С. Г. Рассомахін, І. Д. Горбенко,
М. В. Єсіна

Досвід сумісного використання комп'ютерних та мультимедійних засобів в освітньому процесі

Розглянуто два навчальні комплекси – комплекс центру сертифікації ключів та інтерактивний мультимедійний комплекс. Описано склад кожного із комплексів та їхнього застосування. Подано навчально-методичні матеріали та нормативне забезпечення, що застосовують для навчання під час використання центру сертифікації ключів. Наведено графічні зображення процесу роботи з кожним із комплексів під час занять зі студентами. Окреслено основні переваги використання таких комплексів у процесі навчання. Зроблено висновки щодо оптимальності та необхідності використання таких комплексів в освітньому процесі.

Ключові слова: електронний документообіг, електронний підпис, мультимедійний комплекс, центр сертифікації ключів.

У XXI сторіччі у світовому інформаційному просторі та інформаційних просторах держав вирішуються складні завдання переходу до використання систем електронних документів та електронного документообігу, електронної торгівлі, електронних банківських систем, електронних баз даних тощо. Електронні системи широко впроваджують у науці, освіті, управлінні державою. Одночасно із зазначеним, у таких системах виникли суттєві протиріччя, пов'язані зі складністю надання в них користувачам і власникам послуг цілісності, справжності, доступності, неспростовності з необхідним рівнем гарантій, які вимагають вирішення. Особливо актуальними ці проблеми стали з прийняттям у державах на міжнародному рівні, у тому числі в Україні, основоположних законів «Про електронні документи та електронний документообіг», «Про електронний цифровий підпис», «Про захист інформації в інформаційно-телекомунікаційних системах», «Політики сертифікації ключів» тощо. Особливо проблемними ці питання стали з прийняттям закону «Про електронні довірчі послуги».

На виконання цих законів в Україні створено інфраструктуру відкритих ключів, перш за все – для підтримки системи (електронного) цифрового підпису. Першорядним завданням в Україні, що вимагає свого вирішення, є надання органам державної влади, місцевого самоврядування, юридичним та фізичним особам послуг із забезпечення цілісності, справжності, неспростовності, в більшості випадків – і конфіденційності інформації та різноманітних даних, які подано в електронному вигляді, а також електронних документів і повідомлень, програмного забезпечення, що ними використовуються. Крім того, у зв'язку з інтеграцією України у світовий інформаційний простір, важливим є завдання забезпечення взаємодії органів

державної влади, місцевого самоврядування, юридичних та фізичних осіб на світовому рівні, з використанням іноземних і міжнародних інформаційних та інформаційно-комунікаційних систем, різноманітних інформаційних технологій, відкритих систем типу мережі Інтернет. Практичний досвід і аналіз можливостей показують, що одним із основних і комплексних засобів забезпечення надання зазначених послуг є застосування електронного (цифрового) підпису (ЕП) [1, 3].

Комплекс, що розглядається у цій роботі, є унікальним, оскільки саме такої структури та методичного забезпечення на сьогодні немає в жодному закладі вищої освіти країни. У Національному університеті «Львівська Політехніка» та Державному університеті телекомунікацій встановлено більш спрощену версію *центру сертифікації ключів* (далі – ЦСК), а у Харківському національному університеті радіоелектроніки встановлено програмну версію ЦСК. Також планується ще встановлення центрів сертифікації ключів у Одеській національній академії зв'язку імені О. С. Попова та Київському національному університеті імені Тараса Шевченка, але на цей момент лише ведуться переговори щодо впровадження ЦСК у цих закладах вищої освіти.

Основні переваги розробки полягають у тому, що для цілей навчання створено реально працюючий навчальний ЦСК, який реалізує практично усі функції справжнього акредитованого центру сертифікації ключів. Для максимальної ефективності освітнього процесу розроблена та використовується широка номенклатура настанов та методичних розробок із вивчення та дослідження основних режимів роботи операторів та технічних засобів центру. Фактично, в результаті навчання за відповідними дисциплінами кафедри студенти стають фахівцями у галузі електронного підпису (далі – ЕП) та мають добрі практичні навички.

Інноваційний характер цієї розробки підкріплюється використанням для навчання студентів сучасного повнофункціонального інтерактивного мультимедійного комплексу, аналога якому поки що немає в межах університету. На рис. 1–3 показано процес проведення занять із використанням комплексу центру сертифікації ключів та начального мультимедійного комплексу, а також наведено зображення навчально-методичного забезпечення комплексу (монографії, що розроблені за участі співробітників кафедри безпеки інформаційних систем і технологій).

1. Використання комплексу центру сертифікації ключів

До складу комплексу апаратно-програмних засобів діючого центру сертифікації ключів (ЦСК) національної системи цифрового підпису входить:

– локальна обчислювальна (із доступом до глобальної) мережа;

– комплект мережевого та спеціального обладнання центру сертифікації ключів у складі маршрутизаторів, мережевого криптомодуля «Гряда-301» та IP-шифраторів «Канал-301» (розробка та виробництво АТ «ІІТ»);

– комплект програмного забезпечення функціонування центру сертифікації ключів, фрагмента захищеної мережі та начального мультимедійного комплексу.

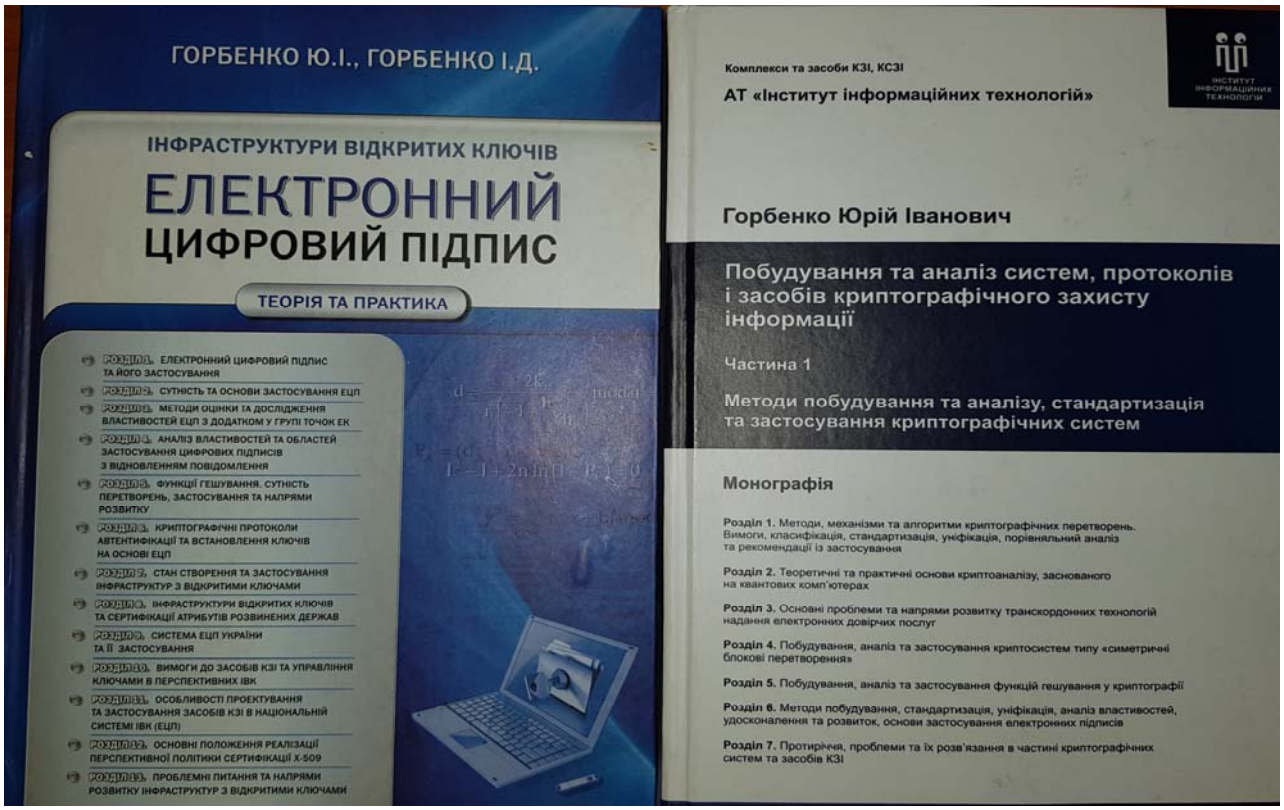

Рис. 1. Склад навчально-методичного забезпечення комплексу

До складу нормативного забезпечення щодо роботи з центром сертифікації ключів входять [2, 3]:

Програмно-експлуатаційна документація:

1) програмний комплекс робочої станції ЦСК;
2) програмний комплекс управління IP-шифраторами;
3) програмний комплекс центру сертифікації ключів;
4) програмний комплекс підготовки параметрів криптографічних алгоритмів і протоколів;
5) програмний комплекс захисту інформації на носіях користувача;
6) програмний комплекс користувача центру сертифікації ключів;
7) програмний комплекс захисту інформації на носіях сервера;
8) програмний комплекс управління шлюзами захисту з'єднань;
9) програмний комплекс клієнта захисту з'єднань.

Настанови програмістам:

1) програмний комплекс користувача ЦСК;

2) програмний комплекс користувача ЦСК. Бібліотека користувача ЦСК «Підпис (OS MS Windows)»;

3) програмний комплекс ЦСК. Службовий програмний комплекс центральних серверів ЦСК;

4) комплекс робочої станції генерації ключів користувачів ЦСК;

5) службовий програмний комплекс центральних серверів ЦСК;

6) програмний комплекс формування та публікації СВС;

7) програмний комплекс центральних серверів ЦСК. Програмний комплекс сервера обробки запитів (CMP-сервера);

8) програмний комплекс користувача ЦСК. Бібліотека користувача ЦСК «Підпис (OS Linux/UNIX)»;

9) програмний комплекс користувача ЦСК. Бібліотека користувача ЦСК «Підпис (Java)».

Настанови операторам:

1. Програмний комплекс користувача ЦСК.
2. Програмний комплекс ЦСК. Програмний комплекс управління ключами ЦСК та серверів ЦСК.
3. Програмний комплекс ЦСК. Програмний комплекс центральних серверів ЦСК. Програмний комплекс монітора TSP-сервера.
4. Програмний комплекс захисту електронної пошти для MS Outlook.
5. Програмний комплекс ЦСК. Комплекс адміністратора безпеки.
6. Програмні компоненти (бібліотеки) носіїв ключової інформації.
7. Програмний комплекс шлюзу захисту з'єднань.
8. Програмний комплекс захисту IP-потоку.
9. Програмний компонент аварійного відключення захищених носіїв на сервері через мережу.
10. Програмний комплекс ЦСК. Комплекс адміністратора реєстрації.
11. Програмний комплекс віддаленого адміністратора реєстрації ЦСК.

Апаратура та методичне забезпечення дозволяють реалізувати теоретичне та практичне вивчення широкого переліку питань функціонування ЦСК та захищених комп'ютерних мереж, серед яких:

– отримання сертифікатів із ЦСК;

– перегляд сертифікатів відкритих ключів;

– блокування власного сертифіката;

– передача запитів за допомогою сервера обробки запитів ЦСК, засобами електронної пошти, за допомогою файлу запиту;

– формування нового сертифіката;

– прийом відповідей на запити;

– управління ключами: генерація ключів, державні алгоритми та протоколи, міжнародні алгоритми та протоколи;

– робота з ключовою інформацією: зчитування особистого ключа, резервне копіювання особистого ключа, зміна паролю захисту особистого

ключа; знищення особистого ключа на носієві, знищення особистого ключа в пам'яті;

– перегляд власного сертифіката;

– захист файлів: підпис файлів, перевірка файлів, шифрування, розшифрування файлів;

– робота з веб-сайтом центра сертифікації ключів та ін.

Рис. 2. Під час занять із центром сертифікації ключів

2. Використання інтерактивного мультимедійного комплексу

До складу навчального мультимедійного комплексу входять:

– оптична інтерактивна дошка «НТ-77»;

– короткофокусний проектор «Epson-435»;

– документ-камера «Epson-EDC 11» та ін.

Апаратура та програмно-методичне забезпечення інтерактивного комплексу у складі комп'ютера викладача, інтерактивної оптичної дошки, короткофокусного проектора та документ-камери дозволяють реалізувати такі функції:

– демонстрацію створення та роботу в реальному часі програмних моделей за допомогою сенсорних функцій оптичної інтерактивної дошки;

– створення та демонстрацію відео і аудіо методичних матеріалів у процесі проведення лекцій та практичних занять, навчальних відеороликів тощо;

– використання функцій «безмежної дошки» у разі графічного викладення матеріалу;

– використання режиму рецензування та редагування графічних матеріалів навчальних презентацій;

– демонстрацію різних об'єктів у 3D-режимі з використанням цифрового 10-разового зуму та можливістю редагування зображень безпосередньо на площині інтерактивної дошки та ін.

Рис. 3. Під час занять із використанням інтерактивної дошки та документ-камери

Таким чином, перевагами розробки, описаної у статті, є:

– максимальний ступінь індивідуалізації навчання разом зі збереженням групової форми занять;

– можливість для кожного студента вивчати і виконувати функції адміністраторів та інженерів центру сертифікації ключів;

– інтенсифікація використання часу для навчання і комп'ютерної техніки за рахунок інтерактивних технологій мультимедійного комплексу;

– глибокий і об'єктивний контроль ступеня освоєння матеріалу за рахунок використання автоматизованих методів тестування студентів;

– практична форма навчання, що підвищує інтерес до знань;

– гнучкість методичного і програмного забезпечення та ін.

Значення вищенаведеної розробки полягає у тому, що на сьогодні вирокистання комплексу центру сертифікації ключів та інтерактивної програмно-методичної технології значно підвищує якість викладання низки дисциплін кафедри безпеки інформаційних систем і технологій факультету комп'ютерних наук.

Література

1. Горбенко І. Д. Прикладна криптологія. Теорія. Практика. Застосування : підручник. / І. Д. Горбенко, Ю. І. Горбенко. – Харків : Форт, 2013. – 868 с.

2. Горбенко Ю. І. Методи побудування та аналізу, стандартизація та застосування криптографічних систем : монографія / Ю. І. Горбенко. – Харків : Форт, 2016. – 959 с.

3. Горбенко Ю. І. Інфраструктури відкритих ключів. Системи ЕЦП. Теорія та практика / Ю. І. Горбенко, І. Д. Горбенко. – Харків : Форт, 2010. – 593 с.