МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ БІЗНЕС-КОЛЕДЖ

Захарова М.В., Хотунов В.І., Люта М.В.,
Бурмістров С.В., Михайлюта С.Л.

Надійність та захист інформації в комп'ютерних системах та мережах. Методичні рекомендації щодо виконання курсової роботи

Черкаси – 2022

***УДК** 004.056*

Рекомендовано до друку рішенням методичної ради
Черкаського державного бізнес-коледжу.
Протокол № 03-22/23 від 27 грудня 2022 р.

Укладачі: Захарова М.В., Хотунов В.І., Люта М.В., Бурмістров С.В., Михайлюта С.Л.

Надійність та захист інформації в комп'ютерних системах та мережах. Методичні рекомендації по виконанню курсової роботи з дисципліни, Черкаси, 2022 р. – 44 с.

Рецензент: Розломій І.О., кандидат технічних наук, старший викладач кафедри інформаційних технологій Черкаського національного університету ім. Б. Хмельницького.

Навчально-методична розробка містить вступ, призначення та завдання до курсової роботи, порядок роботи, загальні відомості до об'єму курсової роботи, порядок виконання та правила оформлення роботи, підготовку до захисту та захист курсової роботи, орієнтовний перелік тем до виконання роботи, список використаних джерел, додатки.

Призначено для здобувачів освітнього ступеня бакалавра спеціальності «Комп'ютерна інженерія».

Затверджено на засіданні кафедри комп'ютерної інженерії та інформаційних технологій
Протокол № 5 від 27 грудня 2022 року

ЗМІСТ

ВСТУП 4
1. ПРИЗНАЧЕННЯ ТА ЗАВДАННЯ КУРСОВОЇ РОБОТИ 5
2. ПОРЯДОК РОБОТИ НАД КУРСОВОЮ РОБОТОЮ 21
3. ЗАГАЛЬНІ ВИМОГИ ДО ОБ'ЄМУ КУРСОВОЇ РОБОТИ 23
4. ПОРЯДОК ВИКОНАННЯ КУРСОВОЇ РОБОТИ 24
5. ПРАВИЛА ОФОРМЛЕННЯ КУРСОВОЇ РОБОТИ 25
5.1 Вимоги до оформлення текстових документів 25
5.2 Порядок комплектування документів 29
6. ПІДГОТОВКА КУРСОВОЇ РОБОТИ ДО ЗАХИСТУ І ЗАХИСТ КУРСОВОЇ РОБОТИ 30
7. ОРІЄНТОВНИЙ ПЕРЕРЛІК ТЕМ ДО ВИКОНАННЯ КУРСОВОЇ РОБОТИ 31
СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ 32
Додатки 34

ВСТУП

Важливою формою активізації процесу засвоєння знань при підготовці фахівців в області інформаційної безпеки є виконання курсових робіт.

Метою курсової роботи є систематизація, закріплення і поглиблення теоретичних знань студентів щодо методології та методики забезпечення інформаційної безпеки інформаційних ресурсів, визначення вихідних даних для проєктування системи захисту інформації, а також набуття навичок вирішення практичних завдань з захисту інформації.

Методичні вказівки з дисципліни «Надійність та захист інформації в комп'ютерних системах та мережах» (НЗІКС) призначені для надання допомоги студентам при виконанні курсової роботи.

Методичні вказівки забезпечують єдність вимог з боку викладача щодо структури, змісту, обсягу, оформлення та підготовки курсової роботи до захисту. Методичні вказівки містять методику та послідовність виконання окремих елементів курсової роботи, рекомендації по оформленню курсової роботи, список рекомендованих джерел.

Основне завдання даної роботи - надання необхідної методичної допомоги, з метою спрямувати зусилля студентів на якісне виконання курсової роботи. Методичні вказівки складено з урахуванням типових вимог до курсових робіт студентів і орієнтовані на підвищення якості їх виконання.

Навчально-методична розробка містить вступ, призначення та завдання до курсової роботи, порядок роботи, загальні відомості до об'єму курсової роботи, порядок виконання та правила оформлення роботи, підготовку до захисту та захист курсової роботи, орієнтовний перелік тем до виконання роботи, список використаних джерел, додатки.

Призначено для здобувачів освітнього ступеня бакалавра спеціальності «Комп'ютерна інженерія».

1. ПРИЗНАЧЕННЯ ТА ЗАВДАННЯ КУРСОВОЇ РОБОТИ

Тематика курсової роботи може будуватися на основі фактичного матеріалу промислових підприємств, на матеріалах виробничої практики студентів, на базі наукових праць викладачів і студентських учбово-дослідних робіт, а також інших розробок.

Завдання на курсову робту є індивідуальним. Припускається розробка комплексних тем, відповідні розділи яких складають зміст робіт декількох студентів даної спеціальності. Така організація дозволяє значно підсилити проробку кожного розділу комплексної теми і підвищити науково-технічний рівень проєктування.

Курсова робота є складовою частиною навчального курсу НЗІКС і призначена для практичного закріплення і розширення отриманих теоретичних знань.

Завданням курсової роботи є вивчення науково-технічної та довідкової літератури в галузі інформаційної безпеки, набуття студентами навичок забезпечення безпеки ІР та обґрунтованого вибору програмних засобів для захисту інформації для конкретного підприємства.

При виконанні курсової роботи слід керуватися такими принципами:

- Система інформаційної безпеки є інтегральною частиною інформаційної системи компанії і повинна функціонувати, не порушуючи експлуатаційних параметрів інформаційної системи.
- Система інформаційної безпеки (ІБ) ґрунтується на політиці безпеки організації, відповідно до якої чітко визначаються фізичні та логічні межі системи.
- Аналіз ризиків є основою проєктування і подальшого використання системи інформаційної безпеки (при введенні системи в експлуатацію ризики повинні бути

знижені до прийнятного, заздалегідь визначеного і затвердженого рівня).

- Впровадження засобів забезпечення ІБ має бути обґрунтовано: інвестуються в систему інформаційної безпеки засоби повинні бути адекватні тим перевагам, які отримає компанія при досягненні заданого рівня інформаційної безпеки.

При виконанні завдання до курсової роботи в якості вихідних даних студенти обирають об'єкт захисту у вигляді офісу фірми чи підприємства (відділу), інформаційної системи, використовуваної на підприємстві, локальної мережі, виділеного приміщення, в якому здійснюється робота з конфіденційною інформацією. Необхідно дати загальну характеристику підприємства.

Потім необхідно провести передпроєктні обстеження системи безпеки інформації всієї організації (якщо підприємство невелике) чи інформаційної безпеки окремої ІТ-системи (мереж передачі даних, обчислювальних систем и систем зберігання даних) для великої організації, розглянувши:

- всі ресурси, на яких зберігається цінна інформація;
- всі мережеві групи, в яких знаходяться ресурси системи (тобто фізичні зв'язки ресурсів один з одним);
- відділи, до яких відносяться ресурси;
- види цінної інформації;
- збиток для кожного виду цінної інформації за трьома видами загроз: зовнішні, внутрішні, комбіновані;
- бізнес-процеси, в яких обробляється інформація;
- групи користувачів, які мають доступ до цінної інформації;
- клас групи користувачів;
- доступ групи користувачів до інформації;
- характеристики цього доступу (вид і права);

- засоби захисту інформації;
- засоби захисту робочого місця групи користувачів.

Крім того, при проведенні діагностичного обстеження / аудиту системи захисту необхідно виконати:

- класифікацію інформаційних ресурсів за ступенем важливості / критичності особи;
- виявлення посадових осіб, відповідальних за цілісність цих ресурсів.

Пропонований порядок визначення вимог до захищеності циркулюючої в системі інформації представлений нижче:

1. Складається загальний перелік типів інформаційних пакетів, циркулюючих в системі (документів, таблиць). Для цього з урахуванням предметної області системи пакети інформації розділяються на типи по її тематиці, функціональним призначенням, схожості технології обробки та ознаками.

На наступних етапах початкове розбиття інформації (даних) на типи пакетів може уточнюватися з урахуванням вимог до їх захищеності.

2. Потім для кожного типу пакетів, виділеного в першому пункті, і кожного критичного властивості інформації (доступності, цілісності, конфіденційності) визначаються (наприклад, методом експертних оцінок):

- перелік і важливість (значущість за окремою шкалою) суб'єктів, інтереси яких зачіпаються при порушенні даної властивості інформації;

- рівень потенційного збитку (незначний, малий, середній, великий, дуже великий) і відповідний рівень вимог до захищеності.

При визначенні рівня потенційного збитку необхідно враховувати:

- вартість можливих втрат при отриманні інформації

конкурентом;
- вартість відновлення інформації при її втраті;
- витрати на відновлення нормального процесу функціонування КС.

Якщо виникають труднощі через великий розкид оцінок для різних частин інформації одного типу пакетів, то слід переглянути розподіл інформації на типи пакетів, повернувшись до попереднього пункту методики.

3. Для кожного типу інформаційних пакетів з урахуванням значущості суб'єктів і рівнів збитків встановлюється ступінь необхідної захищеності по кожному з властивостей інформації (при рівності значущості суб'єктів вибирається максимальне значення рівня).

Аналіз інформаційних ризиків - це процес комплексної оцінки захищеності інформаційної системи з переходом до кількісних або якісних показників ризиків. При цьому ризик - це ймовірний збиток, який залежить від захищеності системи. Отже, з аналізу ризику можна отримати або кількісну оцінку ризиків (ризик вимірюється в грошах), або - якісну (рівні ризику; зазвичай: високий, середній, низький).

Оцінка ризиків інформаційної безпеки здійснюється за допомогою побудови моделі інформаційної системи організації з точки зору ІБ:

Розглядаючи засоби захисту ресурсів з цінною інформацією, взаємозв'язок ресурсів між собою, вплив прав доступу груп користувачів, організаційні заходи, модель досліджує захищеність кожного виду інформації.

Ідентифікувати і оцінити активи, розробити модель порушника і модель загроз, ідентифікувати уразливості - все це стандартні кроки аналізу ризиків.

Таким чином, при проєктуванні ефективної системи захисту необхідно сформулювати вимоги до системи, розробити методи визначення цінності або критичності

інформаційних ресурсів та методи реагування на появу загроз безпеці, застосовувати ефективні механізми захисту для реалізації всіх необхідних функцій, пов'язаних із забезпеченням конфіденційності і цілісності інформації.

В даний час склалися певні підходи до проєктування систем, що забезпечують захист, які можна розділити на два основні класи: побудова індивідуальних систем, найбільш повно враховують умови функціонування об'єкта, що захищається інформатизації, структуру та вимоги до його інформаційній системі, і побудова систем з використанням типових проєктних рішень. Індивідуальне проєктування систем з використанням типових засобів захисту інформації застосовується в рамках попереджуючої стратегії, коли система захисту будується на етапі проєктування (рис. 1.1). Це дозволяє більш глибоко проаналізувати можливий вплив на інформаційні ресурси об'єкта внутрішніх і зовнішніх дестабілізуючих факторів, вибрати оптимальний набір механізмів захисту від них.

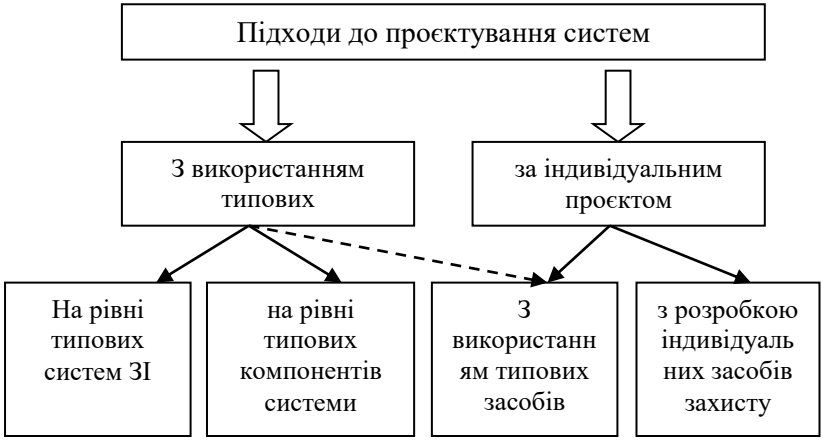

Рисунок 1.1 — Підходи до проєктування систем

Джерело: розробка автора

Індивідуальне проєктування СЗІ з використанням типових засобів захисту інформації застосовується в рамках попереджуючої стратегії, коли система захисту будується на етапі проєктування. Воно дозволяє більш глибоко проаналізувати можливий вплив на інформаційні ресурси об'єкта внутрішніх і зовнішніх дестабілізуючих факторів, вибрати оптимальний набір механізмів захисту від них, визначити організаційну побудову СЗІ. Тому можна стверджувати, що застосування зазначеного підходу дозволяє добитися максимуму рівня безпеки інформації. Основною проблемою при реалізації такого підходу до проєктування стає значне в порівнянні з типовим підходом збільшення часових ресурсів і необхідність залучення для цього більш високого рівня фахівців. І як наслідок веде до істотного подорожчання системи захисту, що не завжди буває виправдано.

Найчастіше невеликі організації не маючи необхідність захисту своїх інформаційних ресурсів не готові до великих вкладень в створення системи захисту інформації. Це відбувається коли вартість активів організації (величина потенційного збитку) невелика в порівнянні з витратами на їх захист. У цих умовах найбільш доцільним представляється створення СЗІ з використанням типових засобів захисту. Разом з тим пропонується визначати склад засобів захисту виходячи з індивідуальних особливостей ОІ (аналізу його складу і погроз).

В даний час на ринку представлений величезний арсенал програмних і технічних засобів, за тим або іншим ступенем забезпечують конфіденційність, цілісність, доступність інформації, що захищається, що володіють різними значеннями показників технічної надійності та ресурсоємності. Крім того, розроблено безліч організаційних механізмів захисту інформаційних ресурсів.

На сьогоднішній день, проєктування системи захисту

інформації полягає у виборі відповідного комплексу засобів захисту з існуючого різноманіття окремих засобів.

В цілому ***засоби забезпечення захисту інформації*** в частині запобігання навмисних дій в залежності від способу реалізації можна розділити на групи:

Технічні (апаратні) засоби. Це різні по типу пристрою (механічні, електромеханічні, електронні та інші), які апаратними засобами вирішують завдання захисту інформації. Вони або перешкоджають фізичному проникненню, або, якщо проникнення все ж таки відбулося, доступу до інформації, у тому числі за допомогою її маскування. Першу частину завдання вирішують замки, грати на вікнах, захисна сигналізація та ін. Другу - генератори шуму, мережеві фільтри, скануючі радіоприймачі і безліч інших пристроїв, "перекривають" потенційні канали витоку інформації або дозволяють їх виявити. Переваги технічних засобів пов'язані з їх надійністю, незалежністю від суб'єктивних чинників, високою стійкістю до модифікації. Слабкі сторони - недостатня гнучкість, відносно великі обсяг і маса, висока вартість.

Програмні засоби включають програми для ідентифікації користувачів, контролю доступу, шифрування інформації, видалення залишкової (робочої) інформації типу тимчасових файлів, тестового контролю системи захисту та ін. Переваги програмних засобів - універсальність, гнучкість, надійність, простота установки, здатність до модифікації та розвитку. Недоліки - обмежена функціональність мережі, висока чутливість до випадкових або навмисним змін, можлива залежність від типів комп'ютерів (їх апаратних засобів).

Змішані апаратно-програмні засоби реалізують ті ж функції, що апаратні і програмні засоби окремо, і мають проміжні властивості.

Організаційні засоби складаються з організаційно-

технічних (підготовка приміщень з комп'ютерами, прокладка кабельної системи з урахуванням вимог обмеження доступу до неї тощо) і організаційно-правових (національні законодавства і правила роботи, встановлюються керівництвом конкретного підприємства). Переваги організаційних засобів полягають у тому, що вони дозволяють вирішувати безліч різнорідних проблем, прості в реалізації, швидко реагують на небажані дії в мережі, мають необмежені можливості модифікації і розвитку. Недоліки - висока залежність від суб'єктивних факторів, в тому числі від загальної організації роботи в конкретному підрозділі.

Поява нових загроз неминуче спричиняє появу засобів захисту від них. Таким чином, ринок засобів захисту інформації постійно розвивається, а значить можна очікувати подальше збільшення номенклатури цих засобів.

Розглянемо приклад. В якості об'єкта дослідження була прийнята складна система, призначена для збору, зберігання, обробки, передачі та подання інформації, необхідної користувачеві. Об'єкт має локальну комп'ютерну мережу з виходом в мережу загального користування типу Internet. Локальна мережа розгорнута за схемою "зірка" за технологією Ethernet з одним сервером і концентратором. В якості мережевого протоколу використовується TCP/IP. Сервер знаходиться в окремому приміщенні і використовується як файл-сервер та сервер СУБД. Локальна база даних загального користування розташована на файл-сервері.

На об'єкті є інформаційні ресурси, конфіденційність, цілісність та доступність яких необхідно забезпечити. Джерелами загроз безпеки інформації можуть бути конкуренти, співробітники, що працюють на об'єкті, помилки при експлуатації, збої обладнання та ін. На сервері використовується розмежування доступу користувачів до файлів, контроль доступу здійснюється операційною

системою.

У багатьох випадках, збір вихідних даних про систему є досить трудомісткою задачею, переважна більшість вихідних даних на деяких етапах відсутня. Тому для опису процесів, в яких присутня невизначеність, застосовується система нечіткого виводу. Механізм нечіткого виводу можна представити у вигляді послідовності процедур: введення продукційних правил в базу даних, задання функції належності вхідних змінних, одержання оцінок вхідних змінних, фазифікації, агрегування, активізації та акумулювання висновків, дефазифікації.

Припустимо, що на основі експертного дослідження ІС отримані наступні оцінки вхідних змінних: ступінь небезпеки загрози та рівень вразливості інформаційного ресурсу. У результаті використання механізму нечіткого виводу одержані оцінки імовірності реалізації загрози (табл. 1).

Оцінка рівня захищеності ІР виконується згідно етапам:

На першому етапі необхідно проведення аналізу структури ІС, визначення задач та особливостей ІС, виявлення вразливих ресурсів ІС. Наприклад, показниками уразливості ресурсу і його особливо важливих компонентів є ступінь уразливості або вірогідність успішної дії порушників. Ресурсами ІС $X = \{X_1, X_2, X_3, ..., X_M\}$ можуть бути дані, засоби обчислювальної техніки, програмне забезпечення.

Таблиця 1

Одержання оцінок імовірностей реалізації загрози

Ступінь небезпеки загрози	Рівень уразливості ресурсу	Імовірність реалізації загрози
0,6	0,764	0,599
0,79	0,87	0,754
0,44	0,37	0,374
0,53	0,41	0,419
0,22	0,01	0,195
0,48	0,64	0,5

Другим етапом є визначення, аналіз і класифікація можливих загроз безпеки ІС. Загрози - події, наслідком яких можуть бути небажані у змісті захищеності впливи на інформацію, а саме порушення цілісності, приступності та конфіденційності інформації. При описі загроз безпеки мають бути ідентифіковані джерела цих загроз. Дослідження впливу загроз безпеки припускає проведення аналізу потенційних загроз, що впливають на ресурси ІС. Аналіз впливу загроз безпеки, у свою чергу, включає складання повного переліку потенційних загроз і дослідження можливості їхнього впливу.

На третьому етапі визначається вплив загроз на інформаційні ресурси та проводиться аналіз поводження ІС. Необхідно визначити множину потенційних загроз R та з кожним ресурсом ІС X_m зв'язати підмножину загроз R_m відносно повної множини R, що можуть впливати на ресурс X_m, скласти таблицю інтенсивностей, визначити імовірні характеристики потоку загроз на ІС. Ймовірнісні характеристики потоку загроз на ІС визначаються співвідношеннями: ймовірність того, що за інтервал часу Δt не відбудеться ні однієї атаки на ІС $P(t,\Delta t)=\exp\left(-\int_{t}^{t+\Delta t}\beta(t)dt\right)$ та ймовірність атаки на інтервалі Δt буде визначатися $P(t,\Delta t)=1-P_0(t,\Delta t)=1-\exp\left(-\int_{t}^{t+\Delta t}\beta(t)dt\right)$.

На четвертому етапі вибирається адекватна множина механізмів захисту. Захист ресурса X_m від загрози R_n може бути з застосуванням декількох механізмів безпеки з множини $M=\{M_1, M_2,..., M_k,..., M_K\}$, тоді стійкість механізму M_{nm} буде дорівнювати $P_{Vnm}=1-\prod(1-P_{Vnm})$. При виборі

механізмів захисту повинні враховуватися можливості управління ними для забезпечення максимально можливого рівня захищеності.

Підвищити рівень захищеності ІР дозволить вибір такого набору механізмів безпеки, який в комплексі при мінімізації вартості дозволить досягти максимізації загального рівня захищеності всієї інформаційної системи в цілому. Вибір механізмів захисту ресурса ІС можна проводити виходячи тільки з функціонального призначення, місця в ІС, властивостей ресурса, що захищається. Оцінка ефективності захисту виконується на рівні окремого механізму захисту, а її результати дозволяють визначити відносну здатність відповідної системи захисту інформації протистояти загрозам.

Кожному з механізмів захисту ставитися у відповідність деякий набір показників, наприклад, вартість, ресурсоємність, рівень захисту, що характеризують ступінь впливу даного механізму на ймовірність реалізації загрози безпеці інформації (рис. 1.2). Якщо всі показники, що описують властивості механізмів захисту і ресурсів ІС, що потребують захисту, виражені кількісно, то проєктування системи захисту інформації зводиться до математичної моделі. Для перетворення якісних показників в кількісні використовуються експертні оцінки.

Застосування ефективних механізмів захисту інформації впливає на значення імовірності реалізації загрози безпеці і коефіцієнта її небезпеки. Зміна коефіцієнта небезпеки загрози при застосуванні механізмів захисту може бути задано у вигляді початкових даних.

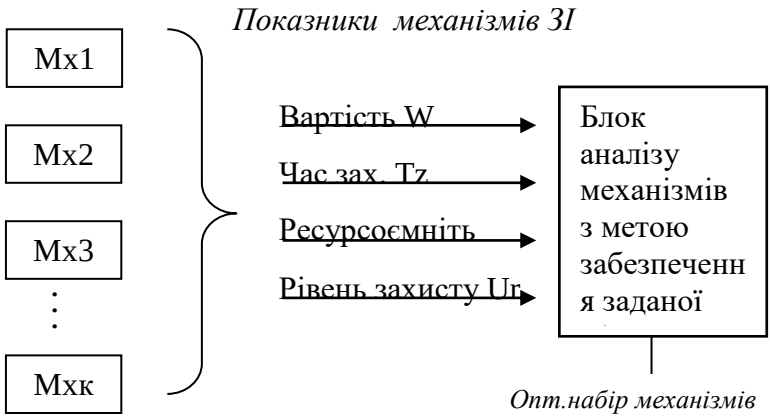

Рисунок 1.2 – Схематичне відображення вибору механізмів захисту

Джерело: розробка автора

Велика частина механізмів захисту впливає на ймовірність реалізації загроз безпеці інформації. Один з способів оцінки такого впливу заснований на задані зниження коефіцієнтів небезпеки та імовірності реалізації загроз в умовах захисту інформації безпосередньо експертами за допомогою нечітких чисел.

Нехай відомі всі можливі загрози безпеці ІС, будь-яка з цих загроз виявляється і реалізується за період часу з ймовірністю близькою до одиниці. Для кожної загрози $R = \{R_1,..., R_n,..., R_N\}$ визначений набір з механізмів захисту $M = \{Mx_1,..., Mx_k,..., Mx_K\}$ із заданими значеннями коефіцієнтів ефективності захисту $\varepsilon_{nk}, k = \overline{1,K}$ у вигляді нечітких чисел. Значення ε_{nk} не залежатиме від значення коефіцієнта небезпеки загрози R_n і імовірності реалізації

загрози P_r, а визначатиметься лише видом загрози та рівнем, до якого може бути знижена небезпека загрози і ймовірність її реалізації. Ефективність захисту ε_{nk} κ-го механізму захисту для n-го виду загрози задається двома зв'язаними таблицями D та H, що визначають, до якого рівня k-й механізм знижує коефіцієнт небезпеки n-й загрози та ймовірність її реалізації відповідно. В даному випадку, ε_{nk} з матриці D - значення коефіцієнта небезпеки.

$$\begin{array}{ll} \textit{Механізм } Mx_1 & \begin{pmatrix} \alpha(\varepsilon_{11}) & \alpha(\varepsilon_{12}) & \dots & \alpha(\varepsilon_{1n}) & \dots & \alpha(\varepsilon_{1N}) \end{pmatrix} \\ \textit{Механізм } Mx_2 & \begin{pmatrix} \alpha(\varepsilon_{21}) & \alpha(\varepsilon_{22}) & \dots & \alpha(\varepsilon_{1n}) & \dots & \alpha(\varepsilon_{2N}) \end{pmatrix} \\ \dots & \begin{pmatrix} \dots & \dots & \dots & \dots & \dots & \dots \end{pmatrix} \\ \textit{Механізм } Mx_k & \begin{pmatrix} \alpha(\varepsilon_{к1}) & \alpha(\varepsilon_{к1}) & \dots & \alpha(\varepsilon_{kn}) & \dots & \alpha(\varepsilon_{kN}) \end{pmatrix} \\ \dots. & \begin{pmatrix} .. & \dots & \dots & \dots & \dots & \dots \end{pmatrix} \\ \textit{Механізм } Mx_K & \begin{pmatrix} \alpha(\varepsilon_{K1}) & \alpha(\varepsilon_{K1}) & \dots & \alpha(\varepsilon_{Kn}) & \dots & \alpha(\varepsilon_{KN}) \end{pmatrix} \end{array}$$

Матриця H - ймовірність реалізації в умовах застосування механізмів захисту. Розглянемо приклад визначення ефективності механізму за допомогою експертних оцінок.

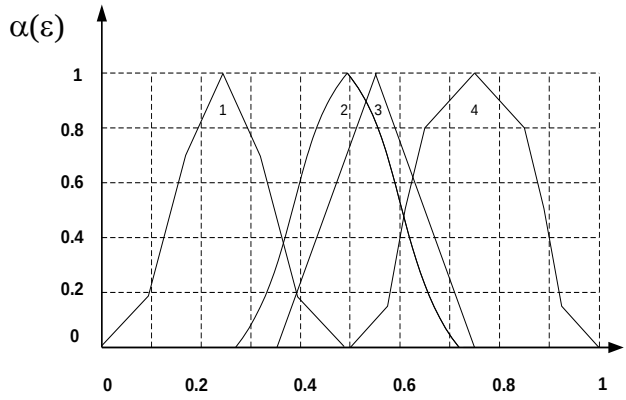

Рисунок 1.3 – Оцінки коефіцієнтів ефективності засобів
Джерело: розробка автора

Матриця D має вигляд:

R_n	0	0,1	0,2	0,3	0,4	0,5	0.6	0.7	0.8	0.9	1
Mx_1	0	0,18	0,83	0,78	0,18	0	0	0	0	0	0
Mx_2	0	0	0	0,09	0,22	1	0,52	0,04	0	0	0
Mx_3	0	0	0	0	0,24	0,73	0,74	0,24	0	0	0
Mx_4	0	0	0	0	0	0	0,4	0,9	0,9	0,1	0

По представленій матриці можна визначити, що найбільш ефективним є механізм Mx_1, оскільки найбільш імовірне значення отриманого коефіцієнта небезпеки дорівнює 0,25 (рис. 2). Коефіцієнт ефективності механізму захисту відповідно коефіцієнта небезпеки загрози може бути визначений через скінчене значення коефіцієнта небезпеки загрози R, те що вийшло після реалізації в системі механізму захисту, або, іншими словами те, наскільки знижується небезпека n-ої загрози в результаті застосування κ-ого механізму захисту

Нечіткі значення коефіцієнтів ефективності механізмів захисту для матриці H визначаються аналогічно. .

У випадку, якщо вибрано декілька механізмів захисту обчислюється за формулою 1:

$$\varepsilon_{nk}(D,H)=\prod_{n=1}^{N}\left(1-\prod_{k=1}^{K}\varepsilon_{nk}(D)\cdot\varepsilon_{nk}(H)\right) \qquad (1)$$

Інший спосіб оцінки впливу механізмів захисту на ймовірність реалізації загрози безпеці ґрунтується на отриманні за допомогою імітаційного моделювання, набору статистичних даних, в умовах застосування механізмів захисту залежності від часу коефіцієнтів небезпеки і імовірності реалізації загроз. Він заснований на визначенні тимчасових залежностей коефіцієнта небезпеки $R_n(t)$ та імовірності реалізації загрози $P(t)$.

Ефективності механізмів захисту в цьому випадку визначається у вигляді коефіцієнтів, залежних від часу, що зменшують коефіцієнт небезпеки загрози $\lambda(t)$ і ймовірність реалізації $\varphi(t)$. В цьому випадку формула (2) для обчислення ефективності захисту інформації у момент часу t має вигляд:

$$Z(t) = \prod_n ((1 - \lambda(t) R_n(t) \cdot \prod_s^S \omega_s P_x \varphi(t) P(t / x_s)))$$

У разі завдання коефіцієнта небезпеки загрози $\lambda(t)$ і коефіцієнта імовірності реалізації $\varphi(t)$ нечіткому вигляді, визначення $R_n(t)$ та $P(t)$, формулу (3) для обчислення ефективності захисту в умовах нечіткості можна представити у вигляді:

$$Z(t) = \prod_n ((1 - \lambda(t) R_n(t) \cdot \prod_s^S \omega_s P_x \varphi(t) P(t / x_s))) \cdot (R_n^{'}(t) \to Z^{'}) \quad (3)$$

де операції множення здійснюються за правилами теорії нечітких множин.

Оцінка ефективності захисту виконується на рівні окремого механізму захисту, а її результати дозволяють визначити відносну здатність відповідної системи захисту інформації протистояти загрозам. При виборі механізмів захисту повинні враховуватися можливості управління ними для забезпечення максимально можливого рівня захищеності. Раціональній вибір механізмів захисту інформації дозволяє здійснити побудову системи захисту інформації при обмежених витратах на реалізацію захисту та підвищити ефективність системи захисту інформації в цілому.

На п'ятому етапі побудуємо модель системи захисту інформації (СЗІ). Захист інформаційного ресурсу X_m від загрози R_n може бути з застосуванням декількох механізмів

безпеки з множини $M = \{M_1, M_2, ..., M_k, ..., M_K\}$. Інтенсивність порушення безпеки ресурсу X_m від загрози R_n: $\overline{\beta}_{nm}(t) = \dfrac{\overline{P}_{nm}(t, t+\Delta t)}{\Delta t}$, де $\overline{P}_{nm}(t, t+\Delta t)$ - імовірність хоча б однієї атаки ІР X_m від загрози R_n за Δt.

Модель СЗІ ІС враховує зміну інтенсивностей потоків атак, що впливають на ІР при застосуванні механізмів безпеки інформації: $\Delta\beta_{nm}(t) = \beta_{nm}(t) - \overline{\beta}_{nm}(t)$. Таким чином, етап побудови системи захисту інформації містить у собі реалізацію обраних механізмів захисту інформаційних ресурсів.

Керівник курсової роботи допомагає студенту скласти календарний графік його виконання і проводить систематичні консультації. Керівник рекомендує студентам основну літературу і довідкові матеріали за темою, призначає в календарному графіку терміни виконання окремих розділів курсової роботи і періодичних звітів про хід роботи.

Контроль керівника ні в якій мірі не звільняє студента від відповідальності за правильність виконання роботи і прийняті рішення. У виборі тих або інших рішень ініціатива надається студенту. При цьому керівник може рекомендувати відповідну літературу, журнальні статті і т.п., переслідуючи основну ціль - поглиблене самостійне вивчення студентом даного питання.

Студент цілком відповідає за прийняті рішення, правильність виконаних алгоритмів, розрахунків, використаних методів і засобів, якість виконання й оформлення курсової роботи, а також за своєчасне його завершення.

2. ПОРЯДОК РОБОТИ НАД КУРСОВОЮ РОБОТОЮ

Виконання курсової роботи починається з одержання індивідуального завдання. Студент повинний розробити і затвердити у керівника календарний графік виконання роботи. У процесі проєктування він консультується з керівником у міру потреби й у зв'язку з виникаючими питаннями.

Рекомендується виконання курсової роботи розбити на такі етапи.

1. Підготовчий етап. Студент повинний зрозуміти поставлену перед ним задачу, ознайомитися з рекомендованою літературою. При цьому варто критично підходити до вивчення джерел: рекомендується відбирати найбільше свіжі, останні дані і використовувати самі авторитетні джерела. Варто ясно уявити цілі розв'язуваної задачі й уважно проаналізувати вимоги, пред'явлені до її розв'язування.

2. Проєктний етап. На цьому етапі студент повинний розглянути різноманітні шляхи розв'язування поставленої задачі,

3. Реалізаціний етап. На початку цього етапу студент повинний вибрати найбільш раціональне рішення і скласти графік подальшої роботи. Варто звернути увагу на повноту, вірність і акуратність ведення документації в ході виконання курсової роботи.

4. Оформлювальний етап. Студент зобов'язаний оформити пояснювальну записку і графічний матеріал відповідно до вимог до оформлення технічної документації, що регламентуються чинними стандартами. Ціллю є забезпечення відповідності пояснювальної записки нормам і підготування студента до захисту курсової роботи.

5. Заключний етап. На цьому етапі проводиться захист

курсових робіт. Студент зобов'язаний подати керівнику остаточно оформлену пояснювальну записку до курсової роботи не пізніше, ніж за два дні до захисту. Керівник перевіряє роботу і дає вказівки про виправлення або доповнення, що студенту варто розглянути і внести в роботу, після чого підписує пояснювальну записку і додатки. На цьому курсова робота вважається закінченою і може бути подана до захисту.

3. ЗАГАЛЬНІ ВИМОГИ ДО ОБ'ЄМУ КУРСОВОЇ РОБОТИ

У пояснювальній записці укладений основний зміст роботи. Загальними вимогами пояснювальної записки є:

- чіткість викладання, логічна послідовність і повна відповідність завданню на курсову роботу;
- переконливість аргументації;
- конкретність викладання результатів роботи.

Структура пояснювальної записки і наближений об'єм окремих розділів такі:

(кількість сторінок)

Титульна сторінка, що оформлена за зразком (див. Додаток А)….	1
Завдання на курсову роботу……..……	1
Анотація……	1
Зміст……	1
Вступ……	1-2
Розділи і підрозділи основної частини ……....	25-30
Висновки ……...	2
Список літератури (не меньше 20-ти джерел інформації) …..……	1-2
Додатки……	10-15

Загальний об'єм пояснювальної записки повинний складати 27 – 35 сторінок максимального об'єму з урахуванням рисунків (без додатків). Перевищення максимального об'єму неприпустимо і розцінюється як невміння студента лаконічно викладати результати курсові роботи.

4 ПОРЯДОК ВИКОНАННЯ КУРСОВОЇ РОБОТИ

Виконання курсової роботи передбачає індивідуальну роботу за змістом обраної теми.

Основна частина пояснювальної записки може містити наступне:

- опис задачі;
- опис предметної області
- мета роботи.
- постановка задачі;
- вхідна і вихідна інформація.

У результаті теоретичного дослідження об'єкту проєктування, розробляється модель об'єкту чи процесу, визначаються його характеристики. Модель повинна з достатньою повнотою описувати процеси, що відбуваються в об'єкті та одночасно не бути складною для розуміння.

Визначення мети роботи. Мета розкриває те, заради чого здійснюється дослідження, та має описувати конкретні кроки, які необхідно здійснити для отримання результатів. Мета дослідження конкретизується у завданнях, сукупність яких дає уявлення про те, що слід зробити для її досягнення. Завдань повинно бути 4–5. Завдання формулюються дієсловами у формі переліку дій: "проаналізувати...", "з'ясувати...", "встановити...", "ідентифікувати...", "побудувати модель...", "оцінити"..., "порівняти...", "обґрунтувати...", "визначити чинники..." тощо.

Курсова робота виконується самостійно з рівномірним розподілом роботи протягом семестру.

5. ПРАВИЛА ОФОРМЛЕННЯ КУРСОВОЇ РОБОТИ

5.1 Вимоги до оформлення текстових документів

Пояснювальна записка є основним документом, запропонованим студентом при захисті курсової роботи. Вона складається відповідно до вимог чинних стандартів. У ній відбиваються етапи роботи і результати, отримані при виконанні курсової роботи.

Пояснювальна записка друкується студентом на одній стороні аркуша білого паперу формату А4:

— шрифт Times New Roman;

— розмір шрифту 14;

— міжрядкова відстань – півтора інтервали;

— вирівнювання – за шириною сторінки;

— поля на титульних листах – 2 см;

— назви структурних частин та розділів – великими літерами, напівжирним шрифтом, по центру, підрозділів – маленькими (крім першої літери), напівжирним шрифтом, по центру;

— відстань між заголовком та основним текстом – 1,5 пт;

— кожну структурну частину (розділ) починати з нової сторінки;

— нумерація сторінок – знизу справа;

— титульні листи, завдання не мають нумерації сторінок, але входять у загальну кількість аркушів у записці;

— анотація не має нумерацію сторінок і в кількість сторінок не входить;

— таблиці повинні мати заголовки і нумеруватися;

— рисунки, графіки, діаграми (відповідно до нумерації таблиць) повинні мати підписи і нумеруватися.

Заголовки структурних елементів роботи і заголовки розділів варто розташовувати посередині рядка і друкувати прописними літерами без крапок наприкінці, не підкреслюючи. Переноси слів у заголовку не допускаються.

Текст документа може містити ілюстрації у вигляді схем, діаграм і рисунків, що пояснюють текст. Як правило, ілюстрації нумеруються арабськими цифрами в межах усього документа. Допускається нумерація в межах кожного розділу (Наприклад: Рисунок 2.11). На ілюстрації дають посилання типу (рисунок 1.2). Посилання на раніше згадувані ілюстрації дають по типу (дивись рисунок 1.2). Ілюстрація не може бути поміщена раніш, чим перше посилання на неї!

Виклад змісту роботи в пояснювальній записці повинний бути стислим, чітким, що виключає можливість суб'єктивного тлумачення, і вестися від першої особи множинного числа, наприклад слова: "приймаємо", "вибираємо" і т.д. вживати не слід. Мова викладення повинна бути технічно грамотною, не містити жаргонних виразів і маловживаних слів.

Скорочення слів у тексті і підписах під ілюстраціями, як правило, не припускається.

Літерним позначенням різноманітних величин (значення символів і числових коефіцієнтів) при першому їхньому використанні варто давати розшифровування безпосередньо під формулою.

У записі обчислень по формулах наводять тільки вихідну формулу, вираз із підставленими цифрами й остаточний результат. Проміжні вирахування виключаються.

Весь текст пояснювальної записки поділяють на розділи. Кожний розділ варто починати з нової сторінки. Розділи в межах усієї пояснювальної записки, а також підрозділи і пункти мають порядкові номери, позначені арабськими цифрами без крапки наприкінці/

Вступ і висновки не нумеруються і виконуються великими

літерами.

Заголовки розділів пишуть великими літерами посередині тексту. Заголовки підрозділів пишуть малими літерами (крім першої великої). У заголовку не допускаються переноси слів. Пропуски над заголовками і під ними – 1,6 пт. Точку наприкінці заголовка не ставлять. Якщо заголовок складається з двох речень, тоді їх розділяють точкою. Заголовок підкреслювати не можна.

Нумерація сторінок пояснювальної записки повинна бути наскрізна. Номер сторінки проставляється арабськими цифрами. На титульних листах цифра 1 не ставиться.

Всі **ілюстрації** іменуються рисунками, що нумеруються послідовно в межах розділу арабськими цифрами. Номер рисунка повинний складатися з номера розділу і порядкового номера рисунка, розділених точкою (наприклад: Рисунок 2.5 - П'ятий рисунок другого розділу). Рисунки повинні бути чіткими. Кожний рисунок повинний супроводжуватися змістовним підписом. Наприклад:

Зображення

Рисунок 2.5 – Структура системи

Джерело: розробка автора

Підписи під рисунками або надписи над таблицями повинні бути стислими і пояснювати основний зміст. Підпис пишеться під рисунками в один рядок із номером. На всі ілюстрації і таблиці повинні бути посилання в тексті.

Таблиці служать для оформлення цифрового матеріалу, приводяться після першого нагадування в тексті. На всі таблиці повинні бути посилання в тексті, при цьому слово "Таблиця" у тексті пишуть повністю. Таблиці повинні

нумеруватися в межах розділу арабськими цифрами. Над лівим верхнім кутом таблиці поміщають напис "Таблиця" із указівкою порядкового номера таблиці. Номер таблиці складається з номера розділу і порядкового номера таблиці, розділених точкою (наприклад: Таблиця 2.4 - Четверта таблиця другого розділу).

Таблицю розміщують таким чином, щоб її можна було читати без повороту записки або з поворотом по годинниковій стрільці. При великій кількості рядків допускається перенос таблиці на інший аркуш. При цьому заголовок поміщають тільки в її першій частині, над іншими частинами пишуть: "Продовження таблиці ….." з вказівкою номера таблиці.

Формули в записці (якщо їх більш однієї) нумерують арабськими цифрами в межах розділу. Номер формули складається з номера розділу і порядкового номера формули в розділі, розділених точкою. Номер ставиться з правого боку аркуша на рівні нижнього рядка формули в круглих дужках, наприклад: (3.1) - перша формула третього розділу. Посилання на формулу вказують порядковим номером формули в круглих дужках, наприклад, "... у формулі (2.1)". Символи і числові коефіцієнти варто приводити безпосередньо під формулою зі слова "де" без двокрапки після нього в тієї ж послідовності, у якій вони дані у формулі з нового рядка.

Пояснення значень символів і числових коефіцієнтів, що входять в формулу, слід приводити безпосередньо під формулою тим же стилем і в тій же послідовності, в якій вони дані в формулі. Перший рядок повинен починатися зі слова "де" без двокрапки після нього.

Формули, які слідують одна за другою і не розділені текстом, розділяють комою.

У список використаних джерел включають усі використані джерела в порядку появи посилань на них у тексті пояснювальної записки. При посиланні в тексті на

використовувану літературу вказують порядковий номер, виділений двома квадратними дужками за списком джерел, наприклад [20].

5.2 Порядок комплектування документів

Документація комплектується в такій послідовності:

- титульний аркуш;
- завдання на курсову роботу;
- анотація;
- зміст;
- вступ
- основна частина;
- висновки;
- список літератури;
- додатки.

6. ПІДГОТОВКА КУРСОВОЇ РОБОТИ ДО ЗАХИСТУ І ЗАХИСТ КУРСОВОЇ РОБОТИ

Курсова робота закінчується захистом. За 5 днів до початку захисту оголошується час і місце його проведення. Перенос дня захисту курсові роботи можливий тільки при наявності поважних причин. Курсові роботи допускаються до захисту тільки з дозволу керівника. Під час захисту перевіряється рівень виконання студентом роботи і глибина розуміння їм виконаної роботи.

У процесі захисту студент повинний показати добрі знання за курсом відповідно до тих питань, що порушені в курсовій роботі, проявити уміння логічно мислити, переконливо обгрунтувати і відстояти (при необхідності) свою точку зору. На захисті доречні питання, що дозволяють перевірити знання по суміжних дисциплінах, на яких засновується розробка даного роботи.

7. ОРІЄНТОВНИЙ ПЕРЕРЛІК ТЕМ ДО ВИКОНАННЯ КУРСОВОЇ РОБОТИ

1. Забезпечення захисту даних в інформаційній системі «*Назва організації або відділу, або процесу*».
2. Захист системного та прикладного програмного забезпечення ІС на «*Назва організації або відділу, або процесу*».
3. Підсистема криптографічного захисту даних КС «Назва організації або відділу, або процесу, типу інформаційного ресурсу (ІР)»
4. Програмна реалізація методів забезпечення надійності функціонування комп'ютерних систем та мереж
5. Механізм/система вибору системи захисту для впровадження на «*Назва організації або відділу, або процесу*» з урахуванням вимог до інформаційної безпеки.
6. Інформаційна безпека, як елемент конкурентоспроможності організації «*Назва організації*».
7. Політика інформаційної безпеки для «*Назва організації або відділу, або процесу*».
8. Системи виявлення атак. Впровадження програмних засобів виявлення атак для інформаційної системи підприємства «*Назва*».
9. Політика інформаційної безпеки для системи (як приклад *кадрового агентства)*.
10. Інформаційна безпека технології віртуальних приватних мереж.
11. Підсистема вибору засобів забезпечення надійності функціонування комп'ютерних систем та мереж
12. Комплексна система інформаційної безпеки комп'ютера, підключеного до локальної мережі.
13. Проєктування системи інформаційної безпеки для відділу «*Назва відділу*» ТОВ «*Назва*».

Примітки: математичні перетворення; розрахунки або програмна реалізація алгоритмів захисту обов'язкові в КР.

СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

1. Василевський О. М., Ігнатенко О. Г. Нормування показників надійності технічних засобів : навчальний посібник. Вінниця : ВНТУ, 2013. 160 с.
2. Василевський О. М., Поджаренко В. О. Практикум з метрологічного нагляду за засобами вимірювань: Навчальний посібник. Вінниця: ВНТУ, 2008. 87 с.
3. Васюра А.С. Елементи та пристрої систем управління автоматики: Навчальний посібник. Вінниця: ВДТУ, 1999. 157 с.
4. Володарський Є. Т., Кошева Л. О. Статистична обробка даних: Навчальний посібник. К.: НАУ, 2008. 308 с.
5. Гавриленко В. В., Серебряков Р. А. Основи надійності комп'ютеризованих систем. Навчальний посібник. К.: НТУ, 2018. 214 с.
6. Джулій В. М., Кльоц Ю. П., Муляр І. В., Чешун В. М. Методи і алгоритми захисту інформаційних ресурсів комп'ютерних систем: навчальний посібник. Хмельницький: ХмНУ, 2020. 196 с.
7. Заміховський Л. М., Калявін В.П. Основи теорії надійності і технічної діагностики систем: Навчальний посібник. Івано-Франківськ: Вид-во "Полум'я", 2019. 360 с.
8. Матвієнко М. П., Розен В. П., Закладний О. М. Архітектура комп'ютера. Навчальний посібник. К: Видавництво Ліра-К, 2016. 264 с.
9. Надійність, контроль комп'ютерних систем та мереж [Текст]: конспект лекцій для студентів спеціальності 123 – «Комп'ютерна інженерія » денної та заочної форм навчання / уклад. О. І. Міскевич, К. Я. Бортник. Луцьк: Луцький НТУ, 2017. 44 с.
10. Тарарака В.Д. Архітектура комп'ютерних систем: навчальний посібник. Житомир : ЖДТУ, 2018. 383 с.

11. Федун І. В. Основи теорії надійності та контролю якості виробів електронної техніки: Лабораторний практикум. Вінниця: ВДТУ, 2003. 71 с.
12. Computer Hardware: Hardware Components and Internal PC Connections - Dublin Institute of Technology, 2015.

Додаток А

ЗРАЗОК ОФОРМЛЕННЯ ТИТУЛЬНОЇ СТОРІНКИ

Черкаський державний бізнес-коледж

(повне найменування вищого навчального закладу)
Кафедра комп'ютерної інженерії та інформаційних технологій

КУРСОВА РОБОТА

з дисципліни «Надійність та захист інформації в комп'ютерних системах та мережах»
на тему_____

Студента (ки) _____
групи
_____
(прізвище та ініціали)
Керівник роботи:
_____
(посада, вчене звання, науковий ступінь, прізвище та ініціали)

Кількість балів: _____
Оцінка: ECTS _____

Черкаси, 2022 рік

ДОВІДКА ПРО УКЛАДАЧІВ

Захарова Марія В'ячеславівна – к.т.н., доцент, доцент кафедри комп'ютерної інженерії та інформаційних технологій Черкаського державного бізнес-коледжу. Працює в ЧДБК з 2018 року. У 2001 році закінчила з відзнакою Черкаський інженерно-технологічний інститут (нині Черкаський державний технологічний університет) за спеціальністю «Інформаційні управляючі системи та технології». Із 2001 року до 2004 року навчалася в аспірантурі Черкаського державного технологічного університету за спеціальністю «Автоматизовані системи управління та прогресивні інформаційні технології». В 2010 р. захистила кандидатську дисертації на тему «Синтез механізмів захисту інформаційних ресурсів від кібератак» за спеціальністю 05.13.21 – Системи захисту інформації. Є автором понад 60 наукових та навчально-методичних праць.

Хотунов Владислав Ігорович – к.пед.н., доцент, завідувач кафедри комп'ютерної інженерії та інформаційних технологій Черкаського державного бізнес-коледжу. Працює в ЧДБК з 2016 року. Закінчив у 2005 році Черкаський національний університет ім. Б. Хмельницького за спеціальністю «математика», отримав диплом спеціаліста. В 2008 року вступив до аспірантури Черкаський національний університет імені Богдана Хмельницького за спеціальністю 13.00.02 – Теорія та методика навчання (математика) та в 2014 р. успішно захистив дисертацію на тему «Методика загальноосвітньої математичної підготовки майбутніх фахівців з інформатики та обчислювальної техніки в коледжах», диплом кандидата педагогічних наук. В 2015 році закінчив магістратуру Черкаського національного університету ім. Б. Хмельницького за спеціальністю «Управління навчальним закладом», кваліфікація керівник підприємства, установи та організації (у сфері освіти та виробничого навчання). Є автором понад 60 наукових та навчально-методичних праць.

Люта Майя В'ячеславівна – завідувач відділення інженерії програмного забезпечення Черкаського державного бізнес-коледжу з 2022 року. В 2001 році закінчила Український державний хіміко-технологічний університет за спеціальністю «Технологія

машинобудування», диплом спеціаліста. В 2011 році закінчила магістратуру Черкаського національного університету ім. Б. Хмельницького за спеціальністю «Педагогіка вищої школи» та в 2021 р. закінчила магістратуру Київського національного університету технологій та дизайну за спеціальністю «Комп'ютерна інженерія». Є автором та співавтором понад 20 наукових праць.

Бурмістров Сергій Владиславович – к.т.н., доцент кафедри комп'ютерної інженерії та інформаційних технологій Черкаського державного бізнес-коледжу. Працює в Черкаському державному бізнес-коледжі з 2005 року. В 1989 р. закінчив Корсунь-Шевченківське педагогічне училище за спеціальністю "Учитель трудового навчання і креслення". В 1997 р. закінчив Черкаський державний університет за спеціальністю "Учитель фізики, математики та обчислювальної техніки". В 2003 р. закінчив Черкаський державний університет за спеціальністю "Учитель англійської мови і літератури". В 2016 році в Черкаському державному технологічному університеті захистив кандидатську дисертацію за спеціальністю 05.13.05 – «комп'ютерні системи та компоненти». Є автором 37 наукових праць.

Михайлюта Сергій Леонтійович – к.т.н., доцент, доцент кафедри комп'ютерної інженерії та інформаційних технологій Черкаського державного бізнес-коледжу з 2021 року. В 1987 р. закінчив з відзнакою Смілянський технікум харчової промисловості, диплом техніка-електромеханіка за спеціальністю «Експлуатація автоматичних пристроїв у харчовій промисловості». В 1992 р. закінчив з відзнакою Черкаський інженерно-технологічний інститут, диплом інженера-електромеханіка за спеціальністю «Приладобудування». В 1995 р. закінчив аспірантуру Черкаського інженерно-технологічного інституту, диплом інженера-дослідника за спеціальністю «Прилади нерушійного контролю навколишнього середовища, матеріалів та виробів». В 2005 р. закінчив Східно-європейський університет економіки і менеджменту, диплом спеціаліста «Психолог. Менеджер персоналу» за спеціальністю «Менеджмент організацій». В 2006 р. захистив кандидатську дисертацію, диплом кандидата технічних наук за спеціальністю «Елементи та пристрої обчислювальної техніки та систем керування». Є автором та співавтором понад 70 наукових та навчально-методичних праць.

Навчальне видання

Захарова Марія В'ячеславівна
Хотунов Владислав Ігорович
Люта Майя В'ячеславівна
Бурмістров Сергій Владиславович
Михайлюта Сергій Леонтійович

Надійність та захист інформації в комп'ютерних системах та мережах.
Методичні рекомендації щодо виконання курсової роботи

Комп'ютерний набір Люта М.В.

Підписано до друку__ ___.2023 р. Формат 60х841/16
Папір офсетний. Гарнітура Times New Roman.
Друк офсетний
Умов. друк. арк. 0,9. Тираж 30 прим. Зам. № 343

За довідками з питань реалізації
звертатися за тел. (0472) 64-05-15