П Р О Г Р А М А

вступного іспиту зі спеціальності

F5 кібербезпека та захист інформації

для здобувачів вищої освіти третього (освітньо-наукового) рівня

Вступне слово

Програма складена з урахуванням програми рівня вищої освіти магістра зі спеціальності F5 кібербезпека та захист інформації. Вона містить п'ять розділів, розроблені питання базуються на освітніх компонентах ОП бакалавра та ОП магістра за спеціальністю F5 кібербезпека та захист інформації, спрямовані на виявлення знань та умінь здобувачів вищої освіти третього (освітньо-наукового) рівня зі спеціальності F5 кібербезпека та захист інформації.

В програмі відображені наступні розділи теоретичних та практичних основ кібербезпеки та захисту інформації:

1. Методи та засоби захисту інформації.
2. Захист каналів зв’язку. Методи та засоби контролю та спецвимірювань.
3. Методи та засоби стеганографії та криптографічного захисту інформації.
4. Організаційно-правове забезпечення, аудит та менеджмент інформаційної безпеки.
5. Кібербезпека систем та мереж.

1. Методи та засоби захисту інформації

1. Форми представлення інформації та їх характеристика.
2. Класифікація і характеристика методів і засобів захисту інформації від витоку технічними каналами.
3. Організаційні та технічні заходи захисту інформації від витоку через технічні канали витоку інформації.
4. Виявлення портативних електронних пристроїв перехоплення інформації: спеціальні обстеження, спеціальна перевірка.
5. Пасивні засоби захисту інформації: Екранування технічних засобів.
6. Пасивні засоби захисту інформації: Заземлення технічних засобів.
7. Пасивні засоби захисту інформації: фільтрація інформаційних сигналів.
8. Пасивні засоби захисту інформації: звукоізоляція.
9. Активні технічні заходи захисту інформації: Просторове та лінійне високочастотне зашумлення.
10. Акустичне та віброакустичне маскування. Виявлення та придушення диктофонів і акустичних закладок.
11. Пасивні та активні методи захисту телефонних ліній.
12. Форми представлення інформації та особливості їх захисту.
13. Технічні канали витоку інформації.
14. Принцип дії лазерного мікрофона.

15. Методи протидії прослуховуванню.
16. Виявлення та придушення закладних пристроїв.
17. Нелінійні локатори, принцип дії та затосування.
18. Комплексні системи технічного захисту інформації.
19. Периметральні системи охорони об’єктів. Системи відео нагляду та контролю доступу.
20. Біометричні системи аутентифікації. Охоронні системи.

2. Захист каналів зв’язку. Методи та засоби контролю та спецвимірювань

1. Канали зв’язку і їх характеристики.
2. Методи захисту інформації в провідних каналах зв’язку.
3. Аналого-цифрове і цифро-аналогове перетворення в цифрових системах зв’язку. Дискретизація сигналів**.**
4. Амплітудна модуляція з подавленою несучою. Детектування модульованих сигналів з подавленою несучою.
5. Частотна і фазова модуляція.
6. Види імпульсної модуляції. Амплітудно-імпульсна та кодо-імпульсна модуляція.
7. Множинний доступ з частотним розділенням**.**
8. Множинний доступ з часовим розділенням**.**
9. Множинний доступ з частотно-часовим розділенням.
10. Множинний доступ з кодовим розділенням.
11. Аспекти застосування принципів системного підходу до захисту інформації в каналах, мережах, системах зв’язку.
12. Методи захисту інформації в безпровідних каналах зв’язку.
13. Методи захисту мовної інформації в каналі зв’язку: накладання захисного шуму, частотні перетворення, перетворення в код з шифруванням.
14. Захист мовної інформації в каналі зв’язку: перетворення з інверсією спектру і статичними перестановками спектральних компонент мовного сигналу.
15. Захист мовної інформації: перетворення з часовими або частотними перестановками (скремблюванням).
16. Похибки вимірювань фізичних величин.
17. Радіоприймальні вимірювальні прилади загального призначення. SDR приймачі.

3. Методи та засоби стеганографії та криптографічного захисту інформації

1. Вбудова повідомлень у незначущі елементи контейнера.
2. Математична модель стегосистеми та стеганографічні протоколи.
3. Атаки на стегосистеми.
4. Пропускна здатність каналів передавання прихованої інформації.
5. Приховування даних у просторовій області зображень. Методи приховування в найменш значущому біті даних, блокове приховування, метод квантування, метод "хреста".
6. Приховування даних у відеопослідодовностях з використанням стандарту

MPEG. Методи вбудовування інформації на рівні коефіцієнтів
7. Методи вбудовування інформації на рівні бітової площини
8. Методи вбудовування інформації в текстових файлах.
9. Класичні алгоритми криптографії. Алгоритми заміни та перестановки.
10. Класичні алгоритми криптоаналізу. Частотний крипто аналіз.
11. Сучасні алгоритми симетричного шифрування. Стандарти AES.
12. Основні обчислювальні алгоритми симетричних криптосистем. Потокові шифри. Блочні шифри. Мережа Фейстеля.
13. Основні алгоритми крипто аналізу симетричних шифрів. Засоби симетричної криптографії.
14. Концепція відкритого ключа. Менеджмент криптографічних ключів. Центри сертифікації відкритих ключів. Сертифікати відкритих ключів. Стандарт X509.
15. Асиметрична система RSA. Основні алгоритми і засоби реалізації.
16. Основні криптографічні протоколи і засоби їх реалізації.
17. Електронний цифровий підпис: принцип дії, основні властивості. Види ЕЦП.
18. Генератори випадкових і псевдовипадкових чисел. Апаратні генератори випадкових чисел. Генератори псевдовипадкових чисел на основі алгоритмів. Статистичні тести NIST STS.
19. Хеш-функції, їх властивості, застосування. Криптографічно стійкі хеш-функції. Приклади хеш-функцій.
20. Кодування інформації, види кодування, відмінність від шифрування.

4. Організаційно-правове забезпечення, аудит та менеджмент інформаційної безпеки

1. Державна таємниця. Види інформації, що відноситься до державної таємниці.Грифи та терміни секретності
2. Адміністративний рівень інформаційної безпеки. Політика безпеки.
3. Ризики інформаційної та кібер безпеки. Оцінювання ризику. Процес управління ризиками.
4. Процедурний рівень інформаційної безпеки та його класи заходів.
5. Інформація з обмеженим доступом (типи, порядок віднесення, інформація, що не може бути віднесена до ІзОД)
6. Організаційні заходи захисту інформації від витоку через ТКВІ.
7. Міжнародні стандарти аудиту інформаційних система та систем управління інформаційною безпекою.
8. Державні та міжнародні стандарти захисту персональних даних.
9. Базові та цільові профілі кіберзахисту. Впровадження стандарту NIST CSF.
10. Процес та план оброблення ризиків. Методи управління ризиками. Поняття залишкового та прийнятного ризику.
11. Поняття загрози, вразливості, інцеденту та впливу. Ідентифікація активів. Цінність інформації та активів.
12. Процес ідентифікації, аутентифікації та авторизації в інформаційних системах. Типи управління доступом. Аналіз сучасних моделей доступу.
13. Державні вимоги до кіберзахисту об’єктів критичної інфраструктури. Базові

вимоги.

14. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу

5. Кібербезпека систем та мереж

1. Принципи захисту програмного забезпечення
2. Життєвий цикл програмного забезпечення
3. Види шкідливого програмного забезпечення
4. Методи розповсюдження шкідливого програмного забезпечення
5. Засоби захисту від шкідливого програмного забезпечення
6. Сканери вразливості інформаційних систем
7. Системи виявлення та запобігання вторгненням. Основні принципи побудови і функціонування.
8. Міжмережеві екрани. Демілітаризована зона.
9. Технологія VPN
10. Основні застосування проксі-серверів
11. Види атак на комп’ютерні мережі і системи, захист від них.
12. Захищені Інтернет-протоколи. Принципи функціонування.
13. Протоколи захисту даних на сеансовому рівні.
14. Протоколи автентифікації та управління доступом у комп’ютерних мережах (RADIUS, Kerberos).
15. Принцип єдиного входу в комп’ютерних системах
16. Забезпечення безпеки в мережах Bluetooth
17. Забезпечення безпеки в мережах Wi-Fi
18. Програмні рішення для централізованого моніторингу, аналізу та управління подіями інформаційної безпеки в IT-інфраструктурі організації.
19. Технології відновлення інформаційної системи після збоїв
20. Поняття та класифікація інцидентів інформаційної безпеки
21. Еталонна модель OSI. Рівні еталонної моделі OSI та їх функції. Мережева модель TCP/IP.
22. Сегментація даних відповідно до протоколів транспортного рівня. Ідентифікація процесів. Поняття портів та сокетів. Безпека на рівні портів.
23. Метод захисту zero trust network access.
24. Технологія VLAN, як засіб безпеки локальної мережі.
25. Системи захисту в мережі Internet. Проблеми безпеки корпоративних інформаційних систем. Типи мережевих атак.
26. Принципи та стандарти в основі побудови ІКС з урахуванням вимог кібербезпеки
27. Важливість багаторівневого захисту (фізичний, мережевий, прикладний рівні)
28. Використання сучасних технологій: SIEM, IDS/IPS, Zero Trust, MFA, криптографії в інформаційно-комунікаційних системах
29. Типові загрози для хмарного середовища (витік або втрата даних, атаки через уразливі API, спуфінг, відмова в обслуговуванні)
30. Порівняння ризиків у хмарній архітектурі порівняно із традиційною (on-

premise);

31. Ключові принципи кіберзахисту в хмарі: (шифрування даних, контроль доступу, багатофакторна автентифікація, аудит подій, сегментація)
32. Моделі розподілу відповідальності між постачальником хмарних послуг та споживачем (Shared Responsibility Model);
33. Роль сертифікацій і стандартів (ISO/IEC 27017, ISO/IEC 27018, SOC 2, CSA STAR) у забезпеченні довіри до хмарних провайдерів

Форми контролю та критерії оцінювання

Організування та проведення вступних випробувань до аспірантури здійснюється відповідно до Правил прийому до аспірантури Національного університету "Львівська політехніка" у відповідному році.

Вступний іспит зі спеціальності F5 кібербезпека та захист інформації проводиться у письмово-усній формі згідно з окремим графіком, який затверджується Ректором Університету та оприлюднюється на інформаційному стенді відділу докторантури та аспірантури й офіційному веб-сайті Університету не пізніше, ніж за 3 дні до початку прийому документів.

Екзаменаційні білети вступного іспиту зі спеціальності F5 кібербезпека та захист інформації формуються в обсязі програми рівня вищої освіти магістра зі спеціальності F5 кібербезпека та захист інформації та затверджуються на засіданні Вченої ради Навчально-наукового інституту ІКТА.

Результати вступного іспиту зі спеціальності оцінюються за 100-бальною шкалою.

Екзаменаційний білет вступного іспиту до аспірантури зі спеціальності F5 кібербезпека та захист інформації містить:

- письмову компоненту з п'яти питань (1-2 питання з кожного розділу, кожне із п'яти питань екзаменаційного білета оцінюється максимально в 20 балів, максимальна сумарна кількість балів – 100 балів);

Критерії оцінювання кожного питання вступного іспиту зі спеціальності F5 кібербезпека та захист інформації є такими:

Оцінка "відмінно" (18-20 балів): вступник в аспірантуру бездоганно засвоїв теоретичний матеріал щодо змісту питання; самостійно, грамотно і послідовно з вичерпною повнотою відповів на питання; демонструє глибокі та всебічні знання, логічно будує відповідь; висловлює своє ставлення до тих чи інших проблем; вміє встановлювати причинно-наслідкові зв'язки, логічно та обґрунтовано будувати висновки.

Оцінка "добре" (14-17 балів): вступник в аспірантуру добре засвоїв теоретичний матеріал щодо змісту питання, аргументовано викладає його; розкриває основний зміст питання, дає неповні визначення понять, допускає незначні порушення в послідовності викладення матеріалу та неточності при

використанні наукових термінів; нечітко формулює висновки, висловлює свої міркування щодо тих чи інших проблем, але припускається певних похибок у логіці викладу теоретичного змісту.

Оцінка "задовільно" (10-13 балів): вступник в аспірантуру в основному засвоїв теоретичний матеріал щодо змісту питання; фрагментарно розкриває зміст питання і має лише загальне його розуміння; при відтворенні основного змісту питання допускає суттєві помилки, наводить прості приклади, непереконливо відповідає, плутає поняття.

Оцінка "незадовільно" (0-9 балів): вступник не засвоїв зміст питання, не знає основних його понять; дає неправильну відповідь на запитання.

Виконання завдань вступного іспиту зі спеціальності F5 кібербезпека та захист інформації передбачає необхідність неухильного дотримання норм та правил академічної доброчесності відповідно до Положення про академічну доброчесність у Національному університеті "Львівська політехніка". За порушення зазначених норм та правил вступники в аспірантуру притягаються до відповідальності згідно вимог чинного законодавства.

Рекомендована література

1. Хорошко В.О., Азаров О.Д., Шелест М.Є. Основи копмп'ютерної стеганографії. Навч. посібн. для студентів і аспірантів. – Вінниця: ВДТУ, – 2003. – 143 с.
2. Грибунін В.Г., Оков І.М., Туринцев І.В. Цифрова стеганографія М.: СОЛОН-Пресс, –2002.
3. Конахович Г.Ф., Пузиренко А.Ю. Комп'ютерна стеганографія. Теорія і практика. – К.: "МК-Пресс", – 2006. – 288 с.
4. Кузнецов О.О. Стеганографія: навч. посібн. / О.О.Кузнецов, С.П.Євсеєв, О.Г.Король. – Харків : Вид. ХНЕУ, – 2011. – 232 с.
5. Дудикевич В. Б. Захист засобів і каналів телефонного зв'язку: Навчальний посібник / В. Б. Дудикевич, В. В. Хома, Л. Т. Пархуць. – Л.: Видавництво Львівської політехніки, – 2012. – 210 с.
6. Дудикевич В. Б. Концептуальні моделі захисту інформації для технологій стаціонарного, стільникового, супутникового зв'язку / В.Б.Дудикевич, Ю.Р.Гарасим, Г.В.Микитин // Вісник Національного університету "Львівська політехніка", Автоматика, вимірювання та керування. – 2010. – №665. – С. 18–26.
7. НД ТЗІ 1.4-001-2000: "Типове положення про службу захисту інформації в автоматизованій системі" від 4 грудня 2000 р. № 53 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806.
8. ДСТУ 3396.1-96: "Захист інформації. Технічний захист інформації. Порядок проведення робіт". Чинний від 01.07.1997 р.
9. ДСТУ ГОСТ 28147-2009. Системи обробки інформації. Захист криптографічний. Алгоритм криптографічного перетворення (ГОСТ 28147-89). – Чинний від 2009-02-01. – Київ : Держстандарт України, 2009.
10. Олійников Р. Принципи побудови і основні властивості нового національного стандарту блокового шифрування України / Р. Олійников, І Горбенко, О. Казимиров [та ін.] // Захист інформації.– квітень-червень 2015.– № 2.– С. 142-157.

11. Совин Я. Р. Ефективна реалізація алгоритму ДСТУ ГОСТ 28147-89 для 8-16-32-бітних вбудованих систем / Я. Р. Совин, В.В. Хома, І. Я. Тишик [та ін.] // НУ "Львівська політехніка", Львів. – 2019.
12. Горбенко І.Д., Горбенко Ю.І. Прикладна криптологія. Теорія і практика. Застосування: монографія. –Харків: Видавництво "Форт", – 2012. –870с.
13. Горбенко Ю.І., Горбенко І.Д. Інфраструктура відкритих ключів. Електронний цифровий підпис. Теорія та практика: монографія. – Харків: Видавництво "Форт", – 2010. – 608с.
14. Основи інформаційної безпеки [Текст] : навч. пос. / Дудикевич В. Б., Хорошко В.О., Яремчук Ю.Є. – Вінниця : ВНТУ, – 2018. – 316 с.
15. Забезпечення інформаційної безпеки держави [Текст] : Навчальний посібник / В. Б. Дудикевич, І. Р. Опірський, П. І. Гаранюк, В. С. Зачепило, А. І. Партика. Львів : Видавництво Львівської політехніки. – 2017. – 204 с.
16. Системи менеджменту інформаційної безпеки [Текст] : навчальний посібник / В.А. Ромака, В.Б. Дудикевич, Ю.Р. Гарасим, П.І. Гаранюк, І.О. Козлюк. Львів: Видавництво Львівської політехніки, – 2012. – 232 с.
17. Микитин Г.В. Комплексні системи безпеки кібернетичного простору кіберфізичної системи на основі концепції "об’єкт – загроза – захист2 / Інформаційні технології: проблеми та перспективи : монографія/ Дудикевич В.Б., Микитин Г. В. / за заг. ред. В.С. Пономаренко. – Х. : Вид Рожко С.Г. , 2017. – 447 с.
18. Бобало Ю. Я. Стратегічна безпека системи "об’єкт – інформаційна технологія": [монографія] / [Бобало Ю.Я., Дудикевич В.Б., Микитин Г.В.] – Львів: Вид-во НУ "Львівська політехніка2. – 2020. – 260 с.
19. Микитин Г.В. Багаторівнева безпека інформаційних систем / В.Б. Дудикевич, Г.В. Микитин // Сучасна спеціальна техніка. – 2019. – № 4. – С. 14-23.
20. Микитин Г.В. Системна модель інформаційної безпеки розумного міста / В.Б. Дудикевич, Г.В. Микитин, М.О. Галунець // Системи обробки інформації. – 2020. – Випуск 2(161). – С. 93-98.
21. Совин Я.Р., Опірський І.Р., Наконечний Ю. М, Стахів М. Ю. Аналіз апаратної підтримки криптографії у пристроях Інтернету речей // Науковий журнал "Безпека інформації", №1 (24), 2018. – с. 36-48.
22. Я. Р. Совин, В. І. Отенко, Є. Ф. Штефанюк. Ефективна реалізація алгоритму блокового симетричного шифрування ДСТУ 7624:2014 ("Калина") для 8/16/32-бітових вбудованих систем // Науково-технічний журнал “Сучасний захист інформації”, №3 (31), 2017. – с. 6-16.
23. Я. І. Грабовський, Я. Р. Совин, І. Я. Тишик. Порівняння реалізацій нових алгоритмів гешування SHA-3 та ГОСТ Р 34.11-2012 для 8/32-бітових мікроконтролерних архітектур // Вісник Національного університету "Львівська політехніка" "Комп’ютерні системи та мережі". – 2015. – № 830. – С. 25-32.
24. Я. Р. Совин, Наконечний Ю. М, Стахів М. Ю. Дослідження характеристик вбудованого генератора випадкових чисел мікроконтролерів родини STM32F4XX згідно з методикою NIST STS // Вісник НУ “Львівська політехніка” – “Автоматика, вимірювання та керування”, № 753, 2013. – С. 37-44.
25. Мікропроцесори в системах технічного захисту інформації [Текст] : навч. посіб. / Я. Р. Совин,Ю. М. Наконечний; Нац. ун-т "Львів. політехніка". — Л.: Вид-во Львів.політехніки, 2011. – 305 с. : рис., табл. – Бібліогр.: – С. 304-305. – ISBN 978-617-607-047-4
26. Дудикевич В.Б., Березюк Б.М. Особливості інцидентів у сучасному кібернетичному просторі та їх вплив на безпеку суспільства // Вісник Нац. ун-ту "Львівська політехніка" "Автоматика, вимірювання та керування". – 2017 . – №880. – С.73-78.
27. Дудикевич В.Б., Березюк Б.М., Піскозуб А.З. Особливості будови та захисту корпоративних сховищ даних // Вісник Нац. ун-ту "Львівська політехніка" "Автоматика, вимірювання та керування". – 2017 . – №880. – С.44-50.

28. Модель методики оцінювання ризиків інформаційних систем, побудованих на Saas платформах / Пантелюк Д.М. Ромака В.А. Гаранюк П.І. Стецяк Т.Б. // Збірник наукових праць Української Академії друкарства "Комп'ютерні технології друкарства" , 2016р . – №35, – С.40-45.
29. Вплив атмосфери на поширення лазерного випромінювання / Совин Я. Р., Пархуць Л. Т., Ракобовчук Л. М. // Сучасний захист інформації. 2024, № 1, – С. 108-113.
30. Вплив інтер'єру приміщення на протидію лазерним системам акустичної розвідки / Пархуць Л. Т., Совин Я. Р., Ракобовчук Л. М. // Кібербезпека: наука, освіта, техніка. 2024 №1 (23). – С. 246-257.
31. Valeriy Lakhno, Valeriy Kozlovskii, Yuliia Boiko, Andrii Mishchenko, Ivan Opirskyy. "Management of information protection based on the integrated implementation of decision support systems", Eastern-european journal of enterprise technologies. Information and controlling system, Vol 5, No 9(89), pp.36-42, (2017). DOI: 10.15587/1729-4061.2017.111081.
32. Zhengbing Hu, Yulia Khokhlachova, Viktoriia Sydorenko, Ivan Opirskyy. Method for Optimization of Information Security Systems Behavior under Conditions of Influences / International Journal of Intelligent Systems and Applications (IJISA), Vol.9, No.12, pp.46-58, 2017. DOI: 10.5815/ijisa.2017.12.05
33. Maksymovych V., Harasymchuk O., Opirskyy I. (2019) The Designing and Research of Generators of Poisson Pulse Sequences on Base of Fibonacci Modified Additive Generator. In: Hu Z., Petoukhov S., Dychka I., He M. (eds) Advances in Computer Science for Engineering and Education. ICCSEEA 2018. Advances in Intelligent Systems and Computing, vol 754. Springer, Cham, pp.43-53. DOIhttps://doi.org/10.1007/978-3-319-91008-6_5
34. Banakh R., Piskozub A., Opirskyy I. (2019) Detection of MAC Spoofing Attacks in IEEE 802.11 Networks Using Signal Strength from Attackers' Devices. In: Hu Z., Petoukhov S., Dychka I., He M. (eds) Advances in Computer Science for Engineering and Education. ICCSEEA 2018. Advances in Intelligent Systems and Computing, vol 754. Springer, Cham. Pp.468-477. https://doi.org/10.1007/978-3-319-91008-6_47.
35. Lyubomyr Parkhuts. Development of optimal algorithms control the exchange of information on the corporate network / Maryna Kostiak, Lyubomyr Parkhuts // Monografia. Wydawnictwo naukowe akademii techniczno-humanistycznej w Bielsku-Białej. – 2016, – P.165-169.
36. L.Parkhuts. Development of a conceptual model of adaptive access rights management with using the apparatus of Petri nets / V. Lakhno, V. Buriachok, L. Parkhuts, H. Tarasova, L. Kydyralina, P. Skladannyi, M. Skrypnyk, A. Shostakovska // International Journal of Civil Engineering & Technology (IJCIET), Volume 9, Issue 11, November 2018, pp. 95–104, ISSN Print: 0976-6308 and ISSN Online: 0976-6316; Journal Impact Factor (2016): 9.7820 Calculated by GISI (www.jifactor.com); InfoBase Index IBI Factor for the year 2015–16 is 4.19; Thomson Reuters' Researcher ID: B-7378-2016 (Scopus).
37. L.Parkhuts. Funding model for port information system cyber security facilities with incomplete hacker information available / V.Lakhno, V.Malyukov, L.Parkhuts, V.Buriachok, B.Satzhanov, A.Tabylov // Journal of Theoretical and Applied Information Technology. – 15th July 2018. – Vol. 96. – № 13. – P. 4215-4225. (Scopus).
38. L.Parkhuts. The objectified procedure and a technology for assessing the state of complex noise speech information protection / V. Blintsov, S. Nuzhniy, L. Parkhuts, Yu. Kasianov // Eastern-European Journal of Enterprise Technologies ISSN 1729-3774. – 2018. – № 5/9. – P. 26-34. (Scopus).
39. L.Parkhuts. Verification of the security systems antagonistic agents behavior model / O.Milov, L.Parkhuts, S.Milevskyi, S.Pohasii // Системи обробки інформації, – 2019, вип. 4 (159). – Харків – С. 65-81.
40. Mykytyn G.V. The concept of creation of multi-level complex system of cyber-physical systems safety/ Dudykevych V.B., Mykytyn G.V., Kret T.B. // Системи обробки інформації. – 2016. – випуск № 5 (142). – С. 87-93.

41. Mykytyn G.V. Security of Cyber-Physical Systems from Concept to Complex Information Security System/ Dudykevych V., Mykytyn G., Kret T., Rebets A. // Advances in Cyber-Physical Systems/ - Volume 1, Number 2 (2016). – С. 67-75.
42. Volodymyr Khoma, Małgorzata Zygarlicka, Yaroslav Sovyn, Yaroslav Reshetar. Implementacja algorytmu kryptograficznego "Kalyna2 w systemach wbudowanych // Przegląd Elektrotechniczny (Electrical Review), ISSN 0033-2097, R. 94. 2018 Nr 4, p. 157-163.
43. Volodymyr Khoma, Vitalii Ivanyuk. High Sensitive Wiretap Detector: Design and Modeling // Przegląd Elektrotechniczny (Electrical Review), ISSN 0033-2097, R. 93. 2017 Nr 2, p. 250-254.
44. Designing an Information System to Create a Product in Terms of Adaptation / Nazarkevych, H., Nazarkevych, M., Kostiak, M., Pavlysko, A. // Studies in Systems, Decision and Controlthis link is disabled, 2023, 462, pp. 153-169. Scopus
45. Methods of Capturing and Tracking Objects in Video Sequences with Subsequent Identification by Artificial Intelligence / Nazarkevych, M., Lutsyshyn, V., Lytvyn, V., Kostiak, M., Kis, Y. // CEUR Workshop Proceedings, 2023, 3421, pp. 237-245. Scopus
46. Methods of Face Recognition in Video Sequences and Performance Studies / Nazarkevych, M., Lutsyshyn, V., Nazarkevych, H., Parkhuts, L., Kostiak, M. // CEUR Workshop ProceedingsThis link is disabled., 2023, 3421, pp. 246-253. Scopus
47. Research on Security Challenges in Cloud Environments and Solutions based on the security-as-Code Approach / Vakhula, O., Opirskyy, I., Mykhaylova, O. // CEUR Workshop Proceedings, 2023, 3550, pp. 55–69
48. Development of the Learning Management System Concept based on Blockchain Technology / Poberezhnyk, V., Balatska, V., Opirskyy, I. // CEUR Workshop Proceedings, 2023, 3550, pp. 143–156
49. Method of assessment of frequency resolution for aircraft / Yevseiev, S., Herasymov, S., Kuznietsov, O., .Matovka, T., Rizak, V. // Eastern-European Journal of Enterprise Technologies, 2023, 2(9-122), pp. 34–45
50. Method of Dataset Filling and Recognition of Moving Objects in Video Sequences based on YOLO / Nazarkevych, M., Lytvyn, V., Kostiak, M., Oleksiv, N., Naconechnyi, N. // CEUR Workshop ProceedingsThis link is disabled., 2024, 3654, pp. 265-276. Scopus
51. A YOLO-based Method for Object Contour Detection and Recognition in Video Sequences / Nazarkevych, M., Kostiak, M., Oleksiv, N., Vysotska, V., Shvahuliak, A.-T. // CEUR Workshop Proceedings, 2024, 3654, pp. 49-58. Scopus
52. Brydinskyi V., Khoma Y., Sabodashko D., Podpora M., Khoma V., Konovalov A., Kostiak M. Comparison of modern deep learning models for speaker verification // Applied Sciences (Switzerland). – 2024. – Vol. 14, iss. 4. – P. 1329-1–1329-12. (Web of Science)
53. Blockchain Application Concept in SSO Technology Context / Balatska, V., Poberezhnyk, V., Petriv, P., Opirskyy, I. // CEUR Workshop Proceedings, 2024, 3654, pp. 38–49
54. Security-as-Code Concept for Fulfilling ISO/IEC 27001:2022 Requirements / Vakhula, O., Kurii, Y., Opirskyy, I., Susukailo, V. // CEUR Workshop Proceedings, 2024, 3654, pp. 59–72.