Scientific journal
PHYSICAL AND MATHEMATICAL EDUCATION
Has been issued since 2013.

Науковий журнал
ФІЗИКО-МАТЕМАТИЧНА ОСВІТА
Видається з 2013.

ISSN 2413-158X (online)
ISSN 2413-1571 (print)

http://fmo-journal.fizmatsspu.sumy.ua/

Жданова Ю.Д., Спасітєлєва С.О., Шевченко С.М. Формування у студентів ІТ-спеціальностей компетентностей в області захисту інформації з використанням криптографічних служб .NET FRAMEWORK Фізико-математична освіта. 2019. Випуск 1(19). С. 48-54.

Zhdanova Yu., Spasiteleva S., Shevchenko S. Formation Of Information Protection Competence To Students Of It-Specialties With Using .Net Framework Cryptographic Services. Physical and Mathematical Education. 2019. Issue 1(19). P. 48-54.

DOI 10.31110/2413-1571-2019-019-1-008
УДК 378.147:004.056.5

Ю.Д. Жданова
Київський університет імені Бориса Грінченка, Україна
y.zhdanova@kubg.edu.ua
ORCID: 0000-0002-9277-4972
С.О. Спасітєлєва
Київський університет імені Бориса Грінченка, Україна
s.spasitielieva@kubg.edu.ua
ORCID: 0000-0003-4993-6355
С.М. Шевченко
Київський університет імені Бориса Грінченка, Україна
s.shevchenko@kubg.edu.ua
ORCID: 0000-0002-9736-8623

ФОРМУВАННЯ У СТУДЕНТІВ ІТ-СПЕЦІАЛЬНОСТЕЙ КОМПЕТЕНТНОСТЕЙ В ОБЛАСТІ ЗАХИСТУ ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ КРИПТОГРАФІЧНИХ СЛУЖБ .NET FRAMEWORK

АНОТАЦІЯ

Формулювання проблеми. *Стаття присвячена проблемі підготовки сучасних фахівців галузі знань «12-Інформаційні технології» (ІТ), а саме формування у студентів спеціалізовано-професійних знань та умінь з криптографічного захисту інформації.*

Матеріали і методи. *У дослідженні були використані теоретичні методи аналізу та узагальнення наукових праць провідних методистів, що розглядали реалізацію компетентнісного підходу у вищій школі, зокрема компетентності майбутніх ІТ-спеціалістів; порівняльні методи зіставлення різних існуючих криптографічних сервісів захисту інформації у процесі вивчення навчальних дисциплін «Прикладна криптологія», «Безпека програм та даних», «Технології безпечного програмування», «Об'єктно-орієнтоване програмування».*

Результати. *Доведена необхідність отримання компетентностей з захисту інформації з визначеним обсягом теоретичних та практичних знань для майбутніх ІТ-спеціалістів трьох спеціальностей: 121 Інженерія програмного забезпечення, 122 Комп'ютерні науки, 125 Кібербезпека. Спираючись на дослідження у психолого-педагогічній літературі та власний досвід, деталізовані суть та структура поняття «компетентності ІТ- спеціаліста з криптографічного захисту інформації». Зроблено наголос на те, що формування даних компетентностей здійснюється у рамках міждисциплінарних зв'язків навчальних дисциплін, а саме: «Прикладна криптологія», «Безпека програм та даних», «Технології безпечного програмування», «Об'єктно-орієнтоване програмування». Визначено перелік вимог до рівня сформованості професійно-значимих характеристик ІТ-спеціаліста в сфері криптографічного захисту інформації. Здійснено аналіз криптографічних бібліотек та запропоновані головні критерії вибору криптографічної служби та сучасного середовища розробки програм. Обґрунтовано актуальність та доцільність використання сучасних криптографічних служб .Net Framework та середовища розробки прикладних програм сімейство інструментів Microsoft Visual Studio для набуття студентами знань та практичних навичок з захисту інформації. Розроблено модель формування та розвитку компетентностей з криптографічного захисту інформації студентів галузі знань «12-Інформаційні технології» та представлено шляхи її реалізації у Київському університеті імені Бориса Грінченка та Державному університеті телекомунікацій.*

Висновки. *Саме на базі програмування криптографічних механізмів захисту інформації ефективно формуються практичні навички застосування криптографічних алгоритмів у процесі опрацювання та передачі даних. Конкретизоване визначення обсягу теоретичних знань та практичних умінь з врахуванням міждисциплінарних зв'язків навчальних дисциплін, пов'язаних з захистом інформації та програмуванням, дозволяє підготувати фахівців з практичними навичками з криптографічного захисту інформації, які є затребуваними на ринку праці.*

КЛЮЧОВІ СЛОВА: *компетентності ІТ-спеціалістів, захист інформації, криптографічний захист, криптографічна бібліотека, криптографічні алгоритми.*

ВСТУП

Постановка проблеми. Головною метою закладів вищої освіти, які готують фахівців галузі знань «12- Інформаційні технології», є підготовка випускників до професійної діяльності в сучасному високорозвиненому інформаційно-комунікаційному середовищі. Тотальна інформатизація суспільства вимагає від освіти вирішення проблеми підготовки таких ІТ-спеціалістів, які в умовах мінливих реалій сьогодення мають бути здатними не тільки сприймати і поновлювати інформацію, а й опрацьовувати її, зберігати та створювати нову. Особливе місце посідає підготовка ІТ-спеціаліста до виконання важливої задачі захисту інформації, яка передбачає вміння використовувати цілий комплекс спеціальних засобів захисту інформації: нормативно-правових, фізичних, інженерно-технічних, криптографічних. Важливість і актуальність питань захисту інформації вже давно вийшли на одне з перших місць серед інших завдань, що вирішуються в процесі проектування, створення та використання сучасних інформаційно-комунікаційних систем. Останнім часом реальні масштаби комп'ютерної злочинності та реальні збитки від несанкціонованого доступу до інформації продовжують зростати (Глобальное исследование утечек конфиденциальной информации в первом полугодии 2018 года). Більшість загроз цілісності і конфіденційності інформації, що циркулює в комп'ютерних системах, можна попередити за допомогою криптографічних методів захисту. Тому підготовка сучасного ІТ-спеціаліста має обов'язково містити знання та уміння з криптографічного захисту інформації в обсязі, передбаченому спеціальністю. Все це підтверджує актуальність визначеної проблеми і спонукає до пошуків шляхів формування у майбутніх фахівців компетенцій в області криптографічного захисту інформації.

Аналіз актуальних досліджень. Дослідники компетентнісного підходу в освіті такі, як І. Єрмаков, І.О. Зимня, А.Г. Каспржак, Т.М. Сорочан, Л.Л. Хоружа, відзначають, що відмінність компетентного фахівця від кваліфікованого полягає у тому, що перший не тільки володіє певним рівнем знань, умінь, навичок, але здатний реалізовувати їх на практиці. Д. Іванов, О. Окуловський зазначають, що компетентнісний підхід – це спроба привести у відповідність рівень освіти необхідного фахівця і потреби ринку праці. Ми згодні з думкою цих вчених, які вважають, що такий підхід акцентує увагу на результат навчання, а сам результат розглядається не як сума засвоєної інформації, а здатність людини на її основі адекватно діяти у різних ситуаціях (Панфілов & Фурманець, 2017).

Реалізація компетентнісного підходу у вищій школі виявила низку проблем щодо здійснення цього процесу. Серед них – відсутність практичної складової, бо компетентнісний підхід цінує не знання, а уміння їх використовувати у професійній діяльності.

Саме тому дослідники вказують на необхідність змін характеру зв'язків і відносин між навчальними дисциплінами. Зв'язки і відносини між навчальними предметами визначаються прийнятою моделлю компетенцій та очікуваними результатами навчальної діяльності (Бурячок, Богуш, Борсуковський, Складанний & Борсуковська, 2018). Для кожної компетенції необхідно набуття знань, умінь, навичок і досвіду діяльності, які можуть розглядатися в рамках різних навчальних дисципліна. Реалізація компетентнісного підходу висуває серйозні вимоги до методики навчання, вимагає уточнення і коригування навчальних і робочих планів, програм навчальних дисциплін. Наші дослідження базуються на досвіді викладання дисциплін «Прикладна криптологія», «Безпека програм та даних», «Технології безпечного програмування», «Об'єктно-орієнтоване програмування» для спеціальностей 121 Інженерія програмного забезпечення, 122 Комп'ютерні науки, 125 Кібербезпека.

Освітні стандарти з ІТ-спеціальностей – це інструмент для визначення сучасних програм підготовки фахівців для ІТ-індустрії. Сьогодні в Україні розроблено освітні стандарти для галузі знань «12-Інформаційні технології». ІТ-спеціальність декларує свій погляд на систему та результати навчання, компетентності, знання та уміння, а отже, і зміст освіти. Існує деяке дублювання у змісті навчання цих трьох спеціальностей. По суті, спеціальності існують в частинах тієї самої предметної області, виконуючи різні завдання, які слугуватимуть одній меті – підвищенню конкурентоспроможності ІТ-випускників закладів вищої освіти на ІТ-ринку праці (Ковалюк, 2018). ІТ-професії, для яких розроблено професійні стандарти в Україні, відповідають номенклатурі професійних профілів Європейської рамки компетенцій (e-CF – European e-Competence Framework) (Европейская модель ИТ-компетенций, 2007). Стандарти професійних компетенцій в області ІТ – це засіб формування соціального замовлення ІТ-індустрії та інструмент для моніторингу та аналізу ринку праці, прогнозування його розвитку, планування відтворення кадрів. Згідно з e-CF модель компетенцій для ІТ-спеціалістів містить 5 областей, 36 компетенцій, 5 рівнів, при цьому одною із компетенцій є Information Security Strategy Development (розробка стратегій інформаційної безпеки), яка визначена для різних областей та рівнів (Европейская модель ИТ-компетенций, 2007). Це підтверджує актуальність запропонованого дослідження з визначення шляхів набуття ІТ-спеціалістами компетенцій з забезпечення безпеки інформації.

Окреслене визначило **мету** нашого дослідження – теоретичне обґрунтування та розробка моделі формування і розвитку компетентностей ІТ-спеціаліста з криптографічного захисту інформації студентів галузі знань «12-Інформаційні технології» у процесі вивчення дисциплін «Прикладна криптологія», «Безпека програм та даних», «Технології безпечного програмування», «Об'єктно-орієнтоване програмування».

МЕТОДИ ДОСЛІДЖЕННЯ

У дослідженні були використані теоретичні методи аналізу та узагальнення наукових праць провідних методистів, що розглядали реалізацію компетентнісного підходу у вищій школі, зокрема компетентності майбутніх ІТ-спеціалістів; порівняльні методи зіставлення різних існуючих криптографічних сервісів захисту інформації у процесі вивчення навчальних дисциплін «Прикладна криптологія», «Безпека програм та даних», «Технології безпечного програмування», «Об'єктно-орієнтоване програмування».

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Задача надання знань з криптографічного захисту інформації майбутньому ІТ- спеціалісту носить системний та міждисциплінарний характер. Необхідно об'єднати зусилля викладачів тих дисциплін, які пов'язані з криптографічним захистом, захистом даних, захистом програмного забезпечення, програмування. Кожна спеціальність галузі «12-

Інформаційні технології» знайомиться з криптографічними методами захисту з різних сторін та в різних обсягах: спеціальність 121 Інженерія програмного забезпечення розглядає як один з об'єктів вивчення теорії, аналізу, розробки, реалізації алгоритмів, зокрема криптографічних; спеціальність 122 Комп'ютерні науки вивчає як один з об'єктів у процесі цифрової обробки сигналів, даних та знань, куди входять і криптографічні перетворення; спеціальність 125 Кібербезпека визначає як один з об'єктів вивчення системи захисту інформації у різних інформаційно-комунікаційних мережах, зокрема системи криптографічного захисту. Проте, загальним у них є необхідність володіти криптографічними перетвореннями як IT-навичкою.

Навчання криптографічним методам захисту у вищих технічних навчальних закладах, які готують спеціалістів галузі знань «12-Інформаційні технології», крім загальних цілей ознайомлення з основними теоретичними положеннями математичних методів перетворення інформації та відповідною термінологією має підпорядковуватись наступним цілям: сформувати теоретичні поняття та практичні навички щодо проведення побудови та аналізу класичних шифрів, блочних шифрів, асиметричних криптосистем та організацію криптографічних протоколів.

Серед фахових компетентностей IT-спеціалістів в області захисту інформації криптографічними методами відзначимо наступні:

– використання стандартних криптографічних систем, криптографічних примітивів та протоколів захисту ресурсів в комп'ютерних системах та мережах;

– здібність до обґрунтування та висування пропозицій щодо застосування конкретних стандартних криптографічних систем, криптографічних примітивів та протоколів захисту ресурсів в комп'ютерних системах та мережах;

– здібність до оцінювання якості криптографічного захисту в інформаційно-комунікаційних системах.

Формування компетентностей з криптографічного захисту буде більш ефективним, якщо отримані теоретичні знання з криптографічних методів захисту інформації будуть підкріплені практичними навичками створення і використання криптографічних алгоритмів.

Практичне застосування криптографічних методів захисту інформації, вважаємо, необхідно вводити в курси з програмування. Для закріплення знань студенти можуть реалізувати прості алгоритми зашифрування/розшифрування, але тільки використання сучасних криптографічних сервісів, бібліотек класів дозволить набути актуальні практичні навички з захисту інформації.

Майбутні спеціалісти повинні набути практичні навички у створенні прикладних програм для реалізації наступних класів алгоритмів:

– симетричні алгоритми (DES, AES/Rijndael, та інші)

– потокові шифри (A5 та інші)

– хеш-функції (сімейство функцій MD5, сімейство функцій SHA та інші);

– алгоритми з відкритим ключем (Diffie-Hellman, El-Gamal, RSA, ECDiffie-Hellman та інші);

– генератори псевдовипадкових послідовностей чисел та інші.

Для вирішення цього завдання доцільно використовувати криптографічні служби, які є програмним засобом, що призначений для вбудовування в інше програмне забезпечення, або вбудовані в обрану мову програмування і такі, що дозволяють виконувати наступні криптоперетворення:

– зашифрування/розшифрування симетричними алгоритмами;

– зашифрування/розшифрування асиметричними алгоритмами;

– побудова і перевірка цифрового підпису;

– хешування та інші.

У результаті такої діяльності у студентів формуються навички працювати з криптографічними службами, використовувати об'єктно-орієнтовані бібліотеки реалізації вказаних алгоритмів.

Криптографічні служби .Net Framework. Еволюція сучасних засобів захисту сприяє появі нових криптографічних сервісів. До відомих криптографічних служб можна віднести такі, як Crypto API (CAPI), Cryptography API: Next Generation (CNG), uaCrypto, Crypto++, CryptLib, Botan, Net Framework (System.Security.Cryptography). Кожна з цих служб має свої переваги, недоліки та сфери застосування. Більшість статей присвячено опису функціональних можливостей служб, їх застосуванню для вирішення конкретних задач, порівнянню ефективності реалізацій криптографічних алгоритмів (Горбенко & Аулов, 2012; *Бібліотека функцій криптографічних перетворень "uaCrypto, версія ICAO"*.; Ковтун, 2010; Яковина, Федасюк, Сенів & Білас, 2007). Визначення головних критеріїв вибору криптографічної служби та сучасного середовища розробки для зручного використання відповідного сервісу є ключовим для закладів вищої освіти, які готують IT-спеціалістів.

Криптографічні сервіси розглядались за такими критеріями:

– підтримка базових криптографічних функцій (генератор випадкових чисел, шифрування/розшифрування, цифровий підпис, хешування, генерація ключів, обмін ключами);

– підтримка функцій для роботи з сертифікатами X 509;

– можливість розширення за рахунок власних алгоритмів та розроблених незалежними постачальниками;

– контроль за виконанням криптографічних операцій та спільною роботою алгоритмів;

– підтримка апаратних засобів, таких як смарт-карти для різних постачальників;

– організація ефективної роботи сховища ключів для збереження та управління ключами;

– реалізація стандартного інтерфейсу криптопровайдера служби;

– наявність комплексу засобів розробки для спрощення процесу інтеграції криптографічних служб в програмне забезпечення, що розробляється.

Важливим є також питання вибору інтегрованого середовища розробки для ефективного використання обраного криптографічного сервісу. Криптографічна служба Net Framework (бібліотека класів System.Security.Cryptography) відповідає зазначеним вимогам і може використовуватися разом з Integrated Development Environment MS Visual Studio.

Як середовище розробки прикладних програм обрано сімейство інструментів *Microsoft Visual Studio*, яке містить інтегроване середовище розробки, сервіс для організації спільної роботи, комплексне рішення для розробки мобільних додатків - Visual Studio Mobile Center, багатоплатформовий редактор коду Visual Studio Code, що робить його одним із лідерів розробки різноманітного програмного забезпечення (Бурячок, Спасітєлєва & Складанний, 2018). IDE Visual Studio 2017 можна використовувати для розробки прикладних програм для Android, iOS, Windows, Linux, веб-додатків, мобільних та хмарних додатків, систем баз даних. При цьому середовище розробки містить набір додаткових інструментів, які дозволять розробникам прикладних програм створювати надійний та захищений код. До таких інструментів можна віднести засоби статичного аналізу для виявлення і усунення потенційно уразливих конструкцій у вихідному коді програми. Аналіз коду працює в додатках .NET Framework і додатках баз даних. Такі можливості як навігація по коду, рефакторинг, real-time функцій модульного тестування і перевірки залежностей, виправлення і налагодження значно покращують якість, безпечність коду та продуктивність розробки. В середовищі розробки можна виконувати профілювання програми, статичний аналіз коду рішення або обраного проекту, змінювати установки аналізу коду для всього рішення або проекту, робити розрахунок набору метрик (цикломатичний номер графа управління програмами, кількість операторів та описів у програмі, ступінь злиття класів та методів класу для рішення) (Using Code Analysis with Visual Studio 2017 to Improve Code Quality, 2017). Робота в такому середовище дає можливість студентам розробляти безпечні додатки, використовуючи засоби для оцінки якості коду та його надійності. Програми, написані будь-якою мовою, що підтримують платформу .NET, можуть користуватися класами і методами стандартної бібліотеки класів платформи .NET Framework.

Розглянемо можливості бібліотеки, які пов'язані з безпекою програм та захистом даних і визначені в просторі імен System.Security (Модель криптографии .NET Framework, 2017). Бібліотека підтримує функціональність внутрішньої системи безпеки Common Language Runtime. Цей простір дає можливість розробляти модулі безпеки для додатків, що базуються на політиках і дозволах, забезпечує доступ до засобів криптографії.

Класи простору імен System.Security.Cryptography реалізують різні аспекти криптографії. Частина класів використовується як оболонка для некерованого коду CryptoAPI, інша частина - реалізована у вигляді керованого коду .NET Framework, також є класи для підтримки криптографії наступного покоління CNG, яка є заміною CryptoAPI. Простір імен System.Security.Cryptography надає криптографічні служби, які реалізовані у вигляді ієрархії класів і підтримує основні симетричні та асиметричні шифри, хеш-алгоритми та генератор випадкових чисел криптографічної якості (Торстейнсон & Ганеш, 2013). Ця криптографічна основа може бути розширена, тобто можна додати власну програмну реалізацію алгоритму шляхом створення відповідного похідного класу або можна підключити модулі сторонніх розробників. Класи простору імен System.Security.Cryptography.XML реалізують стандарт W3C для цифрового підпису XML–об'єктів, а класи простору імен System.Security.Cryptography.X509Certificates забезпечують підтримку операцій з публічними сертифікатами.

Ієрархія класів .NET надає можливість абстрагуватися від конкретної реалізації алгоритму. Класи алгоритмів реалізуються на основі шаблону, який включає два рівня успадкування: абстрактний базовий клас - абстрактний клас алгоритму. Класи першого та другого рівня є абстрактними і містять необхідні властивості та методи для роботи визначених алгоритмів. Тільки класи третього рівня містять методи реалізації відповідних алгоритмів. Частина класів реалізації алгоритму базується на криптопровайдерах CryptoAP; класи, які реалізовані як керований код, мають в назві підрядок «Managed»; класи, які реалізують криптографію CNG, мають у назві підрядок Cng. Класи криптографії наступного покоління (CNG) надають керовану оболонку для власних функцій CNG. На рисунку 1 представлена ієрархія класів шифрування. Рисунок 2 відображає ієрархію класів хеш-алгоритмів.

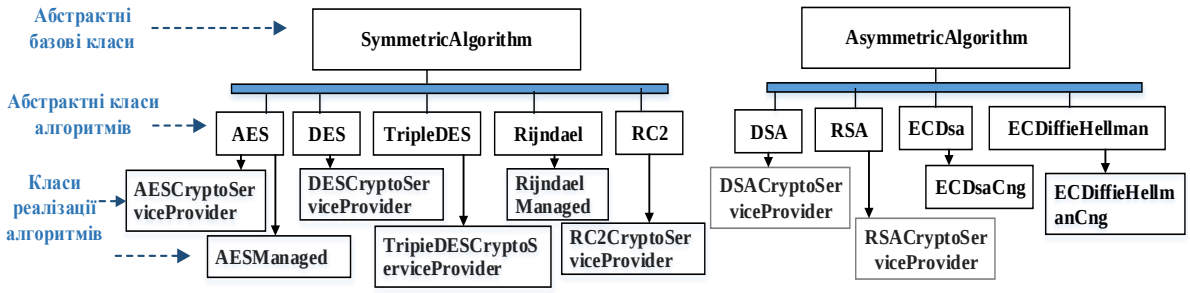

Рис. 1. Ієрархія класів алгоритмів шифрування

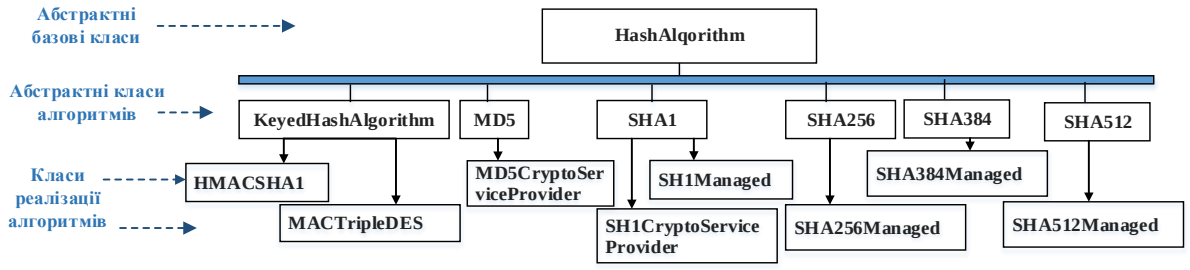

Рис. 2. Ієрархія класів хеш-алгоритмів

Створення ключів та управління ними - це важлива частина процесу шифрування. Класи реалізації алгоритмів відрізняються способом організації бази ключів. База ключів є набором захищених контейнерів ключів. Контейнером ключів називають частину бази даних ключів, яка містить пару ключів для обміну ключами і формування цифрового підпису. Як контейнери ключів (сховищ пар ключів) використовують, наприклад, область тимчасової пам'яті, ділянку реєстру, файл на диску, смарт-карти (Практическое руководство. Хранение асимметричных ключей в контейнере ключей, 2017.). Контейнери дають можливість додаткам зберігати і використовувати ключі, забезпечуючи захист самих ключів від компрометації та модифікування. Контейнери ключів в системі можуть бути двох типів: призначені для користувача і рівня системи. Призначені для користувача контейнери існують в контексті роботи поточного користувача. Контейнери ключів не існують самі по собі, а існують лише в контексті класу реалізації алгоритму. Для кожного класу реалізації існує свій власний набір контейнерів ключів. Це пояснюється тим, що різні класи можуть по-різному реалізовувати навіть один і той же математичний алгоритм. Симетричні алгоритми вимагають створення ключа і вектору ініціалізації (IV) для кожного сеансу роботи. При передачі симетричного ключа і вектору ініціалізації віддаленій стороні симетричний ключ зазвичай шифрується за допомогою асиметричного шифрування. Асиметричні ключі можна зберігати для використання в декількох сеансах або створювати тільки для окремого сеансу. Для збереження закритого ключа слід використовувати контейнер ключа. Центральним в групі класів оболонок CNG є клас провайдера сховища ключів CngProvider та контейнера ключів CngKey, який абстрагує зберігання і використання ключів CNG. Клас CngProvider надає можливість обрати постачальника сховища ключів на базі смарт-карт або програмного постачальника Microsoft. Клас CngKey дає змогу створювати, безпечно зберігати пару ключів або відкритий ключ, відкривати, видаляти, експортувати ключі і посилатися на ключі, використовуючи просте строкове ім'я. Клас цифрових підписів ECDsaCng і клас шифрування ECDiffieHellmanCng використовують об'єкти CngKey.

Алгоритм можна вибирати в залежності від поставленої задачі, наприклад для забезпечення цілісності даних, для забезпечення конфіденційності даних або для створення ключа. Симетричні і хеш-алгоритми призначені для захисту даних від порушення цілісності (захист від зміни) або конфіденційності (захист від перегляду). Хеш-алгоритми використовуються в основному для забезпечення цілісності даних.

Можна визначити перелік рекомендованих алгоритмів для програми створення системи автентифікації, захищеної електронної пошти тощо. Для забезпечення конфіденційності даних можна використати алгоритм шифрування AES; для забезпечення цілісності даних можна використати HMACSHA256 або HMACSHA512 для реалізації хеш-коду перевірки справжності повідомлень; цифровий підпис можна реалізувати за допомогою алгоритму ECDsa на базі еліптичних кривих або алгоритму RSA; для обміну ключами можна використати алгоритм Діффі-Хеллмана на еліптичних кривих – ECDiffieHellman або алгоритм RSA; для генерації випадкових чисел можна використати клас RNGCryptoServiceProvider; для формування ключа на базі паролю можна використати клас Rfc2898DeriveBytes.

При використанні цих класів не обов'язково бути експертом з криптографії. Студенти можуть застосовувати криптографічні методи бібліотеки у своїх проектах, при цьому не витрачаючи час на програмну реалізацію складних алгоритмів шифрування. Наприклад, при створенні екземпляра класу, який реалізує алгоритми шифрування, ключі можуть створюватися автоматично, а прийняті за замовчуванням значення властивостей забезпечують максимальну захищеність. На рисунку 3 представлено приклад одної із студентських програм реалізації алгоритмів AES та TripleDES бібліотеки класів Security.Cryptography для зашифрування/розшифрування текстових файлів, яка може використовуватися для демонстрації роботи алгоритмів шифрування.

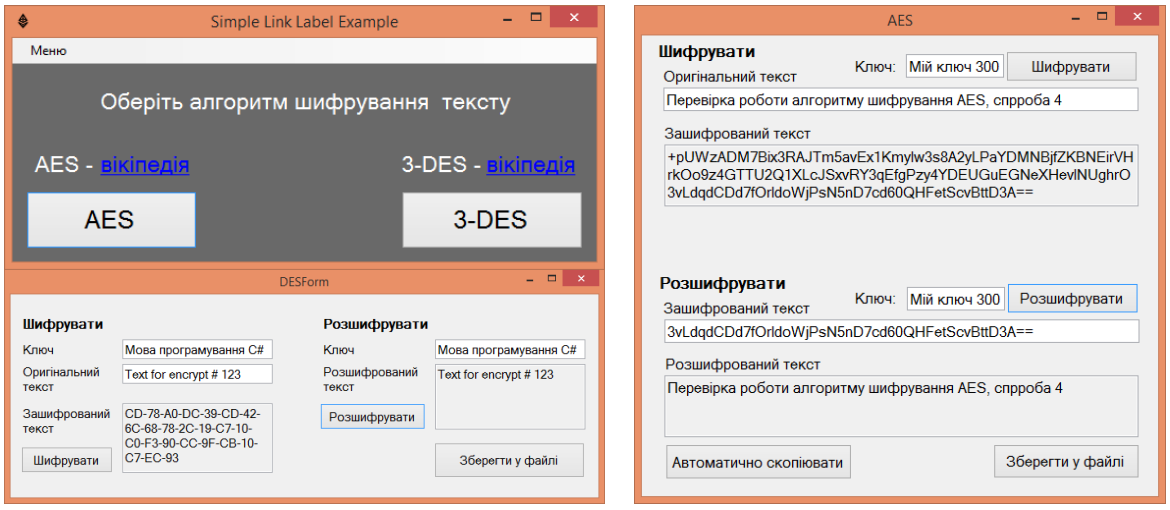

Рис. 3. Програма реалізації алгоритмів Aes та TripleDES

У програмі використовуються класи AESManaged, TripleDESCryptoServiceProvider, які описують властивості для маніпулювання основними параметрами алгоритмів: розміром блоку, режимом роботи, вектором ініціалізації, ключем тощо. Підсистема шифрування використовує методи класів CreateEncryptor() та CreateDecryptor() для виконання шифрування/розшифрування тексту, методи GenerateKey() та GenerateIV() використовуються для генерації ключів та векторів ініціалізації. Об’єктно-орієнтована підсистема візуалізації демонструє процес шифрування, надає інформацію про суть використовуваних алгоритмів та принципів блокових перетворень, що дозволяє використовувати додаток для навчання.

ОБГОВОРЕННЯ

Таким чином, запропонована міждисциплінарна організація вивчення основ криптографічного захисту інформації, як свідчить первинний аналіз результатів навчання, дозволяє надати студентам необхідний обсяг знань з комп'ютерної безпеки та захисту інформації, активізувати науково-дослідницьку роботу студентів у напрямку захисту інформації та створення безпечного програмного забезпечення. Наявність практики з використання сучасних криптографічних бібліотек, таких як CNG, .NET Cryptography, дозволить набути практичні навички з криптографічного захисту інформації.

Крім того, майбутні ІТ-спеціалісти мають усвідомити, що розробка програмного забезпечення – це не тільки інженерно-технічна діяльність. До неї входять також економічні, правові аспекти, аспекти захисту інформації, причому останні в складних та дорогих проектах відіграють вирішальну роль.

Уміння та навички за допомогою програмування вирішувати певні задачі захисту інформації дає студентам впевненість в тому, що вони будуть затребуваними на ринку праці та зможуть розв'язувати подібні задачі у професійній діяльності.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШОГО ДОСЛІДЖЕННЯ

Розроблена модель формування та розвитку компетентностей з криптографічного захисту інформації студентів галузі знань «12-Інформаційні технології» впроваджується у Київському університеті імені Бориса Грінченка та Державному університеті телекомунікацій. Саме на базі програмування криптографічних механізмів захисту інформації ефективно формуються практичні навички застосування криптографічних алгоритмів у процесі опрацювання та передачі даних. Конкретизоване визначення обсягу теоретичних знань та практичних умінь з врахуванням міждисциплінарних зв'язків навчальних дисциплін, пов'язаних з захистом інформації та програмуванням, дозволяє підготувати фахівців з практичними навичками з криптографічного захисту інформації, які є затребуваними на ринку праці. Перспективою подальших наших досліджень є дослідно-експериментальна робота з впровадження у навчальний процес ЗВО та вдосконалення даної моделі формування і розвитку компетентностей ІТ-спеціаліста з криптографічного захисту інформації студентів галузі знань «12-Інформаційні технології».

Список використаних джерел

1. Бібліотека функцій криптографічних перетворень "uaCrypto, версія ICAO". URL: http://it-engineering.com.ua/kataloh/59-uacrypto-v-icao (Дата звернення: 21.01.2019).
2. Бурячок В.Л., Богуш В.М., Борсуковський Ю.В., Складанний П.М., Борсуковська В.Ю. Модель підготовки фахівців у сфері інформаційної та кібернетичної безпеки в закладах вищої освіти України. *Інформаційні технології і засоби навчання,* 2018, Том 67, №5. С. 277-289.
3. Бурячок В.Л., Спасітєлєва С.О., Складанний П.М. Організація розробки безпечних .Net прикладних програм у закладах вищої освіти. *Сучасна спеціальна техніка*. 2018. № 1(52). С. 13-22.
4. Глобальное исследование утечек конфиденциальной информации в первом полугодии 2018 года. URL: https://www.infowatch.ru/report2018_half (Дата звернення: 10.01.2019).
5. Горбенко Ю.И., Аулов И.Ф. Сравнительный анализ криптографических библиотек с открытым кодом и рекомендации по их использованию. *Прикладная радиоэлектроника*. 2012. Том 11. № 2 С. 220–224.
6. Европейская модель ИТ-компетенций. Published on Nov 2, 2012 URL: https://www.slideshare.net/Cleverics/webinar-ecf (Дата звернення: 11.01.2019).
7. Ковалюк Т.В. Узгодження вимог професійних та освітніх ІТ-стандартів до компетентностей випускників ІТ-спеціальностей ВНЗ. URL: http://science.lpnu.ua/sites/default/files/journal-paper/2018/jun/13020/ilovepdfcom-229-240.pdf (Дата звернення: 14.01.2019).
8. Ковтун Я.В. Анализ возможностей интеграции национальных стандартов криптографии в ОС WINDOWS. *Системи обробки інформації*. 2010, випуск 6 (87). С. 42- 45.
9. 9.Модель криптографии .NET Framework, 2017. URL: https://docs.microsoft.com/ru-ru/dotnet/standard/security/cryptography-model (Дата звернення: 14.01.2019)
10. Панфілов Ю., Фурманець Б. Компетентнісний підхід в освіті: досвід, проблеми, перспективи. *Теорія і практика управління соціальними системами.* 2017. № 3. С. 55-67.
11. Практическое руководство. Хранение асимметричных ключей в контейнере ключей, 2017. URL:https://docs.microsoft.com/ru-ru/dotnet/standard/security/how-to-store-asymmetric-keys-in-a-key-container ((Дата звернення: 14.01.2019)
12. Торстейнсон П., Ганеш Г. Криптография и безопасность в технологии .NET. М.: БИНОМ. Лаборатория знаний, 2013. 480 с.
13. Яковина В., Федасюк Д., Сенів М., Білас О. Порівняння швидкодії програмної реалізації алгоритмів симетричного (DES) та асиметричного (RSA) шифрування. 2007. Lviv Polytechnic National University Institutional Repository. URL: http://ena.lp.edu.ua/bitstream/ntb/38502/1/28_181-185.pdf (Дата звернення: 14.01.2019)
14. Using Code Analysis with Visual Studio 2017 to Improve Code Quality, 2017. URL: https://www.azuredevopslabs.com/labs/tfs/codeanalysis/ (Дата звернення: 14.01.2019)

References

1. Biblioteka funktsiy kryptohrafichnykh peretvoren' "uaCrypto, versiya ICAO". [The cryptographic transformation library "uaCrypto, ICAO version"] URL: http://it-engineering.com.ua/kataloh/59-uacrypto-v-icao [in Ukrainian].
2. Buryachok V.L., Bohush V.M., Borsukovs'kyy YU.V., Skladannyy P.M. & Borsukovs'ka V.YU. (2018) Model' pidhotovky fakhivtsiv u sferi informatsiynoyi ta kibernetychnoyi bezpeky v zakladakh vyshchoyi osvity Ukrayiny. [Model of training specialists in the field of information and cybernetic security in higher education institutions of Ukraine] *Information technology and teaching aids*. 67(5), .277-289. [in Ukrainian].

3. Buryachok V.L., Spasityelyeva S.O. & Skladannyy P.M. (2018) Orhanizatsiya rozrobky bezpechnykh .Net prykladnykh prohram u zakladakh vyshchoyi osvity. [Organization of the development of safe .Net applications in higher education institutions] *Modern special technique*, 1(52), 13-22. [in Ukrainian].
4. Global'noye issledovaniye utechek konfidentsial'noy informatsii v pervom polugodii 2018 goda. (2018) [Global study of confidential information leaks in the first half of 2018] URL: https://www.infowatch.ru/report2018_half [in Russian].
5. Gorbenko Yu.I. & Aulov I.F. (2012) Sravnitel'nyy analiz kriptograficheskikh bibliotek s otkrytym kodom i rekomendatsii po ikh ispol'zovaniyu. [Comparative analysis of open source cryptographic libraries and recommendations for their use] *Applied Radio Electronics*, 11(2), 220–224. [in Russian].
6. Yevropeyskaya model' IT-kompetentsiy. (2012) [European model of IT competencies] URL: https://www.slideshare.net/Cleverics/webinar-ecf [in Russian].
7. Kovalyuk T.V. (2018) Uzhodzhennya vymoh profesiynykh ta osvitnikh IT-standartiv do kompetentnostey vypusknykiv IT-spetsial'nostey VNZ. [Harmonization of requirements of professional and educational IT standards to competencies of graduates of IT specialties of higher educational institutions.] URL: http://science.lpnu.ua/sites/default/files/journal-paper/2018. [in Ukrainian].
8. Kovtun Ya.V. (2010) Analyz vozmozhnostey yntehratsyy natsyonal'nykh standartov kryptohrafyy v OS WINDOWS. [Analysis of the possibilities of integrating national cryptography standards in the WINDOWS OS] *Information processing systems*, 6 (87), 42- 45. [in Russian].
9. Model' kriptografii .NET Framework. [The .NET Framework Cryptography Model] URL: https://docs.microsoft.com/en-us/dotnet/standard/security/cryptography-model
10. Panfilov Yu. & Furmanets' B. (2017) Kompetentnisnyy pidkhid v osviti: dosvid, problemy, perspektyvy. [Competency approach in education: experience, problems, perspectives] *The theory and practice of social systems management*. 3(S), 55-67. [in Ukrainian].
11. Prakticheskoye rukovodstvo. Khraneniye asimmetrichnykh klyuchey v konteynere klyuchey, 2017 [A practical guide. Store asymmetric keys in a key container] URL: https://docs.microsoft.com/ru-ru/dotnet/standard/security/how-to-store-asymmetric-keys-in-a-key-container[in Russian].
12. Torsteynson P. & Ganesh G. (2013)Kriptografiya i bezopasnost' v tekhnologii .NET. [Cryptography and security in .NET technology] M.: BINOM. Laboratoriya znaniy, 480 p. [in Russian].
13. Yakovyna V., Fedasyuk D., Seniv M. & Bilas O. (2007) Porivnyannya shvydkodiyi prohramnoyi realizatsiyi alhorytmiv symetrychnoho (DES) ta asymetrychnoho (RSA) shyfruvannya. [Comparison of software implementation speed of symmetric (DES) and asymmetric (RSA) encryption algorithms] *Lviv Polytechnic National University Institutional Repository*. URL: http://ena.lp.edu.ua/bitstream/ntb/38502/1/28_181-185.pdf [in Ukrainian].
14. Using Code Analysis with Visual Studio 2017 to Improve Code Quality. URL: https://www.azuredevopslabs.com/labs/tfs/codeanalysis/

FORMATION OF INFORMATION PROTECTION COMPETENCE TO STUDENTS OF IT-SPECIALTIES WITH USING .NET FRAMEWORK CRYPTOGRAPHIC SERVICES

Yu. Zhdanova, S. Spasiteleva, S. Shevchenko
Borys Grinchenko Kyiv University, Ukraine

Abstract.

Formulation of the problem. *The article deals with the problem of training modern specialists in the field of knowledge "12-Information Technologies". Issues of providing students with specialized and professional knowledge and skills in cryptographic protection of the information are considered.*

Materials and methods. *Ttheoretical methods of analysis and synthesis of the scientific works of scientists who considered the implementation of a competence approach in higher education, in particular the competences of future IT specialists. Comparative methods were used to compare different existing cryptographic protection services in the process of studying academic disciplines "Applied Cryptology", "Security of applications and data", "Secure Programming", "Object-Oriented Programming".*

Results. *The necessity of obtaining information protection competences for future IT specialists has been substantiated. Through the analysis of literature and the use of own experience, the essence and structure of the concept of "competence of the IT specialist in cryptographic protection of the information" have been determined. Formation of these competencies have been carried out within the framework of interdisciplinary links of educational disciplines, namely: "Applied Cryptology", "Security of applications and data", "Secure Programming", "Object-Oriented Programming". The list of requirements for professionally significant characteristics of the IT specialist in the field of cryptographic protection of information has been determined. An overview of cryptographic libraries has been conducted and the main criteria for selecting the cryptographic service and the programming environment have been determined. The model of formation and development of competences in cryptographic protection of the information for students of the field of knowledge "12-Information Technologies" has been developed and the ways of its realization at Borys Grinchenko Kyiv University and the State University of Telecommunications have been offered.*

Conclusions. *In the course of the research it was determined that in the programming of cryptographic protection mechanisms, practical skills of using cryptographic algorithms in the processing and transmission of data have been effectively formed. It is proved that the definition of the volume of theoretical knowledge and practical skills, taking into account the interdisciplinary connections of educational disciplines, allows preparing specialists with practical skills in cryptographic protection of the information. Such specialists are necessary for IT companies in the labor market.*

Keywords: *competence of IT specialists, information protection, cryptographic protection, cryptographic library, cryptographic algorithms.*