МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

ЗАТВЕРДЖУЮ
Голова приймальної комісії
Харківського національного
економічного університету
імені Семена Кузнеця
_____ Володимир ПОНОМАРЕНКО
«25» березня 2021 р.

ПРОГРАМА
ФАХОВОГО ВСТУПНОГО ВИПРОБУВАННЯ

освітній ступінь «бакалавр»

(на основі освітньо-кваліфікаційного рівня молодшого спеціаліста,
освітнього ступеня молодшого бакалавра,
освітньо-професійного ступеня фахового молодшого бакалавра)

Спеціальність:
125 «КІБЕРБЕЗПЕКА»

Харків
2021

Програма вступного екзамену за фахом розроблена для абітурієнтів, які вступають на скорочений термін навчання за освітньо-кваліфікаційним рівнем бакалавра на базі молодшого спеціаліста за спеціальністю 125 «Кібербезпека».

При оцінюванні враховуються:

характеристики відповіді абітурієнта: правильність, логічність, обґрунтованість, цілісність;

якість знань: повнота, глибина, гнучкість, системність, міцність;

сформованість загально навчальних та предметних умінь і навичок;

рівень володіння розумовими операціями: вміння аналізувати, синтезувати, порівнювати, абстрагувати, класифікувати, узагальнювати, робити висновки тощо;

досвід творчої діяльності (вміння виявляти проблеми та розв'язувати їх, формулювати гіпотези);

самостійність оцінних суджень.

Знання – складові вмінь абітурієнтів діяти.

Уміння виявляються в різних видах діяльності і поділяються на розумові і практичні.

Навички – дії доведені до автоматизму у результаті виконання вправ. Для сформованих навичок характерні швидкість і точність відтворення.

Цінності – ставлення виражають особистий досвід абітурієнтів, їх дії, переживання, почуття, які виявляються у відносинах до оточуючого (людей, явищ, природи, пізнання тощо). У контексті компетентнісної освіти це виявляється у відповідальності учнів, прагненні закріплювати позитивні надбання у навчальній діяльності, зростанні вимог до свої навчальних досягнень.

До характеристик якості знань належать:

повнота знань – кількість знань, визначених навчальною програмою;

глибина знань – усвідомленість існуючих зв'язків між групами знань;

гнучкість знань – уміння учнів застосовувати набуті знання у стандартних і нестандартних ситуаціях; знаходити варіативні способи використання знань; уміння комбінувати новий спосіб діяльності із вже відомих;

системність знань – усвідомлення структури знань, їх ієрархії і послідовності, тобто усвідомлення одних знань як базових для інших;

міцність знань – тривалість збереження їх в пам'яті, відтворення їх в необхідних ситуаціях.

Модуль “Кібербезпека”

Тема 1. Механізми і політики безпеки.

Основні поняття та визначення безпеки. Послуги безпеки: конфіденційність, цілісність, доступність, причетність, спостережність. Розподіл послуг безпеки за рівнями моделі *ISO/OSI*. Критерії захищеності комп’ютерних систем.

Тема 2. Механізми шифрування. Симетричні та несиметричні криптосистеми

Математичні основи сучасної теорії захисту інформації. Прості шифри. Принципи симетричного шифрування даних. Криптографічні примітиви та типи структур симетричного шифрування. Принципи шифрування у блокових симетричних шифрах. Принципи архітектури блокових симетричних шифрів (БСШ). Принципи несиметричного шифрування даних. Основні режими використання БСШ. Асиметричні алгоритми шифрування даних *RSA* й Ель Гамаля.

Тема 3. Протоколи автентифікації. Цифрові підписи

Принципи захисту інформації на мережевому рівні. Протоколи захисту та цілісності *IPSec*, *SSL*, *TLS*, їх сутність. Класифікація механізмів автентифікації. *MDC*-коди, основні алгоритми. *MAC*-коди, основні способи формування. Класифікація стандартів електронних цифрових підписів. Основні стандарти цифрового підпису.

Тема 4. Комплексні системи захисту даних

Основні функції систем захисту *PGP* і *CS MIME*. Принципи сумісності на рівні електронної пошти. Принципи побудови захищеної електронної пошті.

Тема 5. Основні види атак на програмне забезпечення. Основи криптоаналізу

Формальне математичне визначення криптосистеми. Критерії та показники ефективності. Класифікація криптоаналітичних атак. Принципи лінійного та диференціального криптоаналізу.

Тема 6. Основи цифровій стеганографії

Основні принципи приховування повідомлення на основі методів стеганографії. Класифікація и принципи приховування алгоритмів цифровій стеганографії.

Тема 7. Основи технології відкритих ключів (PKI).

Основні компоненти та сервіси інфраструктури відкритих ключів. Архітектура та топологія PKI. Сертифікати відкритих ключів X.509.

Тема 8. Захист програмного забезпеченні в Інтернет-технологіях

Основні принципи захисту інформації під час підключення до мережі Інтернет. Використання паролів і механізмів контролю.

Тема 9. Захист персональних даних

Основні принципи захисту персональних даних на основі програмного коду. Моделі захисту персональних даних.

Тема 10. Основні принципи захисту програмного забезпечення

Принципи забезпечення програмного забезпечення на кожному етапі життєвого циклу ПЗ.

Приклад
завдань екзаменаційного білету з кібербезпеки

Завдання 1

1. Метод функціонального перетворення для автентифікації - це
а. Введення паролю
б. Обчислення виразу виду X = 3 + 6
в. Вибір паролю з визначеного набору
2. Протоколи автентифікації з нульовою передачею знань були створені для:
а. автентифікації користувача
б. автентифікації інтелектуальних карт
3. Яку процедури передбачає цифровий підпис
а. Постанови
б. Постперевірки
в. Ідентифікації
г. Авторизації
е. Формування ключів, гешування
4. Яку з перерахованої інформації не містить цифровий підпис:
а. дату формування підпису
б. час закінчення дії таємного ключа даного підпису
в. час начала дії секретного ключа даного підпису
г. інформацію о тому, хто підписав документ
д. власне ЦП
5. Геш-функція –
а. призначена для збільшення якості підписаного документу
б. приймає у якості аргументу повідомлення довільної довжини та повертає геш-значення фіксованої довжини
в. Значення геш-функції не залежить від тексту та дозволяє відновити сам документ
6. Безпека інформації – це:
а. Стан інформації, оброблюється та передається
б. Сукупність цілеспрямованих дій та заходів
7. Цілісність інформації – це:
а. Дані спотворені ненавмисно
б. Дані у системі не відрізняються від даних у вихідних документах
в. Дані спотворені навмисно, але не дуже
8. Шкода безпеці – це:
а. Порушення стану захищеності інформації
б. Атака на засоби обробки інформації
в. Пошук та використання тієї чи іншої уразливості
9. Фундаментальна загроза – це:
а. Витік інформації
б. Порушення якості
в. Відмова в використанні мови
г. Використання ресурсів авторизованим суб'єктом

10. Порушення повноважень – це:
а. Загроза проникнення
б. Загроза впровадження
в. Базові загрози

Завдання 2

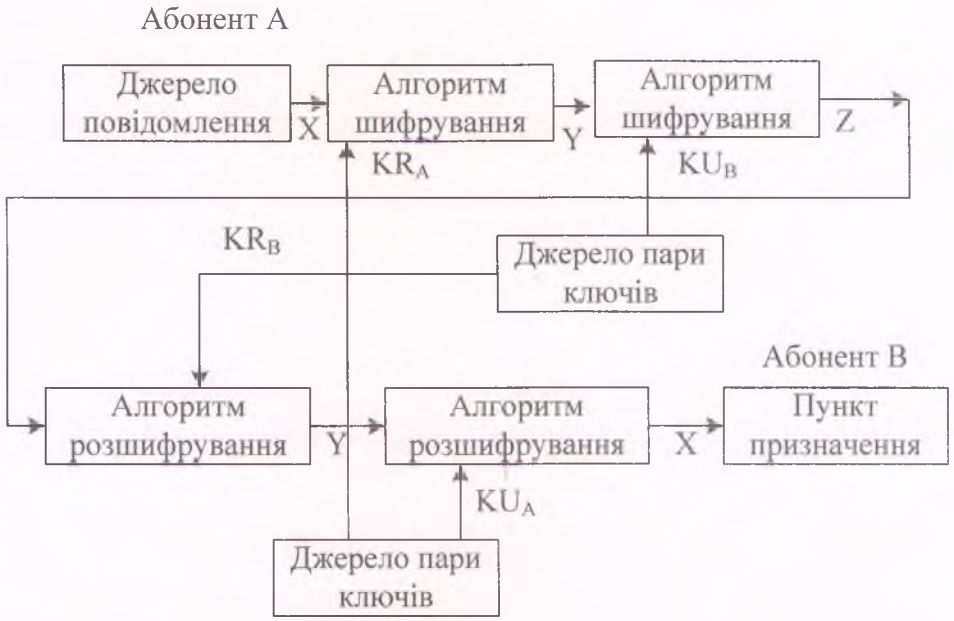
Побудуйте протокол обміну інформації між користувачами А і В за допомогою алгоритму гешування для забезпечення конфіденційності. Визначити достоїнства та недоліки даного протоколу. Порівняйте з протоколами асиметричного шифрування.

РОЗВ'ЯЗАННЯ

Завдання 1

Питання 1: Відповіді: 1 – а, 2 – г, 3 – е, 4 – б, 5 – б, 6 – б, 7 – б, 8 – в, 9 – а, 10 – а.

Завдання 2



Ключами є відкритий і закритий:
KR – (*n*, *b*) – закритий (особистий)
KU – (*n*, *e*) – відкритий

Алгоритм забезпечення автентичності використовує закритий ключ абоненту А: $Y = X^b \bmod n$, алгоритм забезпечення конфіденційності використовує відкритий ключ абоненту В: $Z = Y^e \bmod n$.

Основною перевагою несиметричних алгоритмів є забезпечення доказової стійкості, основним недоліком – низька швидкість на 2–3 порядку нижче симетричних алгоритмів шифрування.

Критерії оцінювання

Кожний білет складається із двох завдань, їх бездоганне виконання оцінюється 200 балами (максимальна оцінка) за шкалою ХНЕУ ім. С. Кузнеця.

Перше завдання з кібербезпеки є діагностичним і являє собою тест, що містить 30 питань. Тестові питання вимагають від абітурієнта знання основ з безпеки інформації в межах тем модуля. Перше завдання оцінюється від 0 до 150 балів. За правильну відповідь на одне питання абітурієнт отримує 5 балів.

Друге завдання – задача на побудову відповідних протоколів взаємозв'язку між користувачами для забезпечення відповідних послуг безпеки, воно є евристичним. Для розв'язання задачі потрібно розробити структурну схему протоколу та відповісти на додаткові питання.

Друге завдання оцінюється у відповідності з наступними показниками:

Оцінка 50 балів. Практичне завдання виконано бездоганно з повним обґрунтуванням кожного етапу виконання завдання, зроблені повні висновки та узагальнення. Приведений протокол обміну відповідає вимогам відповідного стандарту, приведені алгоритми шифрування/розшифрування з повними поясненнями, сформована криптограма (повідомлення) відповідає алгоритму шифрування (розшифрування), визначені достоїнства і недоліки обґрунтовані, проведений порівняльний аналіз обґрунтований. Наведені механізми та послуги в яких використовуються відповідні протоколи (схеми шифрування).

Оцінка 45 балів. Практичне завдання виконано повністю з обґрунтуванням кожного етапу виконання завдання. Приведений протокол обміну відповідає вимогам відповідного стандарту, приведена структурна схема протоколу з повними поясненнями процедур шифрування/розшифрування, сформована криптограма (повідомлення) відповідає алгоритму шифрування (розшифрування), визначені основні достоїнства і недоліки обґрунтовані, в цілому проведений порівняльний аналіз обґрунтований.

Оцінка 40 балів. Практичне завдання виконано повністю. Приведений протокол обміну відповідає вимогам відповідного стандарту, приведені основні процедури шифрування/розшифрування з поясненнями, сформована криптограма (повідомлення) відповідає алгоритму шифрування (розшифрування), але не в повному обсязі визначені основні достоїнства і недоліки, в цілому проведений порівняльний аналіз обґрунтований.

Оцінка 35 балів. Практичне завдання виконано повністю. Приведений протокол обміну відповідає вимогам відповідного стандарту, приведені основні процедури шифрування/розшифрування з поясненнями, сформована криптограма (повідомлення) відповідає алгоритму шифрування (розшифрування), але не в повному обсязі визначені достоїнства і недоліки, проведений порівняльний аналіз не обґрунтований.

Оцінка 30 балів. Практичне завдання виконано повністю. Приведений протокол обміну відповідає вимогам відповідного стандарту, приведені основні процедури шифрування/розшифрування з поясненнями, сформована криптограма (повідомлення) відповідає алгоритму шифрування (розшифрування), але не в повному обсязі визначені достоїнства і недоліки, не проведений порівняльний аналіз.

Оцінка 25 балів. Практичне завдання виконано неповністю. Приведений протокол обміну відповідає вимогам відповідного стандарту, приведені алгоритми шифрування/розшифрування, але сформована криптограма або повідомлення не відповідають алгоритму шифрування або розшифрування, не визначені основні достоїнства і недоліки, не проведений порівняльний аналіз.

Оцінка 20 балів. Практичне завдання виконано неповністю. Приведений протокол обміну в цілому відповідає вимогам відповідного стандарту, приведені алгоритми шифрування/розшифрування, але сформована криптограма і повідомлення не відповідають алгоритму шифрування/розшифрування, не визначені основні достоїнства і недоліки, не проведений порівняльний аналіз.

Оцінка 15 балів. Практичне завдання не виконано. Приведений протокол обміну не відповідає вимогам відповідного стандарту, не приведені алгоритми шифрування/розшифрування, сформована криптограма і повідомлення не відповідають алгоритму шифрування/розшифрування, пояснень процедур не має, не визначені достоїнства і недоліки, не проведений порівняльний аналіз.

Оцінка 10 балів. Практичне завдання не виконано. Протокол обміну не приведений, не приведені алгоритми шифрування/розшифрування, сформована криптограма і повідомлення не відповідають алгоритму шифрування/розшифрування, не визначені достоїнства і недоліки, не проведений порівняльний аналіз.

Оцінка 5 балів. Практичне завдання не виконано. Не сформована криптограма та вибраний другий протокол механізму безпеки.

Підсумкова оцінка за екзамен з кібербезпеки є сумою оцінок (балів), отриманих за кожне завдання.

Обмеження в часі на реалізацію завдань з модулем "Кібербезпека" – 45 хвилин.

Рекомендована література

1. Столлингс В. Криптография и защита сетей: принципы и практика, 2-е изд.: Пер. с англ. – М.: Издательский дом «Вильямс», 2001. – 672 с.: ил. – Парал. тит. англ.
2. Грибунин В. Г. Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. – Москва : СОЛОН-Прес, 2002. – 272 с.
3. Нильс Фергюсон, Брюс Шнайер. Практическая криптография. : Пер. с англ. – М. : Издательский дом"Вильямс", 2004. – 432 с.
4. Брюс Шнайер. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С. Переводчик: Дубнова Н. – Второе издание : – М.: Диалектика, 2003. – 610 с.

Голова атестаційної комісії
факультету інформаційних технологій
ХНЕУ ім. С. Кузнеця к.т.н., доц. **Роман КОРОЛЬОВ**