Облікова картка дисертації

I. Загальні відомості

Державний обліковий номер: 0824U003460

Особливі позначки: відкрита

Дата реєстрації: 04-12-2024

Статус: Захищена

Реквізити наказу МОН / наказу закладу:

II. Відомості про здобувача

Власне Прізвище Ім'я По-батькові:

1. Іосіфов Євген Анатолійович

2. Ievgen Iosifov

Кваліфікація:

Ідентифікатор ORCID ID: Не застосовується

Вид дисертації: доктор філософії

Аспірантура/Докторантура: так

Шифр наукової спеціальності: 125

Назва наукової спеціальності: Кібербезпека та захист інформації

Галузь / галузі знань: інформаційні технології

Освітньо-наукова програма зі спеціальності: «Інформаційна безпека держави»

Дата захисту: 23-01-2025

Спеціальність за освітою: "Системи управління і автоматики"

Місце роботи здобувача:

Код за ЄДРПОУ:

Місцезнаходження:

Форма власності:

Сфера управління:

Ідентифікатор ROR: Не застосовується

III. Відомості про організацію, де відбувся захист

Шифр спеціалізованої вченої ради (разової спеціалізованої вченої ради): PhD 7348

Повне найменування юридичної особи: Київський столичний університет імені Бориса Грінченка

Код за ЄДРПОУ: 02136554

Місцезнаходження: вул. Бульварно-Кудрявська, 18/2, Київ, 04053, Україна

Форма власності: Державна

Сфера управління: Департамент освіти і науки, молоді та спорту виконавчого органу Київської міської ради (Київської міської державної адміністрації)

Ідентифікатор ROR:

IV. Відомості про підприємство, установу, організацію, в якій було виконано дисертацію

Повне найменування юридичної особи: Київський столичний університет імені Бориса Грінченка

Код за ЄДРПОУ: 02136554

Місцезнаходження: вул. Бульварно-Кудрявська, 18/2, Київ, 04053, Україна

Форма власності: Державна

Сфера управління: Департамент освіти і науки, молоді та спорту виконавчого органу Київської міської ради (Київської міської державної адміністрації)

Ідентифікатор ROR:

V. Відомості про дисертацію

Мова дисертації: Українська

Коди тематичних рубрик: 20.56, 20.56.02

Тема дисертації:

1. Методи та засоби забезпечення безпечного розпізнавання та параметризації результатів обробки голосової інформації

2. Methods and Means of Ensuring Secure Recognition and Parameterization of Speech Information Processing Results.

Реферат:

1. Дисертаційна робота присвячена вирішенню актуального наукового завдання, сутність якого полягає в підвищенні ефективності застосування безпечного розпізнавання та параметризації результатів обробки голосової інформації завдяки комбінуванню підходів розпізнавання природної мови та голосової інформації для побудови систем голосової автентифікації, виявлення намірів та визначення емоційного стану суб'єктів в інформаційно-комунікаційних системах (ІКС), а також впровадженню заходів управління кібербезпекою на державних підприємствах та в приватних організаціях. Методологія обробки голосової інформації є потужним інструментом, який має значний вплив на безпеку держави та роботу комерційних організацій через автоматизацію процесів моніторингу електронних комунікацій та аудіоархівів, на основі розпізнавання

в реальному часі мови, емоцій та намірів, чому сприяють декілька факторів, які змушують звернути увагу на методології, на актуальність їх удосконалення, а саме: 1. Зміна ландшафту кіберзагроз. Із появою генеративних моделей та збільшенням обчислювальних можливостей традиційні моделі безпеки, які покладаються на високо структуровані дані перестають адекватно виявляти та реагувати на підроблені аудіодані. Тому актуальними стають задачі по виявленню, реєстрації та реагуванню на нові виклики, а також швидкий розвиток даної галузі. 2. Перехід голосової інформації із телефонних розмов в телеконференції. При використанні традиційних телефонних переговорів до їхнього вмісту потенційно мав доступ оператор зв'язку та державні органи. Тому тривалість та зміст розмов були меншими та піддавалися самоцензуруванню. Із переходом до телеконференцій вартість розмов зменшилася, а розповсюдження методів наскрізного шифрування створило уяву безпечності середовища, то абоненти стали вести більш відверті та довгі розмови, що стало особливо актуальним в епоху віддаленої роботи. Також через збільшення об'єму голосової інформації необхідно швидше зі сторони держави опрацьовувати її для вчасного виявлення, до прикладу, терористичних загроз, а зі сторони приватних підприємств – для виявлення витоку конфіденційних даних. 3. Порушення даних і зовнішні загрози. Діпфейки та введення спотворень в оригінальні аудіодані абонента створюють загрози для перенасичення інформаційної системи запитами. Виявлення та протидія фроду при аналізі намірів, в тому числі, генерації великої кількості фейкових намірів, призводять до перенавантаження зовнішніх пов'язаних системи та обмеженню ресурсів реагування, що створює загрозу недоотримання уваги легітимними суб'єктами. 4. Розширення ролі хмарних служб. Оскільки підприємства та організації все частіше використовують хмарні послуги для зберігання конфіденційних аудіоданих, то виникає потреба в додатковій обробці, в тому числі, деперсоналізації та видалення чутливих даних із аудіопотоку. 5. Вимоги відповідності. До персональних даних абонентів висуваються вимоги щодо їхньої конфіденційності в межах держаних стандартів (GDPR, HIPAA), комерційних (PCI DSS) та/або етичних обмежень. В свою чергу, аудіодані є важким видом інформації для структурованого пошуку та аналізу стосовно висунутих вимог та обмежень. 6. Безперервний моніторинг і адаптивна безпека. Обробка голосових даних може проводитися як архівних, так і в режимі реального часу, але вузьким місцем ІКС є потокова обробка даних. Тому реагування на інциденти може проводитися у два способи: невідкладні дії та розслідування інцидентів, але обидва підходи мають свій набір невирішених завдань. 7. Реагування на інциденти та виявлення загроз. Системи розпізнавання голосової інформації не мають в своєму складі механізмів щодо реагування на інциденти, тому повинні сигналізувати іншим системам в режимі реального часу. Інтеграція із зовнішніми ІКС для забезпеченні безпеки має обмеження на швидкодію та затримки на час обробки запитів, але все одно зменшує потенційну шкоду. Також слід зазначити, що актуальність реагування різко зменшується з плином часу.

2. The dissertation is devoted to solving an urgent scientific problem, the essence of which is to increase the efficiency of applying secure recognition and parameterization of voice information processing results by combining natural language and voice information recognition approaches to build voice authentication systems, detect intentions and determine the emotional state of subjects in information and communication systems, as well as implement cybersecurity management measures at state-owned enterprises and in private. The methodology of voice information processing is a powerful tool that has a significant impact on the security of the state and the work of commercial organizations through the automation of monitoring processes of electronic communications and audio archives, based on real-time recognition of speech, emotions, and intentions, which is facilitated by several factors that make us pay attention to the methodology and the relevance of their improvement: 1. The changing landscape of cyber threats. With the advent of generative models and increased computing power, traditional security models that rely on highly structured data no longer adequately detect and respond to fake audio data. Therefore, the tasks of detecting, registering, and responding to new challenges, as well as the rapid development of this industry, are becoming urgent. 2. Transition of voice information from telephone conversations to teleconferences. When traditional telephone conversations were used, the telecom operator and government agencies potentially had access to their content. Therefore, the duration and content of conversations were shorter and subject to self-censorship. With the transition to teleconferencing, the cost of

calls decreased, and the proliferation of end-to-end encryption methods created a perception of security, subscribers began to have more open and longer conversations, which became especially relevant in the era of remote work. Also, due to the increase in the volume of voice information, the state must process it faster to detect, for example, terrorist threats, and for private enterprises to detect leaks of confidential data. 3. Data breaches and external threats. Deepfakes and the introduction of distortions in the original audio data of a subscriber pose a threat of oversaturation of the information system with requests. Detecting and counteracting fraud in intent analysis, including the generation of a large number of fake intentions, leads to the overloading of externally connected systems and limiting response resources, which poses a threat of not receiving attention from legitimate actors. 4. Expanding the role of cloud services. As businesses and organizations increasingly use cloud services to store confidential audio data, there is a need for additional processing, including depersonalization and removal of sensitive data from the audio stream. 5. Compliance requirements. The personal data of subscribers is subject to confidentiality requirements within the framework of governmental standards (GDPR, HIPAA), commercial (PCI DSS), and/or ethical restrictions. Audio data, in turn, is a difficult type of information to search and analyze in a structured way due to the requirements and restrictions. 6. Continuous monitoring and adaptive security. Voice data can be processed both archived and in real-time, but the bottleneck of information and communication systems is streaming data processing. Therefore, incident response can be carried out in two ways: immediate actions and incident investigation, but both approaches have their own set of unresolved issues. 7. Incident response and threat detection. Voice recognition systems do not have incident response mechanisms, so they must signal other systems in real time. Integration with external information and communication systems for security has limitations on performance and delays in processing requests, but still reduces potential damage. It should also be noted that the relevance of the response decreases dramatically over time.

Державний реєстраційний номер ДіР:

Пріоритетний напрям розвитку науки і техніки: Фундаментальні наукові дослідження з найбільш важливих проблем розвитку науково-технічного, соціально-економічного, суспільно-політичного, людського потенціалу для забезпечення конкурентоспроможності України у світі та сталого розвитку суспільства і держави

Стратегічний пріоритетний напрям інноваційної діяльності: Освоєння нових технологій транспортування енергії, впровадження енергоефективних, ресурсозберігаючих технологій, освоєння альтернативних джерел енергії

Підсумки дослідження: Теоретичне узагальнення і вирішення важливої наукової проблеми

Публікації:

- Іосіфов, Є. (2023). Комплексний метод по автоматичному розпізнаванню природньої мови та емоційного стану. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3(19), 146–164. https://doi.org/10.28925/2663-4023.2023.19.146164.
- Марценюк, М., Козачок, В., Богданов, О., Іосіфов, Є., & Бржевська, З. (2023). Аналіз методів виявлення дезінформації в соціальних мережах за допомогою машинного навчання. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(22), 148–155. https://doi.org/10.28925/2663-4023.2023.22.148155.
- Іосіфов, Є., & Соколов, В. (2024). Методи аналізу природної мови та застосування нейронних мереж в кібербезпеці. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 4(24), 398–414. https://doi.org/10.28925/2663-4023.2024.24.398414.
- Іосіфов, Є., & Соколов, В. (2024). Порівняльний аналіз методів, технологій, сервісів та платформ для розпізнавання голосової інформації в системах забезпечення інформаційної безпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 1(25), 468–486.

https://doi.org/10.28925/2663-4023.2024.25.468486.

Наукова (науково-технічна) продукція:

Соціально-економічна спрямованість:

Охоронні документи на ОПІВ:

Впровадження результатів дисертації: Впроваджено

Зв'язок з науковими темами: 0122U200483

VI. Відомості про наукового керівника/керівників (консультанта)

Власне Прізвище Ім'я По-батькові:

1. Соколов Володимир Юрійович
2. Volodymyr Y. Sokolov

Кваліфікація: к. т. н., доцент, 05.13.06

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Київський столичний університет імені Бориса Грінченка

Код за ЄДРПОУ: 02136554

Місцезнаходження: вул. Бульварно-Кудрявська, 18/2, Київ, 04053, Україна

Форма власності: Державна

Сфера управління: Департамент освіти і науки, молоді та спорту виконавчого органу Київської міської ради (Київської міської державної адміністрації)

Ідентифікатор ROR:

VII. Відомості про офіційних опонентів та рецензентів

Офіційні опоненти

Власне Прізвище Ім'я По-батькові:

1. Шевченко Віктор Леонідович
2. Victor L. Shevchenko

Кваліфікація: д. т. н., професор, 01.05.02

Ідентифікатор ORCID ID: 0000-0002-9457-7454

Додаткова інформація:

Повне найменування юридичної особи: Інститут програмних систем Національної академії наук України

Код за ЄДРПОУ: 05540149

Місцезнаходження: проспект Академіка Глушкова, буд. 40, корп. 5, Київ, 03187, Україна

Форма власності: Державна

Сфера управління: Національна академія наук України

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Назаркевич Марія Андріївна

2. Mariia A. Nazarkevych

Кваліфікація: д. т. н., професор, 21.05.01

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Національний університет "Львівська політехніка"

Код за ЄДРПОУ: 02071010

Місцезнаходження: вул. Степана Бандери, буд. 12, Львів, 79013, Україна

Форма власності: Державна

Сфера управління: Міністерство освіти і науки України

Ідентифікатор ROR:

Рецензенти

Власне Прізвище Ім'я По-батькові:

1. Крючкова Лариса Петрівна

2. Larysa P. Kruchkova

Кваліфікація: к.т.н., доц., 05.12.02

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Київський столичний університет імені Бориса Грінченка

Код за ЄДРПОУ: 45307965

Місцезнаходження: вул. Бульварно-Кудрявська, 18/2, Київ, 04053, Україна

Форма власності: Комунальна

Сфера управління: Держадміністрація

Ідентифікатор ROR:

Власне Прізвище Ім'я По-батькові:

1. Киричок Роман Васильович

2. Roman V. Kyrychok

Кваліфікація: д.філософ, доц., 125

Ідентифікатор ORCID ID: Не застосовується

Додаткова інформація:

Повне найменування юридичної особи: Київський столичний університет імені Бориса Грінченка

Код за ЄДРПОУ: 02136554

Місцезнаходження: вул. Бульварно-Кудрявська, 18/2, Київ, 04053, Україна

Форма власності: Державна

Сфера управління: Департамент освіти і науки, молоді та спорту виконавчого органу Київської міської ради (Київської міської державної адміністрації)

Ідентифікатор ROR:

VIII. Заключні відомості

Власне Прізвище Ім'я По-батькові голови ради	Коршун Наталія Володимирівна
Власне Прізвище Ім'я По-батькові головуючого на засіданні	Коршун Наталія Володимирівна
Відповідальний за підготовку облікових документів	Сало Ганна Вікторівна
Реєстратор	УкрІНТЕІ
Керівник відділу УкрІНТЕІ, що є відповідальним за реєстрацію наукової діяльності	Юрченко Тетяна Анатоліївна