$s = (s_{L(s)-1}, \text{K}, s_0)$, $0 < r < n$, $0 < s < n$, длину цифровой подписи L_D: $L_D \geq 2L(n)$, кратную 16. Функция должна возвращать цифровую подпись $D = (D_{L_D-1}, \text{K}, D_0)$ длиной L_D.

Функция предназначена для выполнения преобразование цифровой подписи в байтовую последовательность, где части (r, s) следуют друг за другом (старший байт первым), для однозначной интерпретации различными программными продуктами.

Преобразование массива байт, содержащего цифровую подпись, в пару целых чисел согласно п. 5.11 стандарта

Функция преобразования массива байт, содержащего цифровую подпись, в пару целых чисел содержит в качестве аргументов двоичный ряд $D = (D_{L_D-1}, \text{K}, D_0)$ четной длины L_D. Функция должна возвращать пару целых чисел $r = (r_{L(r)-1}, \text{K}, r_0)$ и $s = (s_{L(s)-1}, \text{K}, s_0)$.

Функция предназначена для выполнения преобразования байтовой последовательности (где части (r, s) следуют друг за другом – старший байт первым) в числа (r, s) цифровой подписи – для однозначной интерпретации различными программными продуктами.

УДК 612.391

ПРО НАПОВНЕННЯ ЗМІСТУ ПРОФІЛЮЮЧИХ НАВЧАЛЬНИХ ДИСЦИПЛІН СПЕЦІАЛІЗАЦІЇ “ЕЛЕКТРОННІ АПАРАТИ БАНКІВСЬКИХ СИСТЕМ І ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ”

Юрій Зіньковський, Вадим Клименко
НТУУ „КПІ”

Анотація: **Приведені дані профілюючої дисципліни навчального плану спеціалізації.**
Summary: **The date of profile subject of educational curriculum specialization.**
Ключові слова: **Спеціалізація “Електронні апарати банківських систем і засоби захисту інформації”, профілююча дисципліна.**

Відповідно до Постанови КМУ № 664 від 23. 04. 1999 р. “Про розроблення та запровадження науково-обґрунтованої системи підготовки спеціалістів в галузі технічного захисту інформації” в Національному технічному університеті України “Київський політехнічний інститут” на Радіотехнічному факультеті на кафедрі Радіоконструювання і виробництва радіоапаратури відкрита нова спеціалізація “Електронні апарати банківських систем і засоби захисту інформації”. Нині відбудеться перший випуск спеціалістів нової спеціалізації. Нормативні матеріали навчального процесу створені для забезпечення необхідної якості підготовки спеціалістів нового навчального напряму, яка б відповідала сучасним вимогам.

Профілюючою дисципліною навчального плану спеціалізації є дисципліна “Методи та апаратура захисту інформації”.

Дисципліна читається для спеціалістів та магістрів спеціалізації “Електронні апарати банківських систем і засоби захисту інформації” спеціальності “Виробництво електронних засобів” у десятому семестрі кафедрою Радіоконструювання і виробництва радіоапаратури обсягом 135 навчальних годин (68 – аудиторних; 67 – курсова робота та самостійна робота студентів). Аудиторні години: 51 – лекції; 17 – лабораторні заняття.

Мета вивчення дисципліни — надати випускникам спеціалізації (спеціалістам та магістрам) необхідні знання в галузі захисту інформації, що дозволить їм розробляти та запроваджувати необхідні методи та технічні рішення щодо захисту інформації в процесах та операціях інформаційної діяльності. Курс дисципліни має за мету вивчення організаційно-методичних, аналітичних, фізичних, інженерно-фізичних, теоретико-інформаційних, алгоритмічних, програмно-технічних аспектів проблеми, а основних можливих каналів витоку та несанкціонованого вилучення інформації; пошуку, нейтралізації та знешкодження каналів можливої втрати інформації. Метою також є вивчення методів упорядкування діяльності, стандартизації та сертифікації в галузі захисту інформації.

До складу тематичного плану дисципліни увійшло одинадцять розділів:

- основні поняття, визначення, функціональні та методичні завдання захисту інформації;
- правове та нормативно-метрологічне забезпечення системи захисту інформації;
- ліцензійні умови та правила проведення підприємницької діяльності, пов'язаної з технічним захистом інформації;
- стандартні методи та засоби захисту інформації;
- основні технічні канали загроз несанкціонованого вилучення інформації та можливих атак на інформацію;
- методи, технічні засоби та апаратура захисту інформації, виявлення та знешкодження засобів можливої атаки;
- методи захисту інформації в автоматизованих інформаційних системах, комп'ютерах, комп'ютерних мережах зв'язку;
- захист інформації в інформаційно-захищених приміщеннях та офісах;
- захист інформації в банківських комп'ютерах та серверах;
- перспективи використання ультразвукової інтроскопії для захисту інформації;
- захист інформації масових роздрібних електронних платежів в мережі Інтернет платіжної системи „Пейкеш" України.

Правовою базою постановки нового навчального процесу є Закони України "Про інформацію", "Про захист інформації в автоматизованих системах", "Про державну таємницю", "Про національну систему конфіденційного зв'язку", постанови КМУ: "Концепція технічного захисту інформації в Україні", "Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю" та ін.

Становленню та вдосконаленню навчального процесу в галузі захисту інформації сприяє на кафедрі Радіоконструювання та виробництва радіоапаратури колектив науково-дослідного Центру систем технічного захисту інформації "ТЕЗІС" НТУУ "КПІ".

Щорічно проходять переддипломну практику та захищають атестаційні роботи за тематикою НДЦ бакалаври, спеціалісти та магістри кафедри.

Багато з них розподіляються в установи замовників фахівців, в тому числі і в колективі НДЦ "ТЕЗІС".