Голові спеціалізованої вченої ради Д 26.062.17
при Національному авіаційному університеті
03058, м. Київ, пр. Любомира Гузара, 1.

ВІДГУК
офіційного опонента

начальника кафедри захисту інформації та кібербезпеки Житомирського військового інституту імені С. П. Корольова доктора технічних наук, професора Грищука Руслана Валентиновича на дисертацію Гочара Сергія Феодосійовича "Методологія оцінювання ризиків кібербезпеки інформаційних систем об'єктів критичної інфраструктури", поданої ним на здобуття наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – системи захисту інформації

Актуальність теми

Суттєве зростання ризиків кібербезпеки інформаційних систем (ІС) об'єктів критичної інфраструктури (ОКІ) як в Україні, так і в світі висуває все нові й нові вимоги до їх кіберзахисту. На сьогодні забезпечення кіберзахисту ІС ОКІ досягається шляхом впровадження в них комплексних систем захисту інформації або систем інформаційної безпеки з підтвердженою відповідністю. Як в першому, так і в другому випадку впровадження тієї чи іншої системи захисту інформації передбачає оцінювання відповідних ризиків. Стає очевидним, чим повніше та коректніше буде проведено оцінювання, тим меншою буде ймовірність нанесення збитків ІС ОКІ.

Існуюча на сьогодні методологія оцінювання ризиків кібербезпеки зорієнтована в основному на ІС, які не віднесені до категорії критичних. В ній, як правило, не враховується суб'єктивний ризик. Як показує досвід, його неврахування може призвести до катастрофічних наслідків як для безпеки окремо взятої держави, так і світу в цілому. Прикладами тому є: кібератака *BlackEnergy* на енергосистеми Івано-Франківської, Київської та Чернівецької областей, яка мала місце в Україні наприкінці 2015 р. – початку 2016 р.; кібератака *Stuxnet* на атомну станцію в м. Бушер, яка мала місце в Ірані в 2010 р. тощо. Таким чином, подальший розвиток методології оцінювання ризиків кібербезпеки ІС у відношенні до ОКІ залишається актуальною науковою проблемою. *Отже, зважаючи на зв'язок теми дисертації Гончара С. Ф. з означеними вище питаннями, вважаємо її достатньо обґрунтованою та актуальною.*

Оцінка обґрунтованості наукових положень, висновків та рекомендацій, сформульованих у дисертації, їх достовірність, новизна

Загальна характеристика дисертації

У **вступі** здобувачем обґрунтовано актуальність обраної теми, показано її зв'язок з науковими програмами, планами, темами, сформульовано мету і задачі дослідження, визначено об'єкт, предмет та методи дослідження, відображено наукову новизну й практичне значення одержаних результатів, наведено дані щодо особистого внеску здобувача, результати апробації, дані про публікації та структуру й обсяг роботи.

У **першому розділі** здобувачем приведено результати аналізу сучасних методів та засобів оцінювання ризиків кібербезпеки ІС ОКІ. Зокрема здобувачем з одного боку проаналізовано чинне нормативно-правове забезпечення кібербезпеки ІС ОКІ, а з іншого – приведено результати аналізу останніх наукових досліджень і публікацій за обраною темою. За результатами аналізу *здобувачем встановлено*, що існуючі підходи не враховують вплив людського чинника на процес оцінювання ризиків кібербезпеки ІС ОКІ. Як наслідок *показано*, що подальший розвиток методології оцінювання ризиків кібербезпеки ІС ОКІ

51.11/03
від 20.03.2020

повинен зосередитися на вирішенні питань кількісного оцінювання комплексного ризику з урахуванням і технічної складової оцінювання, і впливу людського фактору.

Позитивною рисою першого розділу є те, що здобувач всебічно підійшов до вивчення стану проблеми – і в законодавчій складовій визначив існуючі недоліки, і в науковій складовій визначив подальші напрямки розвитку методології оцінювання ризиків. *Таким чином, одержані здобувачем у першому розділі результати виступили науковим підґрунтям для постановки проблеми в загальному вигляді та формалізації на її основі частинних наукових задач, які також приведені у розділі.*

У **другому розділі** приведено результати аналізу факторів, які впливають на стан кібербезпеки ІС ОКІ. Зокрема *подано модель загроз ІС ОКІ* до кібератак, що стало підґрунтям для *створення структурної моделі взаємодії* елементів таких систем. На відміну від відомих *розроблена модель дозволила* конкретизувати походження джерел загроз кібербезпеки ІС ОКІ як із зовнішнього, так і внутрішнього контурів управління.

З метою визначення ймовірності реалізації загроз кібербезпеки ІС ОКІ у другому розділі *здобувачем запропоновано* встановити взаємозв'язок між загрозами, вразливостями і ризиками, що в цілому відповідає класичному підходу до опису ймовірності виникнення кібератаки в ІС ОКІ. Такий підхід *дозволив встановити* життєвий цикл процесу аналізу ймовірності реалізації загроз. В основу оцінювання небезпеки кібератак в ІС ОКІ *здобувачем покладено* вперше введений показник негативного впливу, але при цьому, на жаль, не приведено його фізичну розмірність.

Науковий базис другого розділу дисертації становить метод визначення актуальності загрози кібербезпеки ІС ОКІ. На наш погляд, вдалим є рішення здобувача щодо подання розробленого методу у вигляді схеми (рис. 2.10, с. 142 дисертації, рис. 2, с. 13 автореферату відповідно). Таке подання результатів дослідження сприяє легкому ознайомленню фахівцями з суттю одержаних здобувачем нових наукових результатів. *Таким чином, запропоновані в другому розділі моделі та метод є теоретичним підґрунтям для розроблення методології оцінювання ризиків кібербезпеки ІС ОКІ.*

Третій розділ дисертації здобувач присвятив розробленню методів розрахунку суми ризиків кібербезпеки ІС ОКІ. Так зокрема, обґрунтовано та розроблено два методи.

Перший розроблений здобувачем метод відноситься до групи графоаналітичних методів. Його *перевагою* є можливість графічної візуалізації складних для сприйняття експертом процесів, які описують зв'язки між, власне, ризиком та ймовірністю від його настання та збитками. *Позитивною стороною* подання одержаного наукового результату є те, що його достовірність підтверджено рядом модельних прикладів. Це дозволяє покроково перевірити і сам метод, і одержуваний результат, а також його збіжність з результатами інших відомих досліджень.

Другий метод, який розроблено в розділі відноситься до групи аналітичних методів оцінювання ризику. Даний метод, *на відміну від відомих, дозволяє* в аналітичному вигляді визначати суму ризиків та подавати їх, залежно від початкових умов, у різній варіації. *Таким чином, одержані у третьому розділі наукові результати є основною для створення систем підтримки прийняття рішень щодо застосування заходів зі зменшення ризику.*

У **четвертому розділі** розроблено метод розрахунку комплексного ризику кібербезпеки ІС ОКІ. Під час розроблення методу *здобувачем враховано* об'єктивну та суб'єктивну складові ризику. При цьому сформульовано досить коректний висновок про те, що комплексний (результуючий) ризик не може бути алгебричною сумою суб'єктивної та об'єктивної складових. Вирішення даної задачі здійснено за рахунок втілення сформульованої особисто здобувачем ідеї щодо здійснення операцій у векторному просторі над числовими характеристиками векторів ризику, а саме їх довжинами та кутом між ними.

У третьому розділі здобувачем також розроблено модель комплексного ризику ІС ОКІ, яку можна вважати подальшим розвитком векторної моделі. На відміну від неї *нова модель враховує* весь можливий діапазон варіації кутів між векторами ризику. *Адекватність моделі*

підтверджено здійсненням її інтерпретації на основі введеного показника адекватності сприйняття ризику для кожного з кутів між векторами ризику. Таким чином, розроблені моделі стали основною для обґрунтування та подання в четвертому розділі дисертації нового методу обчислення комплексного ризику. Даний метод, на відміну від відомих, дозволяє враховувати величину впливу людського фактору на процес оцінювання ризиків в ІС ОКІ. *Таким чином, на основі математичного апарату теорії лінійної алгебри, аналітичної геометрії та функції комплексної змінної здобувачеві вдалося обґрунтувати та розробити новий метод розрахунку комплексного ризику кібербезпеки ІС ОКІ.*

П'ятий розділ дисертації здобувача присвячений створенню на основі запропонованих моделей та методів системи оцінювання ризиків кібербезпеки ІС ОКІ. Також показано, що створювана система оцінювання ризиків кібербезпеки ІС ОКІ ґрунтується на побудованій в розділі методології оцінювання ризику. *Перевагою розробленої методології* є те, що вона дозволяє будувати програмні та програмно-апаратні комплекси для оцінювання ризиків ІС ОКІ. Здобувачем *аргументовано доведено*, що створювані комплекси, на відміну від відомих, мають розширений функціонал, що дозволяє аналізувати розраховане значення ризику з гранично-допустимим значенням та наданням варіантів рішень щодо вибору методів оброблення ризику. Таким чином, в новостворювані системи захисту запропоновано закласти елементи системи підтримки прийняття рішень. Також у даному розділі подано спосіб виявлення кібератак на ІС ОКІ, який дозволяє реалізувати технологію інтелектуального аналізу даних в масштабі часу, наближеному до реального.

На основі створеної методології у розділі також розкривається сутність структурного рішення обчислювальної системи оцінювання ризику кібербезпеки ІС ОКІ. Його, як і попереднє рішення, зведено до апаратно-програмного комплексу, який в автоматизованому режимі здійснює розрахунок збитків від множини сумісних подій, що враховують ймовірність виникнення події та величину негативних наслідків. У розділі також розроблено "Калькулятор комплексного ризику", який дозволяє розраховувати повний ризик. *Таким чином, у розділі закладено основи для створення нового класу систем захисту інформації з елементами систем підтримки прийняття рішення, які спроможні розраховувати повний ризик кібербезпеки ІС ОКІ.*

Шостий розділ дисертації є заключним. У розділі подано результати експериментальних досліджень систем оцінювання ризиків кібербезпеки ІС ОКІ. Зокрема розкриті структури алгоритмів обчислення ризиків. Приведено результати перевірки роботоспроможності розробленої методології на реальній комплексній системі захисту інформації та інформаційно-телекомунікацій системі захищеного вузла Інтернет доступу ПрАТ "Фарлеп-Інвест". *Таким чином, у розділі обґрунтовано роботоспроможність розробленої методології та її можливість для практичного застосування для оцінювання ризиків ІС ОКІ.*

У **висновках** приведено основні одержані результати, їх наукову та практичну цінність, дані щодо впровадження результатів роботи.

У **додатках** до дисертації наведено: копії актів реалізації; копії патентів України на корисні моделі; лістинги роботи створених програмних засобів; загрози кібербезпеки ІС ОКІ.

Сформульовані в дисертації наукові положення, висновки та рекомендації достатньо повно обґрунтовані здобувачем та викладені в доказовій формі.

Наукова новизна одержаних особисто здобувачем результатів полягає у такому.

– *удосконалена* структурна модель взаємодії елементів ІС ОКІ, яка, за рахунок використання параметрів оцінювання рівня впливу внутрішніх та зовнішніх дестабілізуючих чинників на суб'єкт деструктивних дій, дозволяє розробити модель порушника даної інформаційної системи з урахуванням кіберзагроз, об'єктами яких є адміністратор, користувачі, технічний персонал;

– *удосконалено* метод визначення актуальності загрози кібербезпеки ІС ОКІ, який, за рахунок використання параметрів оцінювання потенційного рівня загрози, визначених з

використанням удосконаленої структурної моделі взаємодії елементів ІС, а також параметрів, що характеризують потенційних порушників для реалізації загрози, дозволяє розробити модель загроз даної ІС з урахуванням кіберзагроз, об'єктами яких є адміністратор, користувачі, технічний персонал;

– *вперше* розроблено методи обчислення сумарного ризику кібербезпеки ІС ОКІ, які, за рахунок використання параметрів оцінювання актуальності загрози, визначених з використанням удосконаленої структурної моделі взаємодії елементів ІС та удосконаленого методу визначення актуальності загрози, а також параметрів, що характеризують, для кожного ризику, наслідки повного знищення інформаційного активу, ймовірностей подій, що призводять до таких ризиків, дозволяють розраховувати суму визначеної множини ризиків, загальні наслідки та ймовірність їх реалізації;

– *вперше* розроблено векторну модель та модель комплексного ризику кібербезпеки ІС ОКІ, яка, за рахунок використання величини скалярного добутку векторів ризиків, визначених з використанням методу обчислення сумарного ризику, а також величин об'єктивних та суб'єктивних складових ризиків, дозволяє ввести довжину векторів ризиків, кут між ними та здійснювати векторні операції над ними;

– *вперше* розроблено метод обчислення комплексного ризику кібербезпеки ІС ОКІ, який, за рахунок використання значень довжин векторів ризику та кутів між ними, визначених з використанням векторної моделі та моделі комплексного ризику, дозволяє здійснювати оцінювання зазначених ризиків з урахуванням величини впливу людського чиннику;

– *вперше* розроблено методологію оцінювання ризику кібербезпеки ІС ОКІ, яка, за рахунок використання удосконаленої структурної моделі взаємодії елементів, удосконаленого методу визначення актуальності загрози, методу обчислення сумарного ризику, векторної моделі та моделі комплексного ризику, методу обчислення комплексного ризику, дозволяє забезпечити підтримку створення обчислювальних систем для автоматизації процесу оцінювання ризиків кібербезпеки ІС ОКІ;

– *вперше* запропоновано структурні моделі (рішення) обчислювальних систем для розрахунку суми ризиків кібербезпеки ІС ОКІ, які, за рахунок використання удосконаленої структурної моделі взаємодії елементів, удосконаленого методу визначення актуальності загрози, методу обчислення сумарного ризику, векторної моделі та моделі комплексного ризику, методу обчислення комплексного ризику, методології оцінювання ризику, дозволяють автоматизувати процес розрахунку сумарного ризику та обчислення комплексного ризику з урахуванням величин об'єктивної та суб'єктивної складових.

Достовірність наукових положень

Достовірність наукових положень дисертаційної роботи підтверджується:

– коректною постановкою наукової проблеми та часткових наукових задач дисертаційного дослідження (с. 69–70 дисерт. та с. 3, с. 4 автореф.);

– використанням в роботі теоретично обґрунтованих та широко апробованих на практиці методів теорії ризиків, системного аналізу, експертних оцінок, методів теорії комплексних чисел, векторної алгебри, лінійної алгебри та аналітичної геометрії, теорії ймовірностей, випадкових процесів, математичного та комп'ютерного модулювання;

– збіжністю результатів моделювання та експериментальних перевірок з відомими експериментальними даними інших академічних досліджень, відповідністю отриманих теоретичних результатів з результатами експерименту (с. 277–284 дисерт., с. 28, с. 29 автореф.);

– відповідністю наукових положень основним законам і явищам природи.

Наукове значення дисертаційної роботи полягає в подальшому розвитку теорії захисту інформації в частині, що стосується створення методології оцінювання ризиків кібербезпеки ІС ОКІ.

Практичне значення дисертації полягає в створенні діючого алгоритмічного, програмного та програмно-апаратного забезпечення, що може використовуватися для оцінювання ризиків кібербезпеки ІС ОКІ при створенні комплексних систем захисту інформації або систем управління інформаційною безпекою з підтверджено відповідністю.

Практична значущість одержаних результатів і достовірність наукових положень підтверджені актами впровадження (копії – с. 291–300 дисерт.), патентами України на корисну модель (копії – с. 301–305 дисерт.) і про що зазначено в авторефераті на с. 6 та с. 31 відповідно. Зазначені факти підтверджують особистий внесок здобувача в науку.

Мова та стиль викладення дисертації та автореферату дозволяють зрозуміти суть розроблених наукових положень і одержаних практичних результатів. Дисертація і автореферат у цілому відповідають вимогам, які висуваються до його оформлення відповідно до Порядку присудження наукових ступенів, затвердженого постановою Кабінету Міністрів України від 24.07.2013 р. № 567 (із змінами) та Вимог до оформлення дисертації, затверджених наказом Міністерства освіти і науки України від 12.01.2017 р. № 40. Зміст дисертації та автореферату викладено послідовно та логічно. Поряд з тим є деякі орфографічні неточності, наприклад на с. 212 дисертації та деякі некоректності на с. 27 дисертації (с. 8 автореферату відповідно).

Підтвердження повноти викладу основних результатів дисертації в опублікованих працях

За напрямом дисертаційного дослідження здобувачем опубліковано 51 наукову працю. У тому числі: 1 монографію, 2 наукові статті в міжнародних рецензованих виданнях, що входять до наукометричної бази даних *Scopus*, 11 наукових статей в наукових виданнях, що входять до інших міжнародних наукометричних баз, 14 наукових статей у вітчизняних фахових наукових журналах та збірниках наукових праць, 5 патентів України на корисну модель, 18 матеріалів та тез доповідей на конференціях.

Перераховані публікації з достатньою повнотою відбивають наукові та практичні результати дисертації та у цілому відповідають вимогам до публікацій результатів дисертації на здобуття наукового ступеня доктора наук, які висуваються наказом Міністерства освіти і науки України від 29.09.2019 р. №1220. З праць, що їх опубліковано у співавторстві, у дисертації використано лише ті результати, які отримано здобувачем самостійно.

Зауваження щодо змісту дисертації та її оформлення

До основних недоліків дисертаційної роботи можна віднести такі.

1. У першому розділі під час аналізу чинного нормативно-правового забезпечення здобувач достатньо однобоко розглядає його сучасний стан. Як випливає з результатів аналізу основний акцент ним поставлено на розгляді національного законодавства, при цьому міжнародні практики, наприклад *NIST 800-30*, *BSI-Standard 100-3*, *ISO/FDIS 31000* та ін., залишилися поза увагою. Поряд з тим справедливо слід відмітити, що на с. 31 дисертації здобувач згадує імпелемнтований Україною міжнародний стандарт *ISO/IEC 27005*, але цього, на жаль, не достатньо.

2. Другий недолік також стосується якості опрацювання публікацій за темою дисертації. З одного боку їх достатньо багато в кількісному відношенні, з іншого – якісний бік не можна визнати задовільним. На наш погляд є некоректним аналіз підручників (с. 75 дисертації й далі), а також конспекту лекцій (с. 81 відповідно). При цьому здобувач у першому розділі не бере до уваги іноземні та вітчизняні монографії провідних вчених за даною тематикою, результати фундаментальних досліджень, викладені в дисертаціях, науково-дослідні та дослідно-конструкторські роботи тощо. Приведення б результатів таких досліджень сприяло б більш аргументованому підтвердженню актуальності обраної теми.

3. Не можна погодитися з досить вільним оперуванням та ототожненням здобувачем таких споріднених, але різних за суттю категорій як "інформаційна безпека" та *"безпека інформації"*. В першому випадку категорія *"інформаційна безпека"* на с. 92 уживається некоректно, оскільки в контексті чинної нормативно-правової бази вона стосується захищеності людини, суспільства та держави, а відповідно й використовуваних ними ІС ОКІ, від деструктивних інформаційних впливів, а саме впливів інформаційно-психологічного спрямування. В іншому випадку категорія *"безпека інформації"* (див. там само) не розглядається в контексті її захищеності від порушення базових властивостей, таких як конфіденційність, цілісність, доступність. Як наслідок подана у п. 2.1 модель загроз ІС ОКІ не набула строгого формалізованого вигляду.

Недолік стосовно уживаних категорій також має місце в частині, що стосується термінів *"оцінювання ризику"*, *"розрахунку ризику"* та *"обчислення ризику"*, що також не можна ототожнювати.

4. На наш погляд, в авторефераті на с. 11 та дисертації с. 123 вираз, що описує негативний вплив на стан енергетичної безпеки держави (регіону), до якого може призвести кібератака на ІС ОКІ слід зводити до єдиного способу подання або надавати йому додаткове обґрунтування.

5. Даний недолік випливає з попереднього. Не приведення фізичної розмірності збитку h дещо ускладнює сприйняття зв'язку між теорією та практикою. Наприклад, у третьому розділі під час визначення залежності наслідків знищення інформаційного активу від їх ймовірностей та величини ризику (с. 154 дисертації, с. 15 автореферату відповідно) здобувач оперує нормованою від 0 до 1 величиною такого показника, як наслідки. Далі ж за текстом, приводячи модельний приклад, розмірність даного показника вже варіює. В одному випадку від 0 до 200, в іншому – від 0 до 50 (с. 159, с. 160 дисертації відповідно), при цьому незрозуміло варіації чого саме має на увазі здобувач.

6. При поданні ризиків в евклідовому векторному просторі здобувач цілком справедливо зауважує, що у разі ортогональності векторів суб'єктивного та об'єктивного ризику скалярний їх добуток дорівнюватиме нулю. При цьому не пояснює, яким чином розрахувати векторний ризик за запропонованою моделлю, якщо ортогональність ненульових суб'єктивного та об'єктивного векторів ризику в 2-мріному евклідовому просторі матиме місце на практиці або ж косинус кута між згаданими векторами варіюватиме від 90 до 180 градусів.

7. У п'ятому розділі дисертації для обчислення суми ризиків в якості базових параметрів здобувач пропонує використовувати параметри, визначені на основі методу експертних оцінок. Але зважаючи на їх широкий спектр, залишилось відкритим питанням – який саме метод слід застосовувати та як вибір того чи іншого методу вплине на результати оцінювання ризиків ІС ОКІ?

8. Здобувач на с. 225–235 розкриває новий спосіб виявлення кібератак на ІС ОКІ. При цьому він безапеляційно (без числового підтвердження) відмічає, що запропонований спосіб фактично в три рази підвищує втрати противника на проникнення в систему. Як мінімум таке твердження потребує експериментального підтвердження, а також урахування того, що кількість захисних рубежів для кожної окремо взятої ІС має бути пропорційною до сумарного ризику. У всіх інших випадках це, очевидно, призведе до необґрунтованих фінансових витрат на створення системи захисту.

9. У дисертації в заключному розділі не знайшло відображення питання порівняння результатів оцінювання ризиків ІС ОКІ на основі розробленого *"Калькулятору ризиків"* з іншими відомими аналогами, наприклад такими, як *FAIR-U*, *Cybersecurityrisk Calculator, Cybersecurity Risk Calculator, Ризик-калькулятор* тощо, що доступні у відкритому доступі. Приведення б таких даних сприяло б більш аргументованому та якісному підтвердженні одержаних результатів.

10. На наше переконання експериментальні дослідження, результати яких розкриті в шостому розділі дисертації, повинні бути оформлені більш строго, як того вимагає теорія планування та оформлення експерименту. Додержання б таких вимог дозволило б встановити зв'язок між метою експерименту, його завданнями та одержаними результатами. При цьому слід відмітити, що ознаки планування експерименту та його результати дисертантом представлені в роботі, але не структуровані.

11. Зважаючи на вагомість одержаних результатів, в дисертації не знайшли місце практичні рекомендації, від яких робота тільки б виграла у поданні.

12. Приведені у додатку акти впровадження досить доказово підтверджують вклад здобувача в науку, а також практичну цінність одержаних результатів. Поряд з тим вважаємо приведення деяких актів недоречним.

Зазначені недоліки дещо впливають на якість подання дисертації, але їх наявність не знижує практичної, а тим паче наукової цінності одержаних здобувачем результатів.

Висновки

Отже, на основі критичного вивчення дисертації, автореферату дисертації та праць здобувача, опублікованих за темою дисертації, об'єктивно **встановлено:**

– дисертаційна робота Гончара С.Ф. відповідає вимогам Порядку присудження наукових ступенів, затвердженого постановою Кабінету Міністрів України від 24.07.2013 р. № 567 (із змінами);

– дисертаційна робота відповідає п. 1 паспорту спеціальності 05.13.21 – системи захисту інформації;

– зміст автореферату ідентичний основним положенням дисертації;

– результати наукових досліджень, за якими здобувач захистив кандидатську дисертацію, на захист докторської дисертації не виносяться;

– використання чужих наукових результатів без посилань на авторів у дисертації не виявлено, що свідчить про особистий внесок здобувача в науку;

– дисертація Гончара С. Ф. є завершеною кваліфікаційною науковою працею, що місить нові науково обґрунтовані результати проведених здобувачем досліджень, які вирішують конкретну науково-прикладну проблему, пов'язану з розробленням методології оцінювання ризиків ІС ОКІ. Дана науково-прикладна проблема має істотне значення для подальшого розвитку теорії захисту інформації і створення нових класів систем захисту інформації;

– автор дисертації, ГОНЧАР Сергій Феодосійович заслуговує на присудження наукового ступеня доктора технічних наук за спеціальністю 05.13.21 – системи захисту інформації.

Офіційний опонент –
начальник кафедри захисту інформації та кібербезпеки
Житомирського військового інституту імені С. П. Корольова

доктор технічних наук, професор Р. В. ГРИЩУК

"19" березня 2020 р.

Підпис професора Грищука Р. В. засвідчую.
Начальник відділу персоналу та стройового

О. В. КОВАЛЬЧУК