ЗАТВЕРДЖУЮ
Проректор з навчальної роботи
Національного технічного
університету України
"Київський політехнічний інститут
імені Ігоря Сікорського"
к.філос.н., проф.
Анатолій МЕЛЬНИЧЕНКО

"12" березня 2024 р.

ВИТЯГ

з протоколу № 3 від 6 березня 2024 р. розширеного засідання
кафедри інформаційної безпеки
Національного технічного університету України
"Київський політехнічний інститут імені Ігоря Сікорського"

БУЛИ ПРИСУТНІ:

- з кафедри інформаційної безпеки:

директор НН ФТІ, д.т.н. професор Новіков О. М., завідувач кафедри д.т.н. професор Ланде Д. В., д.т.н. професор Зубок В. Ю., к.т.н. доцент Стьопочкіна І. В., к.т.н. доцент Демчинський В. В., доцент, к.т.н. доцент Гальчинський Л. Ю., доцент, к.т.н. доцент Коломиець М. В., к.т.н. доцент Литвинова Т. В., доцент, к.т.н. Носок С. О., доцент, к.т.н. доцент Родіонов А. М., к.т.н. с.н.с доцент Смирнов С. А., старший викладач Наконечна Ю В., старший викладач, к.ф.-м.н. Рибак О. В., к.т.н. доцент Луценко В.М., к.т.н. доцент Прогонов Д.О., асистент Кіреєнко О.В., ст.викладач Степаненко В.М, к.т.н. доцент Репа Ф.М.;

- з кафедри математичного моделювання та аналізу даних:

заст. дир. ФТІ з наукової роботи, к.ф-м.н. доцент Терещенко І. М.;

- з кафедри математичних методів захисту інформації:

в.о. завідувача кафедри, к.т.н. доцент Яковлев С. В.;

Запрошені з інших організацій:
Київський столичний університет імені Бориса Грінченка, д.т.н., професор Коршун Н. В.

СЛУХАЛИ:

1. Повідомлення аспіранта кафедри інформаційної безпеки Полуциганової Вікторії Ігорівни за матеріалами дисертаційної роботи "Метод оцінки ризику на основі аналізу структури зв'язків загроз та

вразливостей у кіберсистемах", поданої на здобуття ступеня доктора філософії з галузі знань 12 – Інформаційні технології за спеціальністю 125 – Кібербезпека та захист інформації.

Освітньо-наукова програма Кібербезпека.

Тему дисертаційної роботи "Метод оцінки ризику на основі аналізу структури зв'язків загроз та вразливостей у кіберсистемах" затверджено на засіданні Вченої ради Навчально-наукового фізико-технічного інституту КПІ імені Ігоря Сікорського (протокол № 12/2018 від "28" листопада 2018 року) та перезатверджено на засіданні Вченої ради Навчально-наукового фізико-технічного інституту КПІ імені Ігоря Сікорського (протокол № 16 від "25" грудня 2023 року).

Науковим керівником затверджений к.ф.-м.н. с.н.с. Смирнов С. А.

2. Запитання до здобувача.

Запитання по темі дисертації ставили:

Д.т.н. професор Новіков О. М., д.т.н. професор Ланде Д. В., к.т.н. доцент Гальчинський Л. Ю., к.ф-м.н. доцент Терещенко І. М., к.ф.-м.н. Рибак О. В.

3. Виступи за обговореною роботою.

В обговоренні дисертації взяли участь:

Д.т.н. професор Новіков О. М., д.т.н. професор Ланде Д. В., д.т.н. професор Коршун Н. В., к.т.н. доцент Коломицев М. В.

УХВАЛИЛИ:

ПРИЙНЯТИ такий висновок про наукову новизну, теоретичне та практичне значення результатів дисертаційного дослідження:

1. Актуальність теми дослідження. Сьогодні аналіз ризиків внаслідок вразливостей має велике значення для оцінки безпеки системи. Такий підхід особливо важливий у кіберсистемах. Складний зв'язок між уразливими місцями визначається загрозами, які потенційно використовують їх наявність. Робота містить моделі та методи побудови, аналізу та класифікації загроз залежно від вразливостей, які в системі. На основі проведеного аналізу структури сумісності вразливостей запропоновано метод синтезу оцінки ризику. Такий підхід дозволяє краще зрозуміти зв'язки між уразливими місцями кіберсистем, а також ступінь небезпеки та впливу кожного з них окремо та разом.

Найпоширенішим припущенням є те, що всі вразливості є незалежними та реалізуються внаслідок або випадкових подій, або зловмисних намірів. У роботі запропоновано метод, який дозволяє моделювати вразливості складних систем в цілому, з урахуванням їх прихованих зв'язків. Методи Q-аналізу використано для дослідження структури системи взаємопов'язаних уразливостей, які виникають у процесі реалізації загроз. Наведено приклад

застосування методів Q-аналізу для синтезу оцінки ризику та запропоновано пояснення природи та впливу деяких потенційних загроз та їх комбінацій.

Оцінювання ризиків при реалізації загроз кіберінцидентів є основою для створення систем захисту кіберсистем. Запропонований метод включає урахування впливу структурних особливостей у взаємозалежності між вразливостями та загрозами та допомагає точніше оцінити рівень ризику та зрозуміти його природу та характер.

2. Зв'язок роботи з науковими програмами, планами, темами

Дисертаційна робота виконувалась у відповідності до наукової складової освітньо-наукової програми «Кібербезпека». Теоретичні та практичні результати застосовуються у навчальному процесі кафедри інформаційної безпеки «КПІ ім. Ігоря Сікорського» при підготовці та викладанні курсів «Рішення в умовах невизначеності та ризику», «Проблеми кібербезпеки критичної інфраструктури», «Математичні моделі кібербезпеки». Наукові дослідження виконувались здобувачем на кафедрі інформаційної безпеки КПІ ім. Ігоря Сікорського в рамках НДР «Підтримка прийняття рішень в умовах невизначеності та конкурентної взаємодії» (номер держреєстрації 0124U001957) під керівництвом доцента КПІ ім. Ігоря Сікорського, кандидата фізико-математичних наук, старшого наукового співробітника Смирнова С.А.

3. Наукова новизна отриманих результатів

У дисертації вперше одержані такі нові наукові результати:

– Вперше побудовано модель зв'язків загроз та вразливостей у кіберсистемі у вигляді симплеціального комплексу, яка представляє складну структуру їх взаємозалежностей, для класифікації загроз і вразливостей та для оцінювання потенційних втрат і ризиків;

– Вперше розроблено алгоритми аналізу симплекційного комплексу та його синтезу на основі повного набору структурних характеристик комплексу;

– Вперше розроблено метод класифікації загроз та вразливостей у складній системі з урахуванням характеристик власної розмірності підсистем, їх примикання та наслідування, що дозволяє надійніше оцінювати ризики в кіберсистемі в залежності від варіантів атак;

– Розроблено процедуру побудови байєсівської оцінки ризику з врахуванням структури вразливостей системи та складеної функції втрат.

4. Теоретичне та практичне значення результатів роботи

Отримані в дисертаційній роботі результати можуть бути застосовані в різних областях діяльності для розрахунку ризику в системах складної структури, в першу чергу в кіберсистемах, на основі аналізу взаємозв'язків між вразливостями та загрозами.

Наукові напрацювання дисертаційного дослідження використані під час підготовки матеріалів до засідання Ради національної безпеки і оборони

України з питання «Про стан справ у енергетичній сфері», рішення Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України, а також у процесі розроблення Загальних правил обміну інформацією про кіберінциденти, затверджених рішенням НКЦК. Теоретичні та практичні результати наукового дослідження використані для вдосконалення державної політики з питань національної безпеки у сфері забезпечення кібербезпеки, насамперед щодо підвищення рівня кіберзахисту інформаційно-комунікаційних систем об'єктів критичної інфраструктури, зокрема паливно-енергетичного сектору.

Теоретичні та практичні результати застосовуються у навчальному процесі кафедри інформаційної безпеки НТУУ «КПІ ім. Ігоря Сікорського» при підготовці та викладанні курсів «Рішення в умовах невизначеності та ризику», «Проблеми кібербезпеки критичної інфраструктури», «Математичні моделі кібербезпеки». Моделі та методи розроблені в дисертації використані в Науково-дослідні роботі «Підтримка прийняття рішень в умовах невизначеності та конкурентної взаємодії» державний реєстраційний номер 0124U001957, що підтверджує наукову та практичну цінність отриманих результатів дослідження.

5. Апробація/використання результатів дисертації

Наукові напрацювання дисертаційного дослідження використані під час підготовки матеріалів до засідання Ради національної безпеки і оборони України з питання «Про стан справ у енергетичній сфері», рішення Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України, а також у процесі розроблення Загальних правил обміну інформацією про кіберінциденти, затверджених рішенням НКЦК. Теоретичні та практичні результати наукового дослідження використані для вдосконалення державної політики з питань національної безпеки у сфері забезпечення кібербезпеки, насамперед щодо підвищення рівня кіберзахисту інформаційно-комунікаційних систем об'єктів критичної інфраструктури, зокрема паливно-енергетичного сектору.

Апробація матеріалів дисертаційного дослідження проведено на 8 науково-практичних конференціях.

6. Дотримання принципів академічної доброчесності

За результатами проведеної науково-технічної експертизи (експерт к.т.н. доцент Коломицев М. В.) дисертація Полуциганової Вікторії Ігорівни визнана оригінальною роботою, яка не містить елементів фальсифікації, компіляції, фабрикації, плагіату та запозичень.

7. Перелік публікацій за темою дисертації із зазначенням особистого внеску здобувача.

За результатами досліджень опубліковано 12 наукових публікацій, у тому числі:

- 3 статті у наукових фахових виданнях України за спеціальністю,

- 8 тез виступів на наукових конференціях;
- 1 стаття, що додатково відображають результати дисертації.

1. Polutsyganova V., Smirnov S. The inverse problem of Q-analysis of complex systems structure in cyber security. Theoretical and applied cybersecurity. 2023. Vol. 4, no. 1. P. 61 – 68. URL: https://doi.org/10.20535/tacs.2664-29132022.1.274123 (date of access: 10.11.2023).

У роботі здобувачем наведено розроблений алгоритм відновлення або синтезу симплеціальних комплексів з елементарного набору симплексів за допомогою локальних бінарних карт і структурного дерева. Цей алгоритм використовується для зменшення обсягу даних, які необхідно зберігати для характеристики системи, якщо комплекс описує велику складну систему таку, як система кібербезпеки.

2. Polutsyhanova V. I. System construction of cybersecurity vulnerabilities with Q-analysis. *Theoretical and applied cybersecurity*. 2023. Vol. 5, no. 1. P. 52-55. URL: https://doi.org/10.20535/tacs.2664-29132023.1.285430 (date of access: 08.11.2023).

У роботі здобувачем запропоновано метод, який дозволяє будувати моделі складних систем на основі їх уразливостей з урахуванням прихованих зв'язків. При цьому, наведено можливості Q-аналізу для дослідження структури системи взаємопов'язаних уразливостей, які виникають в процесі реалізації проекту. Наведено приклад застосування методів Q-аналізу та запропоновано пояснення природного стану системи, а також впливу деяких потенційних загроз та їх комбінацій.

3. Polutsyhanova V. I. Vulnerability classification using Q-analysis. *Theoretical and applied cybersecurity*. 2023. Vol. 5, no. 2. P. 56–61. URL: https://doi.org/10.20535/tacs.2664-29132023.2.285431

У роботі здобувачем представлено метод розрахунку оцінки ризиків для систем складної структури та наведено приклад побудови, аналізу та класифікації вразливостей залежно від загроз, які вони породжують. Такий підхід висвітлює зв'язки та сумісну реалізацію між уразливими місцями, а також ступінь впливу кожної з них на рівень загроз.

4. Медведенко (Полуциганова) В. І., Смирнов С. А. Використання q-аналізу для дослідження зв'язків у банківських системах. *XV Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики»*: Всеукр. науково-практ. конференція студентів, аспірантів та молодих вчен., м. Київ, 25–27 трав. 2017 р. Київ, 2017. С. 44–46.

У роботі здобувачем наведено результати досліджень взаємозв'язку уразливостей від загроз, які вони породжують, для інформаційної системи банківських установ за допомогою Q-аналізу. Проведено пошук зв'язків вищих порядків у досліджуваній системі та надані рекомендації для практичного застосування результатів у процесах прийняття рішень для посилення інформаційної безпеки в банківських установах.

5. Медведенко (Полуциганова) В. І., Смирнов С. А. Використання алгоритмів q-аналізу на прикладі банківської системи. *XVI Всеукраїнська*

науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики»: Всеукр. науково-практ. конференція студентів, аспірантів та молодих вчен., м. Київ, 26–27 квіт. 2018 р. Київ, 2018. С. 33–36.

У роботі здобувачем представлено розроблені алгоритми Q-аналізу для систем з великою кількістю елементів та описано їх застосування на прикладі інформаційної системи банківської установи. Проведено аналіз результатів роботи алгоритмів, надані рекомендації для їх використання в процесах прийняття рішень щодо посилення інформаційної безпеки в банківських установах.

6. Polutsyhanova V. The inverse problem of q-analysis. *XVIII Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики»:* Всеукр. науково-практ. конференція студентів, аспірантів та молодих вчен., м. Київ, 12–13 трав. 2020 р. С. 113–115.

У роботі здобувачем запропоновано метод відновлення симплеціальних комплексів з елементарного симплексу за допомогою локальних карт і структурного дерева. Цей метод зменшує обсяг даних, що зберігаються, і покращує процес управління, якщо комплекс описує складну систему.

7. Полуциганова В. І., Смирнов С. А. The inverse problem of Q-analysis of complex systems structure. *Інформаційні технології та безпека. Матеріали XXI міжнародної науково-практичної конференції. Випуск 22*, м. Київ, 2021. С. 48–51.

У роботі здобувачем висвітлено метод оберненої задачі Q-аналізу, тобто відновлення комплексу за допомогою локальних карт і структурного дерева. Представлено загальний приклад практичного використання.

8. Полуциганова В. І., Смирнов С. А. Оцінювання ризиків складних систем з використання методів Q-аналізу. *Інформаційні технології та безпека матеріали XXII міжнародної науково-практичної конференції*, м. Київ, 2022. С. 51–52.

У роботі здобувачем наведено розроблений метод оцінювання ризиків для структурно та функціонально складних систем, в яких уразливості, а як наслідок, і збитки від них, можуть реалізовуватись одночасно.

9. Полуциганова В. І., Смирнов С. А. Structure of vulnerability in complex systems and risk assessment. МІЖНАРОДНА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ «Виклики і загрози для критичної інфраструктури» 21-22 березня 2023 р. м. Київ, Україна. С. 334-335.

У роботі здобувачем представлено розроблену методику оцінки ризиків для структурно-функціональної складності інформаційних систем, в якій уразливості можуть реалізовуватися разом. За допомогою Q-аналізу описані структурні залежності між уразливими місцями, що дозволяє отримати більш точну оцінку збитків.

10. Полуциганова В. І., Смирнов С. А. Оцінка ризиків в кібербезпеці за допомогою Q-аналізу. *XXI Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми*

фізики, математики та інформатики»: Всеукр. науково-практ. конференція студентів, аспірантів та молодих вчен., м. Київ, 12–13 трав. 2023 р. Київ, 2017. С. 172–173.

У роботі здобувачем розглянуто модель оцінки кібернетичного ризику з урахуванням зв'язків високих порядків та моделювання системи за допомогою Q-аналізу.

11. Polutsyhanova V. I., Smirnov S. A. Assessing cybersecurity risk with Q-analysis. *Всеукраїнська науково-практична конференція «Theoretical and Applied Cybersecurity» (TACS-2023)*, Kyiv, 26 May 2023. P. 57–60.

У роботі здобувачем представлено метод удосконалення оцінювання кібернетичного ризику з урахуванням зв'язків між уразливостями та загрозами на основі моделювання кіберсистеми за допомогою Q-аналізу.

12. Полуциганова В. І., Смирнов С. А. Методологія побудови основних метрик q-аналізу та їх застосування. *Системні дослідження та інформаційні технології.* 2019. № 3. С. 76 – 88. URL: https://doi.org/10.20535/srit.2308-8893.2019.3.07 (date of access: 10.11.2023).

У роботі здобувачем впроваджено такі поняття, як структурне дерево, локальні карти та процедура наслідування, які дозволяють роз'яснити сенс метрик системи, отриманих за допомогою Q-аналізу. На цій основі розроблено алгоритми для визначення основних метрик системи, які застосовано до банківської системи.

Якість та кількість публікацій відповідають "Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії», затвердженого Постановою Кабінету Міністрів України від 12 січня 2022 р. № 44".

ВВАЖАТИ, що дисертаційна робота Полуциганової В. І. "Метод оцінки ризику на основі аналізу структури зв'язків загроз та вразливостей у кіберсистемах", що подана на здобуття ступеня доктора філософії з галузі знань 12 – Інформаційні технології за спеціальністю 125 – Кібербезпека та захист інформації за своїм науковим рівнем, новизною отриманих результатів, теоретичною та практичною цінністю, змістом та оформленням повністю відповідає вимогам, що пред'являють до дисертацій на здобуття ступеня доктора філософії та відповідає напрямку наукового дослідження освітньо-наукової програми КПІ ім. Ігоря Сікорського Кібербезпека зі спеціальності 125 – Кібербезпека та захист інформації.

РЕКОМЕНДУВАТИ:

1. Дисертаційну роботу "Метод оцінки ризику на основі аналізу структури зв'язків загроз та вразливостей у кіберсистемах", подану Полуциганową Вікторією Ігорівною на здобуття наукового ступеня доктора філософії, до захисту у разовій спеціалізованій вченій раді.

2. Вченій раді КПІ ім. Ігоря Сікорського утворити разову спеціалізовану вчену раду у складі:

Голова:

Д.т.н., професор, директор НН ФТІ КПІ ім. Ігоря Сікорського **Новіков Олексій Миколайович**;

Члени:

Рецензенти:

Д.т.н., професор, завідувач кафедри інформаційної безпеки КПІ ім. Ігоря Сікорського **Ланде Дмитро Володимирович**;

К.т.н. доцент, доцент Спеціальної кафедри № 5 ІСЗЗІ КПІ ім. Ігоря Сікорського **Цуркан Василь Васильович**;

Офіційні опоненти:

Д.т.н. професор, професор кафедри інформаційної та кібернетичної безпеки ім. професора Володимира Бурячка Київського столичного університету імені Бориса Грінченка **Коршун Наталія Володимирівна**;

Д.т.н. професор, професор кафедри кібербезпеки та захисту інформації Київського національного університету імені Тараса Шевченка **Толюпа Сергій Васильович**

Головуючий на засіданні
д.т.н., професор, завідувач
кафедри інформаційної безпеки
КПІ ім. Ігоря Сікорського _____ Дмитро ЛАНДЕ

Вчений секретар
кафедри інформаційної
безпеки к.т.н., доцент _____ Володимир ДЕМЧИНСЬКИЙ