навчального призначення. При підготовці студентів спеціальності «Кібербезпека» в першу чергу слід звернути на наступні категорії програмних засобів:

1. Спеціалізовані програми і пакети (Advanced Grapher, Axum, Dynamic Solver, Electronics Work-Bench, Grapher, Gran1, Gran-3D, MathPlot, MicroCAP, SigmaPlot, Proteus, Simulink) – вони дозволять реалізовувати дослідження базових принципів утворення технічних каналів витоку цифрової інформації, на рівні електричних схем та у вигляді окремих блоків обчислювальних машин.
2. Системи комп'ютерної математики (CMS — Computer Mathematical System) або універсальні математичні системи (GAUSS, MathCad, Matlab, Maple, Mathematica) – дані засоби дозволять студентам систематизувати та оптимізувати розрахунки рівнів небезпечних сигналів у різних середовищах поширення та показників захищеності інформації.

Звичайно, не кожний пристрій технічної розвідки або технічного захисту інформації, можна замінити простою функціональною моделлю, не кожний метод захисту можна продемонструвати у вигляді лабораторної роботи, не кожну проблему захисту можна дослідити експериментально або віртуально. Але слід пам'ятати, насправді спеціалістом може називатись та людина, яка не тільки знає як робити, а й вміє ці знання застосувати на практиці, у реальних умовах. Тому, надважливим є завдання показати студенту у достатній мірі саме практичну сторону захисту інформації.

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Том 1. Технические каналы утечки информации./ А.А. Хорев - М.: НПЦ «Аналитика», 2008. - 436 с.

2. Яремчук Ю.Є., Катаєв В.С., Гижко М.Ю. Можливості практичного застосування тепловізорів у питаннях захисту інформації. — "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні" — 2016 — №1.- С.99-105.

3. Катаєв В.С. Дослідження проблеми локалізації закладних пристроїв при застосуванні нелінійної локації Тези доповідей, Тези доповідей II-ої Міжнародної науково-технічної конференції «Інформаційна безпека в сучасному суспільстві». – Львів, 2016. – С. 50–51.

4. James M. Moses, K.P. Trout. A Simple Laser Microphone for Classroom Demonstration - The Physics Teacher Vol. 44, December 2006

5. Тютюнник О. І., Михалевич В. М. Використання систем комп'ютерної математики для створення програмних засобів навчального призначення - Вісник Вінницького політехнічного інституту — 2013 — № 6 . – С. 111–116.

**Катаєв Віталій Сергійович** – аспірант кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, kataev@vntu.net.

Науковий керівник: **Яремчук Юрій Євгенович** – д.т.н., професор кафедри кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця.

**Vitalii Kataiev**– graduate student of the Department of Management and Security of Information Systems; Vinnytsia National Technical University , Vinnytsia, kataev@vntu.net.

Supervisor: **Iurii Iaremchuk** - doctor of sciences, professor of the Department of Management and Security of Information Systems; Vinnytsia National Technical University , Vinnytsia.