КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (4), 2019
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2019.4.4453
УДК 378.147:004.056.5

Жданова Юлія Дмитрівна
канд. ф.-м. наук, доцент, доцент кафедри комп'ютерних наук та математики
місце роботи: Київський університет імені Бориса Грінченка, м. Київ, Україна
OrcID: 0000-0002-9277-4972
y.zhdanova@kubg.edu.ua

Спасітєлєва Світлана Олексіївна
канд. ф.-м. наук, доцент, доцент кафедри комп'ютерних наук та математики
місце роботи: Київський університет імені Бориса Грінченка, м. Київ, Україна
OrcID: 0000-0003-4993-6355
s.spasitielieva@kubg.edu.ua,

Шевченко Світлана Миколаївна
канд. пед. наук, доцент, доцент кафедри комп'ютерних наук та математики
місце роботи: Київський університет імені Бориса Грінченка, м. Київ, Україна
OrcID: 0000-0002-9736-8623
s.shevchenko@kubg.edu.ua

ЗАСТОСУВАННЯ БІБЛІОТЕКИ КЛАСІВ SECURITY.CRYPTOGRAPHY ДЛЯ ПРАКТИЧНОЇ ПІДГОТОВКИ СПЕЦІАЛІСТІВ З КІБЕРБЕЗПЕКИ

Анотація. Стаття присвячена проблемі підготовки сучасних фахівців спеціальності «125 - Кібербезпека», а саме формування у них в процесі навчання спеціалізовано-професійних знань та умінь з криптографічного захисту інформації.
Доведена необхідність отримання практичних знань з захисту інформації з визначеним обсягом теоретичних знань для майбутніх фахівців спеціальності «125-Кібербезпека». Шляхом аналізу літератури та використання власного досвіду деталізовані суть та структура поняття «компетентності з криптографічного захисту інформації». Зроблено акцент на те, що формування даних компетентностей здійснюється у рамках міждисциплінарних зв'язків навчальних дисциплін, а саме: «Прикладна криптологія», «Технології безпечного програмування». Визначено список вимог до рівня сформованості професійно-значимих характеристик спеціаліста з кібербезпеки в сфері криптографічного захисту інформації. Зроблено огляд криптографічних бібліотек та визначені 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 даних. Розроблена модель формування та розвитку компетентностей з криптографічного захисту інформації студентів спеціальності «125-Кібербезпека» та представлено шляхи її реалізації у Київському університеті імені Бориса Грінченка.
Саме на базі програмування криптографічних механізмів захисту інформації ефективно формуються практичні навички застосування криптографічних алгоритмів при обробці та передачі даних. Чітке визначення обсягу теоретичних знань та практичних умінь з врахуванням міждисциплінарних зв'язків навчальних дисциплін, пов'язаних з захистом даних та програмуванням, дозволяє підготувати фахівців з практичними навичками з криптографічного захисту інформації, які є затребуваними на ринку праці.

Ключові слова: захист даних; криптографічний захист; криптографічна бібліотека; криптографічні алгоритми.

ISSN 2663 - 4023

1. ВСТУП

Постановка проблеми. Головною задачею закладів вищої освіти, які готують фахівців спеціальності «125-Кібербезпека», є підготовка випускників до професійної діяльності в сучасному високорозвиненому інформаційно-комунікаційному середовищі. Тотальна інформатизація суспільства вимагає від освіти вирішення проблеми підготовки таких спеціалістів, які в умовах мінливих реалій сьогодення мають бути здатними не тільки сприймати і поновлювати інформацію, а й оброблювати її, зберігати та створювати нову. Особливе місце посідає підготовка спеціаліста з кібербезпеки до виконання важливої задачі захисту даних, 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 [1]. Більшість загроз цілісності і конфіденційності інформації, що циркулює в комп'ютерних системах, можна попередити використанням механізмів безпеки, що реалізуються за допомогою криптографічних методів захисту. Тому підготовка сучасного спеціаліста має обов'язково включати знання з криптографічного захисту інформації в обсязі, передбаченому спеціальністю [2]. Все це підтверджує актуальність визначеної проблеми і спонукає до пошуків шляхів формування у майбутніх фахівців практичних знань в області криптографічного захисту інформації.

Аналіз основних досліджень і публікацій. До питання формування та розвитку професійної компетентності майбутніх фахівців у процесі навчання у закладах вищої освіти звертаються багато вчених. Різні аспекти цієї проблеми були висвітлені у наукових дослідженнях В. Баркасі, І. Бондаренко, С. Вітвицької, О. Вознюк, Л. Голованчук, О. Дубасенюк, І. Зимньої, Д. Іванова, Л. Карпової, С. Козак, А. Маркової, Г. Мельниченко, О. Окуловського, О. Палій, Ю. Панфілова, Л. Петровської, О. Пометун, Л. Пуховської, С. Савельєвої, Н. Саєнко, С. Сисоєвої, Н. Тализіної, Б. Фурманцева та багатьох інших. Вони одностайні в тому, 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. На їх думку, такий підхід акцентував увагу на результаті навчання, причому як результат ними розглядається не сума засвоєної інформації, а здатність людини на її основі адекватно діяти в різних ситуаціях [3].

Аналіз ситуації з реалізацією компетентнісного підходу у вищій школі, зроблений Ю. Панфіловим та Б.Фурманцем [3], дозволив встановити низку проблем щодо здійснення цього процесу. Серед них – відсутність практичної професійної підготовки. У студентів відсутній досвід застосування теоретичних знань на практиці, володіння нюансами й особливостями їх реалізації в конкретних умовах, що не дозволяє ефективно формувати необхідні компетентності. Компетентнісний підхід цінує не знання, а здатність їх використання. 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 освітньої діяльності [4].

Практична реалізація такого підходу у Київському університеті імені Бориса Грінченка на кафедрі інформаційної та кібернетичної безпеки почалася з розробки Освітньої програми. «З метою підготовки до роботи в реальному середовищі майбутньої професійної діяльності та отримання випускниками освітньої кваліфікації бакалавр з кібербезпеки освітня програма передбачає надання студентам: …сучасних компетентностей та практичних навичок з програмування, розробки та управління базами даних, формування моделей захисту інформації та політик безпеки, технічного і криптографічного захисту інформації, побудови захищених IP і TCP мереж та обслуговування сертифікатів відкритих ключів, побудови комплексних систем захисту інформації на об'єктах інформаційної діяльності…» [5].

Вважаємо, що дисципліни «Прикладна криптологія», «Технології безпечного програмування» мають потужний потенціал для формування практичних навичок у сфері кіберзахисту та програмування, що при відповідній методичній організації навчання стане підґрунтям для розвитку професійних компетенцій [2].

Мета статті. Метою нашого дослідження є розробка методики формування практичних навичок з криптографічного захисту інформації студентів спеціальності «125-Кібербезпека» у процесі вивчення дисциплін «Прикладна криптологія», «Технології безпечного програмування».

2. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Задача надання знань з криптографічного захисту інформації майбутньому спеціалісту з кібербезпеки носить системний та міждисциплінарний характер. Необхідно об'єднати зусилля викладачів, які викладають дисципліни, пов'язані з криптографічним захистом, програмуванням. Так, криптографія знайомить з теоретичними основами математичних перетворень даних та практичними напрямами їх застосування і розглядається як засіб розв'язання конкретних класів задач з захисту даних. Аналіз і дослідження криптографічних механізмів захисту інформації на базі програмування дає можливість практичного застосування криптографічних алгоритмів при обробці та передачі даних.

Криптографічні методи захисту інформації. Як визначалося вище, одною з компетентностей майбутніх спеціалістів з кібербезпеки є розробка стратегій інформаційної безпеки, зокрема забезпечення криптографічного захисту інформації. Спеціальність 125 Кібербезпека розуміє як один з об'єктів вивчення системи захисту інформації в різних інформаційно-комунікаційних мережах, зокрема системи криптографічного захисту, тому для майбутніх спеціалістів існує необхідність володіти криптографічними перетвореннями як IT-навичкою.

Навчання криптографічним методам захисту у вищих технічних навчальних закладах, які готують спеціалістів з кібербезпеки, 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 спеціалістів, що формуються після опанування криптографічними методами захисту, відзначимо наступні:

- використання стандартних криптографічних систем, криптографічних примітивів

ISSN 2663 - 4023

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.

Одною з задач дисциплін, що вивчають криптографічні методи захисту інформації, є сприяння формуванню спеціалізовано-професійних компетентностей, які пов'язані з оволодінням методиками використання засобів програмування для розв'язування практичних задач.

Практичне застосування криптографічних методів захисту при обробці даних обов'язково 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 придбати практичні навички в 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 набуття цих навичок 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.

Студенти мають вміти 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 [6]–[7]. Визначення головних критеріїв вибору криптографічної служби та сучасного середовища розробки для зручного використання відповідного сервісу є ключовим для закладів вищої освіти, які готують спеціалістів з кібербезпеки.

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 викладеним 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 [8]. 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. 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 [9]. 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 [10]. Бібліотека підтримує функціональність внутрішньої системи безпеки Common Language Runtime. Цей простір дозволяє 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 [11]. 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 дозволяє абстрагуватися від конкретної реалізації алгоритму. Класи алгоритмів реалізується на основі шаблону, що 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.

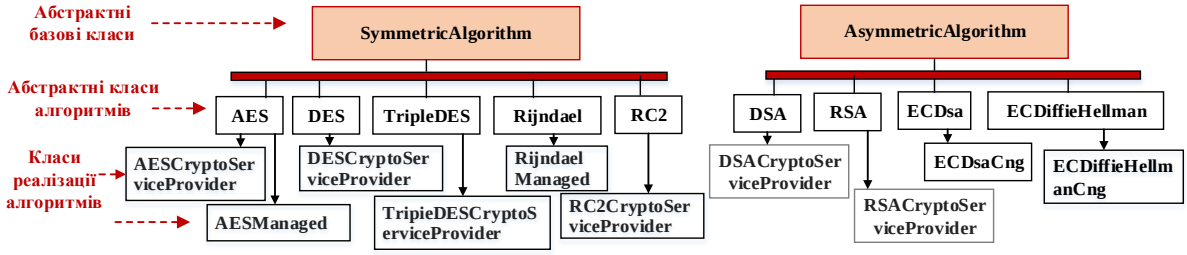

Рис. 1. Ієрархія класів алгоритмів шифрування

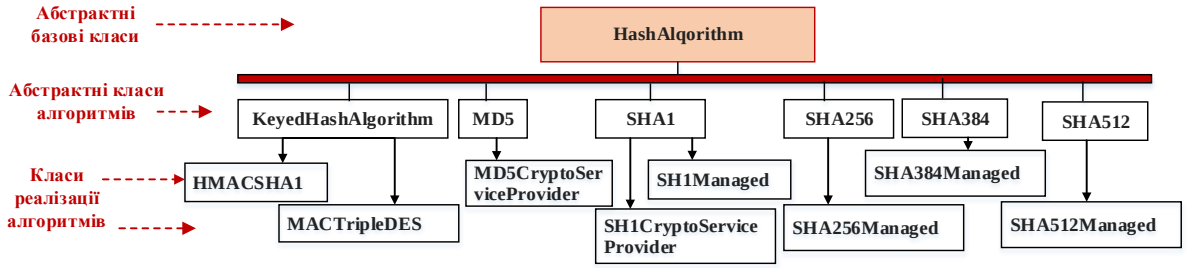

Рис. 2. Ієрархія класів хеш-алгоритмів

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. Для кожного класу реалізації існує свій власний набір контейнерів ключів. [12]

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 список рекомендованих алгоритмів для програми створення системи автентифікації, захищеної електронної пошти тощо. Для забезпечення конфіденційність даних можна використати алгоритм шифрування AES; для забезпечення цілісності даних можна використати HMACSHA256 або HMACSHA512 [13] 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 формуванні 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.

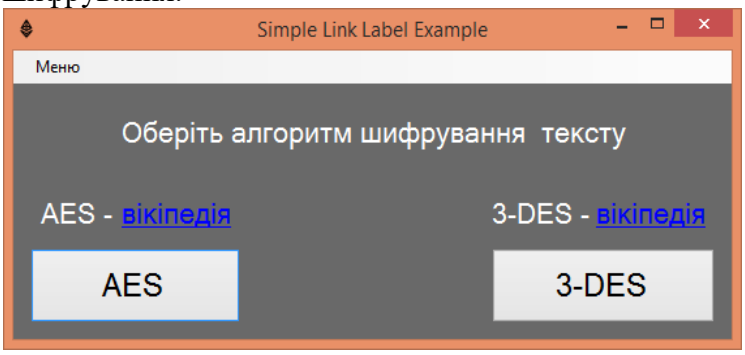

Рис. 3. Програма реалізації алгоритмів Aes та TripleDES

В 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.

3. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Описана модель формування та розвитку компетентностей з криптографічного захисту інформації студентів спеціальності «125-Кібербезпека» впроваджується у Київському університеті імені Бориса Грінченка. Саме на базі програмування криптографічних механізмів захисту інформації ефективно формуються практичні навички застосування криптографічних алгоритмів при обробці та передачі даних. Чітке визначення обсягу теоретичних знань та практичних умінь з врахуванням

міждисциплінарних зв'язків навчальних дисциплін, пов'язаних з захистом даних 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 закладів вищої освіти та вдосконалення даної моделі формування і розвитку компетентностей з криптографічного захисту інформації студентів спеціальності «125-Кібербезпека».

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Глобальное исследование утечек конфиденциальной информации в первом полугодии 2018 года. [Онлайн] Режим доступу: https://www.infowatch.ru/report2018_half [20 січ. 2019]
[2] Ю. Д. Жданова, С. О. Спасітєлєва, С.М. Шевченко, "Формування у студентів ІТ-спеціальностей компетентностей в області захисту інформації з використанням криптографічних служб .NET FRAMEWORK", *Фізико-математична освіта*. Випуск 1(19). С. 48-54, 2019.
[3] Ю. Панфілов, Б. Фурманець, "Компетентнісний підхід в освіті: досвід, проблеми, перспективи", *Теорія і практика управління соціальними системами.* № 3. С. 55-67, 2017.
[4] В.Л. Бурячок, В.М. Богуш, Ю.В. Борсуковський, П.М. Складанний, В.Ю. Борсуковська, "Модель підготовки фахівців у сфері інформаційної та кібернетичної безпеки в закладах вищої освіти України", *Інформаційні технології і засоби навчання,* том 67, №5, с.277-289, 2018.
[5] *Освітньо-професійна програма. 125.00.01. Безпека інформаційних і комунікаційних систем першого (бакалаврського) рівня освіти.* Київський університет імені Б. Грінченка, 2018. [Онлайн] Режим доступу: http://kubg.edu.ua/images/stories/Departaments/vstupnikam/fitu/2018/2019_bak_op_kiber.pdf [13 берез. 2019]
[6] Ю.И. Горбенко, И.Ф. Аулов, "Сравнительный анализ криптографических библиотек с открытым кодом и рекомендации по их использованию", *Прикладная радиоэлектроника*. Том 11, № 2, с. 220–224, 2012.
[7] *IT Engineering - Бібліотека функцій криптографічних перетворень "uaCrypto, версія ICAO".* [Онлайн] Режим доступу: http://it-engineering.com.ua/kataloh/59-uacrypto-v-icao [20 лют. 2019]
[8] В.Л. Бурячок, С.О. Спасітєлєва, П.М. Складанний "Організація розробки безпечних .Net прикладних програм у закладах вищої освіти", *Сучасна спеціальна техніка*. № 1(52), с. 13-22, 2018.
[9] Using Code Analysis with Visual Studio 2017 to Improve Code Quality, 2017. [Онлайн] Режим доступу: https://www.azuredevopslabs.com/labs/tfs/codeanalysis/ [14 січ. 2019]
[10] Модель криптографии .NET Framework, 2017. [Онлайн] Режим доступу: https://docs.microsoft.com/ru-ru/dotnet/standard/security/cryptography-model [4 лют. 2019]
[11] П. Торстейнсон, Г. Ганеш. *Криптография и безопасность в технологии .NET*. М.: БИНОМ. Лаборатория знаний, 2013. 480 с.
[12] Практическое руководство. Хранение асимметричных ключей в контейнере ключей, 2017. [Онлайн] Режим доступу: https://docs.microsoft.com/ru-ru/dotnet/standard/security/how-to-store-asymmetric-keys-in-a-key-container [лют.М.С. Пасєка, Н.М. Пасєка, М.Я. Бестильний, В.І. Шакета, "Аналіз використання високоефективної реалізації функцій хешування SHA-512 для розробки програмних систем", *Кібербезпека: освіта, наука, техніка.* № 3(3). С. 112-119, 2019. https://doi.org/10.28925/2663-4023.2019.3.112121

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (4), 2019
ISSN 2663 - 4023

Yulia D. Zhdanova
PhD, Associate Professor, Associate Professor of the Department of Computer Science and Mathematics
Borys Grinchenko Kyiv University, Kyiv, Ukraine
OrcID: 0000-0002-9277-4972
y.zhdanova@kubg.edu.ua

Svitlana O. Spasiteleva
PhD, Associate Professor, Associate Professor of the Department of Computer Science and Mathematics
Borys Grinchenko Kyiv University, Kyiv, Ukraine
OrcID: 0000-0003-4993-6355
s.spasitielieva@kubg.edu.ua,

Svitlana M. Shevchenko
PhD, Associate Professor, Associate Professor of the Department of Computer Science and Mathematics
Borys Grinchenko Kyiv University, Kyiv, Ukraine
OrcID: 0000-0002-9736-8623
s.shevchenko@kubg.edu.ua

APPLICATION OF THE SECURITY.CRYPTOGRAPHY CLASS LIBRARY FOR PRACTICAL TRAINING OF SPECIALISTS FROM THE CYBER SECURITY

Abstract. The article deals with the problem of training modern specialists of the specialty "125 - Cyber Security". Issues of providing students with specialized and professional knowledge and skills in cryptographic protection of the information are considered.
The necessity of obtaining practical knowledge on information protection with a certain amount of theoretical knowledge for future cybersecurity specialists has been substantiated. Through the analysis of literature and the use of own experience, the essence and structure of the concept of "competence on 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", "Secure Programming". The list of requirements for professionally significant characteristics of a cybersecurity 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 article demonstrates the need to use modern cryptographic .Net Framework services and the Microsoft Visual Studio application development environment to provide students with the knowledge and practical skills of information protection. The model of formation and development of competences on cryptographic protection of the information for students of the specialty “125-Cyber Security” has been developed and the ways of its realization at Borys Grinchenko Kyiv University have been offered.
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: information protection; cryptographic protection, cryptographic library, cryptographic algorithms.

REFERENCES

[1] 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] [Online]. Available: https://www.infowatch.ru/report2018_half. [Jan. 20, 2019]. (in Russian).
[2] Yu.D. Zhdanova, S. Spasiteleva, S. and S.M. Shevchenko. "Formuvannya u studentiv IT-spetsial′nostey

kompetentnostey v oblasti zakhystu informatsiyi z vykorystannyam kryptohrafichnykh sluzhb .NET FRAMEWORK" ["Formation Of Information Protection Competence To Students Of It-Specialties With Using .NET FRAMEWORK Cryptographic Services. "] *Physical and Mathematical Education*, 19(1), pp.48-54, 2019 (in Ukrainian).

[3] Yu. Panfilov, B. Furmanets′, "Kompetentnisnyy pidkhid v osviti: dosvid, problemy, perspektyvy" ["Competency approach in education: experience, problems, perspectives"] *The theory and practice of social systems management*. no.3, pp. 55-67, 2017 (in Ukrainian).

[4] V.L Buryachok, V.M. Bohush, YU.V. Borsukovs′kyy, P.M. Skladannyy and V.YU. Borsukovs′ka, "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 Learning Tools*, 67(5), 277-289, 2018. (in Ukrainian).

[5] *Osvitn'o-profesiyna prohrama. 125.00.01. Bezpeka informatsiynykh i komunikatsiynykh system pershoho (bakalavrs'koho) rivnya osvity.* Kyyivs′kyy universytet imeni B. Hrinchenka, 2018. [Educational and professional program. 125.00.01. Safety of information and communication systems of the first (bachelor) level of education. Kyiv Boris Grinchenko University, 2018] [Online] Available at: http://kubg.edu.ua/images/stories/Departaments/vstupnikam/fitu/2018/2019_bak_op_kiber.pdf [Mar. 15, 2019] (in Ukrainian).

[6] Yu.I. Gorbenko, I.F Aulov. "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 useendation] *Applied Radio Electronics*, 11(2), 220–224, 2012 (in Russian).

[7] *IT Engineering - Biblioteka funktsiy kryptohrafichnykh peretvoren' "uaCrypto, versiya ICAO*". [It-engineering.com.ua. (2019). *IT Engineering - The library of functions of cryptographic transformations "uaCrypto, version ICAO"*. [Online] Available at: http://it-engineering.com.ua/kataloh/59-uacrypto-v-icao. [Fab. 20, 2019]. (in Ukrainian).

[8] V.L. Buryachok, S.O. Spasityelyeva, P.M. Skladannyy "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, 2018 (in Ukrainian).

[9] Using Code Analysis with Visual Studio 2017 to Improve Code Quality, 2017. [Online]. Available: https://www.azuredevopslabs.com/labs/tfs/codeanalysis/. [Jan. 14, 2019].

[10] Model' kriptografii .NET Framework, 2017. [The .NET Framework Cryptography Model] [Online] Available : https://docs.microsoft.com/en-us/dotnet/standard/security/cryptography-model [Feb.4, .2019]. (in Russian).

[11] P. Torsteynson, and G. Ganesh *Kriptografiya i bezopasnost' v tekhnologii .NET.* [*Cryptography and security in .NET technology*] M.: BINOM. Laboratoriya znaniy, 2013 480p. (in Russian).

[12] Prakticheskoye rukovodstvo. Khraneniye asimmetrichnykh klyuchey v konteynere klyuchey, 2017 [A practical guide. Store asymmetric keys in a key container] [Online] Available at: https://docs.microsoft.com/ru-ru/dotnet/standard/security/how-to-store-asymmetric-keys-in-a-key-container. [Feb. (in Russian).

M.S. Pasyeka, N.M. Pasyeka, M.YA. Bestyl′nyy and V.I. Shaketa. "Analiz vykorystannya vysokoefektyvnoyi realizatsiyi funktsiy kheshuvannya SHA-512 dlya rozrobky prohramnykh system", ["Analysis of the use of the highly effective implementation of SHA-512 hash functions for software systems development" *Cybersecurity: education, science, technology*, vol 3, no 3, pp 112-121, 2019. https://doi.org/10.28925/2663-4023.2019.3.112121 (in Ukrainian).