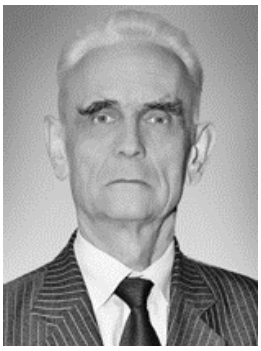
# БЕЗПЕКА СИСТЕМ ЕЛЕКТРОННОГО УРЯДУВАННЯ / SECURITY OF ELECTRONIC MANAGEMENT SYSTEMS

**DOI: 10.18372/2225-5036.30.18576**

# БЕЗПЕКА ТЕХНОЛОГІЙ ФУНКЦІОНУВАННЯ ЦЕНТРУ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ЗАКЛАДУ ВИЩОЇ ОСВІТИ

**Валерій Дудикевич, Галина Микитин, Захар Лосев**

*Національний університет "Львівська політехніка"*



**ДУДИКЕВИЧ Валерій Богданович**, д.т.н., професор, заслужений винахідник України
*Рік та місце народження*: 1941 рік, с. Біло-Скелювате Ново-Світлівського району Луганської обл.,Україна.
*Освіта*: Львівський політехнічний інститут, 1963 рік.
*Посада*: професор кафедри захисту інформації Національного університету «Львівська політехніка», керівник Західного регіонального навчально-наукового центру захисту інформації.
*Наукові інтереси*: інформаційна безпека, технічний захист інформації, число-імпульсні перетворювачі кодів для вимірювання і управління.
*Публікації*: понад 600 наукових публікацій, серед яких біля 200 винаходів, монографії, наукові статті , підручники та навчально -методичні посібники.
*E-mail*: vdudykev@gmail.com.
*Orcid ID*: 0000-0001-8827-9920.

**МИКИТИН Галина Василівна**, д.т.н., професор
*Рік та місце народження*: 1962 рік, м. Тлумач Івано-Франківської області, Україна.
*Освіта*: Львівський політехнічний інститут, 1986 рік.
*Посада*: професор кафедри захисту інформації Національного університету «Львівська політехніка».
*Наукові інтереси*: безпека інформаційно-комунікаційних технологій, безпека кіберфізичних систем, безпека технологій процесів інтелектуалізації.
*Публікації*: більше 300 наукових публікацій, серед яких наукові статті, монографії, довідник та навчально-методичні посібники.
*E-mail*: cosmos-zirka@ukr.net.
*Orcid ID*: 0000-0003-4275-8285.

**ЛОСЕВ Захар Олександрович,** магістрант
*Рік та місце народження*: 2001 рік, м. Костянтинівка Донецької області, Україна.
*Освіта:* Національний університет "Львівська політехніка", 2023 рік.
*Посада:* магістрант кафедри захисту інформації Національного університету «Львівська політехніка».
*Наукові інтереси:* безпека комп'ютерних мереж, безпека кіберфізичних систем.
*Публікації*: тези Всеукраїнської науково-практичної конференції.
*E-mail*: zaharlosev888@gmail.com.
*Orcid ID:* 0009-0007-7562-6808.

***Анотація***. *У цій статті розглянуто питання інформаційного забезпечення (ЦІЗ) НУ "Львівська політехніка" розвинуто підхід до безпечного функціонування центру в кібернетичному просторі та комунікаційному середовищі на ос-нові створення систем безпеки інформаційно-комунікаційних технологій згідно концепції "об'єкт – загроза – захист". Розроблено програмну реалізацію шифрування інформації на основі алгоритму AES засобами Python з метою забезпечення безпечного функціонування баз даних в кібернетичному просторі ЦІЗ.*

***Ключові слова***: *центр інформаційного забезпечення, інформаційні ресурси, інформаційні системи, інформаційні процеси, комунікаційні системи, загрози, комплексні системи безпеки, шифрування інформації.*

**Постановка проблеми**

Триває розвиток підходів і технологій безпечного функціонування ЦІЗ, зокрема за такими напрямками:

– створення бази знань автоматизованої експертної системи для аналізу ризиків інформаційної безпеки;

– розроблення моделей безпеки баз даних;

– розроблення профілю Рамкової концепції кібербезпеки для управління ризиками програм;

– шифрування голосових повідомлень при одноранговому зв'язку за допомогою модифікованого і полегшеного алгоритму AES.

З метою цілісного представлення процесу безпечного функціонування ЦІЗ закладу вищої освіти розглянемо структури кібернетичного простору і комунікаційного середовища НУ "Львівська політехніка" та системи їх безпеки на основі концепції "об'єкт – загроза захист".

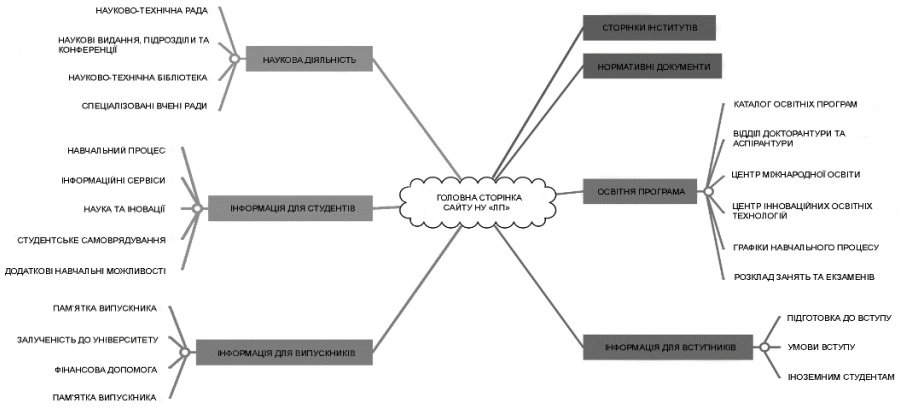
Об'єкт дослідження – кібернетичний простір та комунікаційне середовище ЦІЗ Національного університету "Львівська політехніка".

Предмет дослідження – безпека інформаційних ресурсів, інформаційних систем, інформаційних процесів та безпровідних комунікаційних систем ЦІЗ закладу вищої освіти.

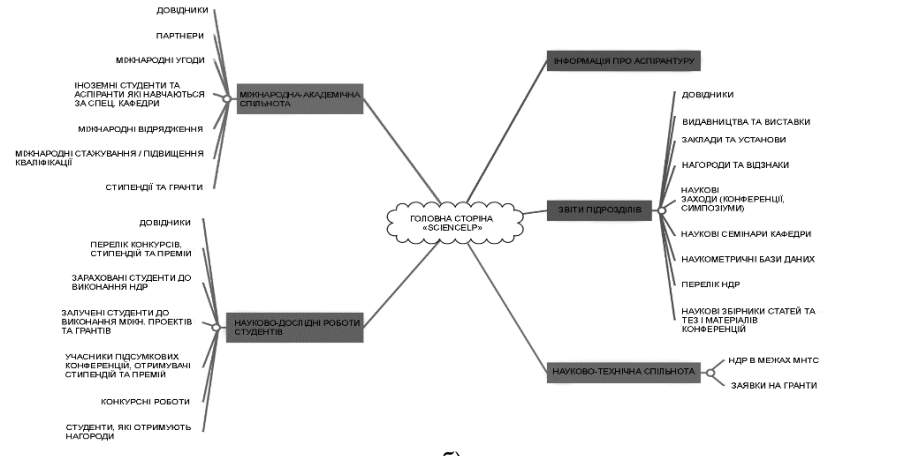
Методи дослідження – системний аналіз і технології інформаційної безпеки.

**Мета та постановка завдання**

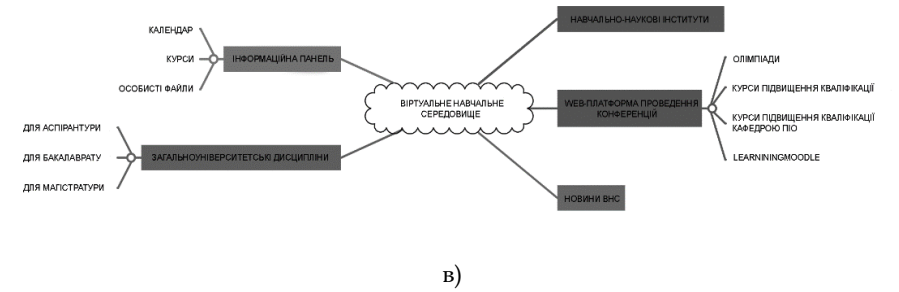
Мета роботи – побудова систем безпеки: кібернетичного простору на рівні – інформаційних ресурсів, систем і процесів; комунікаційного середовища на рівні – безпровідних технологій зв'язку згідно концепції "об'єкт – загроза – захист" і, на цій основі, створення програмної реалізації шифрування інформації в базах даних на основі AES з метою забезпечення безпечного функціонування ЦІЗ НУ "Львівська політехніка".




а)




б)




в)

Рис. 1. Кібернетичний простір центру інформаційного забезпечення: цільові інформаційні ресурси (а, б, в)

**Виклад основного матеріалу**

Кібернетичний простір НУ "Львівська політехніка": "об'єкт – загроза – захист" Кібернетичний простір закладу вищої освіти НУ Львівська політехніка представлений складовими: інформаційними ресурсами, інформаційними системи, інформаційними процеси. Інформаційні ресурси – сукупність документів у інформаційній системі (бібліотеках, архівах, банках даних тощо).

Представлена структура цільових інформаційних ресурсів НУ "Львівська політехніка", які функціонально сформовані на рівні захищених: баз даних, баз знань, масивів інформації, сховищ даних, баз моделей, сховищ даних, баз моделей (рис. 1).

Представлена комплексна система безпеки сегменту інформаційних ресурсів – баз даних на основі концепції "об'єкт – загроза – захист" (табл. 1).

Таблиця 1

Бази даних: загрози – технології безпеки

| Бази даних | | | |
|---|---|---|---|
| Загрози | | Захист | |
| Апаратні | Програмні | Апаратний | Програмний |
| вбудовування логічної бомби;<br>введення невірних даних;<br>знищення інформації і засобів її обробки;<br>розкрадання інформації засобів її обробки;<br>пошкодження облад-нання;<br>помилки операторів;<br>помилки при обслуговуванні;<br>несанкціонований Доступ до адміністра-тивної частини;<br>відключення або виведення з ладу підсистем забезпечення функціонування системи | відмова програмного забезпечення;<br>зміна даних;<br>модифікація даних;<br>витік, порушення цілісності, справжності й збережності інформації при її обробці;<br>"чистка сміття" на диску або в оперативній пам'яті;<br>установка неперевіре-них виконуваних модулів і командних процедур, де можуть знаходитися "троянські коні", "черв'яки";<br>створення або зміна записів бази даних захисту | підвищення достовірнос-ті даних, що вводяться;<br>контроль та обмеження доступу;<br>посилення оперативно-го реагування на атаки в напрямку інформаційних ресурсів організації;<br>контроль звернень до захисних компонентів інформаційної системи;<br>реагування при НСД;<br>моніторинг активності в системі управління захистом;<br>реєстрація у журналі дій та операцій | захист паролем;<br>шифрування даних і програм;<br>захист полів та записів таблиць бази даних;<br>розділення прав доступу до об'єктів бази даних;<br>забезпечення цілісності зв'язків таблиць;<br>антивірусне програмне забезпечення;<br>цифровий псевдонім;<br>запобігання створення несанкціонованої інформації;<br>управління потоком захищених процедур і програм при передаванні з одного сегмента БД в інший |

Таблиця 2

Бази знань: технології безпеки

| Бази знань | | | |
|---|---|---|---|
| Загрози | | Захист | |
| Апаратні | Програмні | Апаратний | Програмний |
| введення невірних даних;<br>знищення інформації і засобів її обробки;<br>розкриття конфіденційної інформації;<br>пошкодження обладнан-ня;<br>порушення роботи системи або її частин;<br>відмови програмного та апаратного забезпечення:<br>фізичне руйнування системи або виведення з ладу найбільш важливих її компонентів | відмова програмного забезпечення;<br>зміна даних;<br>модифікація даних;<br>витік, порушення цілісності інформації при її обробці;<br>витік інформації про функціонування системи захисту кодів доступу чи паролів;<br>несанкціоноване отримання та використання привілеїв;<br>пошкодження вторинних знань | контроль доступу;<br>аутентифікація;<br>виявлення сторонніх засобів;<br>контроль процесу передавання;<br>захист обробки даних;<br>створення резервних копій;<br>фільтрація даних;<br>використання обладнан-ня IT з малим рівнем випромінювання;<br>установка джерел безперебійного живленняня | захист доступу до даних;<br>розмежування доступу;<br>аутентифікація;<br>надійне місце зберігання даних;<br>шифрування передачі інформації;<br>архівування даних;<br>цифровий підпис і криптосистеми з відкри-тим ключем;<br>резервне копіювання даних |

В наступній таблиці представлена комплексна система безпеки сегменту інформаційних ресурсів – баз знань на основі концепції "об'єкт – загроза – захист" (табл. 2).

Інформаційні системи – організаційно-технічні системи, в яких реалізується технологія обробки інформації з використанням технічних і програмних засобів. В основному ІС класифікуються за: способом реалізації в інформаційній системі; за ступенем охоплення задач управління; за класом реалізованих технологічних операцій; за типом користувацького інтерфейсу; за способом побудови мережі; за предметними сферами обслуговування. За ступенем охоплення завдань управління найбільш використовувані на практиці автоматизовані системи обробки інформації (АСОІ), автоматизовані системи управління, системи автоматизації офісу, системи підтримки прийняття рішень (СППР), експертні системи. Безпечне функціонування кібернетичного простору ЦІЗ НУ "Львівська політехніка" на рівні збору, обробки, аналізу інформації та прийняття ефективного управлінського рішення забезпечують, зокрема – АСОІ та СППР. Автоматизована система обробки інформації – комплекс взаємопов'язаних методів і засобів збору і обробки інформації, необхідних для автоматизації процесів та управління об'єктами (рис. 2).

Система підтримки прийняття рішення – автоматизована система збору та аналізу інформації на основі системи управління базою даних (СУБД) та системи управління базою моделей (СУБД) з метою прийняття ефективного управлінського рішення станом відповідного об'єкта інфраструктури (рис. 3).

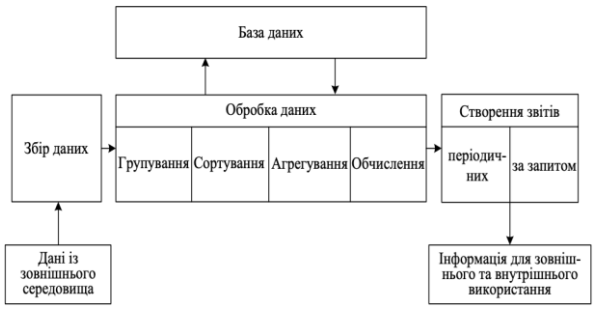



Рис. 2. Кібернетичний простір ЦІЗ: структура АСОД

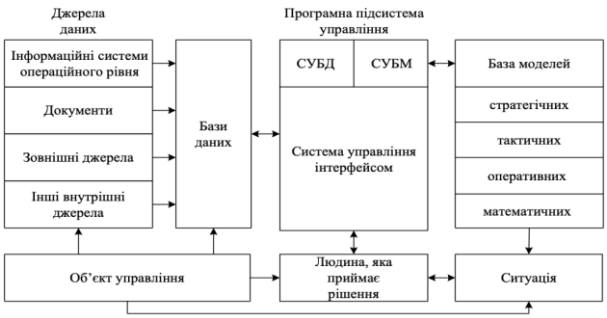



Рис. 3. Кібернетичний простір ЦІЗ: структура СППР

Таблиця 3

АСОІ, СППР: цілеспрямовані загрози – технології безпеки

| Загрози | Захист |
|---|---|
| SQL-injections | WAF та IPS;<br>використання PAM-систем;<br>валідація вхідних даних;<br>екранування спеціальних символів;<br>використання сканерів вразливостей. |
| Використання вразливих та застарілих компонентів | регулярне та автоматизоване оновлення компонентів;<br>проведення сканування ПЗ на вразливості;<br>завантаження компонентів тільки із офіційних сайтів та тільки використовуючи безпечне з'єднання;<br>видалення компонентів, які більше не використовуються в системі. |
| Несанкціоноване отримання доступу до інформації в системі | шифрування даних "at rest";<br>видалення критичних даних із системи як тільки вони стають непотрібними;<br>використання найбезпечніших протоколів і алгоритмів для передачі даних;<br>зберігання паролів використовуючи сильні,<br>адаптивні та "підсолені" функції хешування;<br>бекапування даних. |
| DdoS-атаки | WAF and CDN;<br>high-availability setup;<br>автоматизоване керування пропускною здатністю мережі;<br>фільтрування та скидання пакетів у випадку потенційних flood-атак;<br>автоматичне масштабування ресурсів середовища.<br>Моніторинг мережі; |
| Фізичне пошкодження / знищення даних та устаткування | розмежування доступу до приміщень/території;<br>камери відеонагляду;<br>зміцнення захисту територій (грати на вікнах, електрична огорожа, охорона);<br>екранування приміщень. |
| Виведення з ладу інформаційних ресурсів | використання CDN систем;<br>DB replication;<br>Auto-scaling;<br>резервний постачальник послуг хмарного обчислення |

Цілеспрямовані загрози кібернетичному простору ЦІЗ на рівні: АСОІ, СППР. Представлені технології безпеки для інформаційних систем у просторі "об'єкт – загроза – захист" за впливу цілеспрямованих загроз (табл. 3).

Інформаційні процеси – процеси створення, збору, зберігання, обробки, відображення, передавання, розповсюдження інформації. Представлено функціонування ІП в ЦІЗ НУ "Львівська політехніка" на рівні етапів: фази, операцій, обробки (рис. 4).


Рис. 4. Кібернетичний простір ЦІЗ: ІП – фаза, операція, обробка

Розглянемо систему безпеки інформаційних процесів на рівні фаз: сприйняття / збір / відбір; передавання; обробки; зберігання; представлення / впливу у просторі "об'єкт – загроза – захист" (табл. 4).

Комунікаційне середовище ЦІЗ: об'єкт – загроза – захист. Безпровідна технологія LTE – мобільний стандарт високошвидкісного передавання даних 4G, який еволюціонував на основі технології UMTS (рис. 5). Функціонування LTE:

1) пристрій користувача ініціює з'єднання звернувшись до станції LTE, яка займається управлінням радіоканалами та мобільністю і виконує динамічний розподіл адрес між користувачами;

2) звертання до MME (Mobile Management Entity – мобільна управлінська сутність) для встановлення з'єднання між користувачем і базовою мережею, автентифікації, управління ключами шифрування, зберігання інформації про користувача;

3) звертання до S-GW (Serving Gateway – службовий шлюз), що відповідає за маршрутизацію і пересилку пакетів даних;

4) звертання до P-GW (Packet Data Network Gateway – шлюз пакетних даних мережі) для надання абоненту IP-адреси та фільтрації пакетів;

5) користувач під'єднаний до мережі Internet та має доступ до інформаційних ресурсів ЦІЗ. Використання: доступ до цільових ресурсів ЦІЗ (рис. 1) користувачі можуть отримати з мобільних пристроїв, використовуючи мережу LTE.

Таблиця 4

Інформаційний процес – фаза: загрози – технології безпеки

| Об'єкт: інформаційні процеси | Загрози | | Захист інформації | |
|---|---|---|---|---|
| 1. Фази | Цілеспрямовані | Випадкові | Апаратний | Програмний |
| 1.1. Сприйняття / збір / відбір | порушення конфіденційності інформації; відключення або виведення з ладу підсистем забезпечення функціонування системи | помилки людини, як джерела інформації; людини оператора; неправильні дії обслуговуючого персоналу; помилки людини, як ланки, що приймає рішення. | 1. Guardant<br>2. eToken<br>3. SenseLock<br>4. HASP | 1. ЕЦП<br>2. StarForce<br>3. LaserLock<br>4. Fairplay<br>5. Adobe Digital Editions |
| 1.2. Передавання | отримання несанкціонованого віддаленого доступу; затримання передавання повідомлення; фізичне руйнування системи або виведення з ладу найбільш важливих її компонентів | завади в лініях зв'язку від впли-вів зовнішніх фак-торів; збої чи нестабільність роботи технічних пристроїв; електромагнітне випромінювання; відмова систем живлення | 1. CryptoPhone G10i<br>2. Luna SA<br>3. nShield Connect<br>4. Бар'єр-301<br>5. Гряда-301 | 1. Secret Disk Server NG<br>2. RedPhone<br>3. Secret Net LSP<br>4. Secure Pack Rus<br>5. Thales |
| 1.3. Обробка | вхід в інформаційну систему в обхід засобів захисту; порушення конфіденційності інформації; втрата (знищення) інформації; вірусні атаки | відмови програмного та апаратного забезпечення; збої чи нестабільність роботи технічних пристроїв; стихійні лиха | 1. Luna CA4<br>2. Luna PCI<br>3. ProtectServer Gold (мініпристрій)<br>4. KOKON-R | 1. TrueCrypt<br>2. R-Crypto Disk Security<br>3. Secret Disk Server NG |
| 1.4. Зберігання | злам шифрів криптографічного захисту інформації; фізичне руйнування системи; порушення цілісності та конфіденційності інформації; | технічні несправності мережі і компонентів; відмова систем живлення; помилки людини | 1. М-590<br>2. Secure IDE<br>3. РУТОКЕН<br>4. CryptoLine 358<br>5. Кристал-1Д | 1. BestCrypt Volume Encryption<br>2. Secret Disk<br>3. WISeCrypt<br>4. Crypto Composer |
| 1.5. Представлення / вплив | віддалений запуск додатків; порушення конфіденційності інформації | несанкціонований доступ до адміністративної частини відмова систем живлення; помилки операторів | 1. Бар'єр-301<br>2. Luna PCI<br>3. nShield Solo<br>4. HASP | 1. Secure Pack Rus<br>2. Fairplay<br>3. LaserLock<br>4 Adobe Digital Editions |

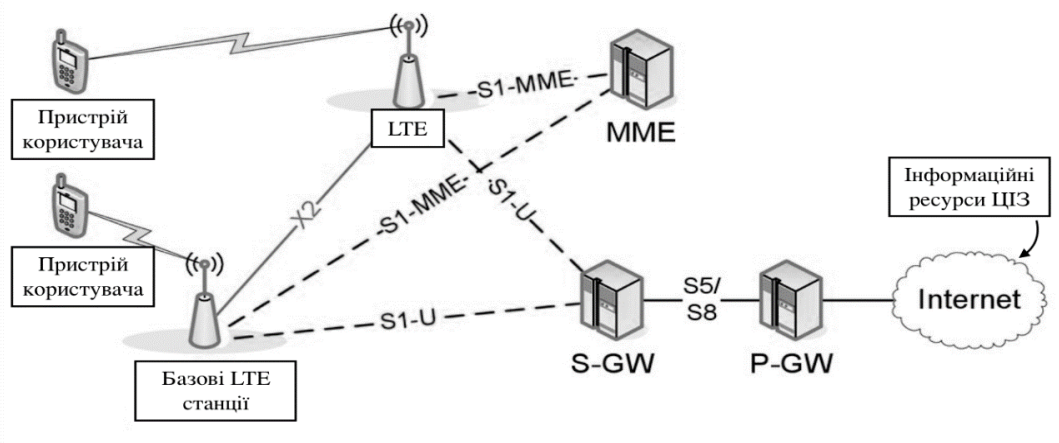



Рис. 5. Комунікаційне середовище ЦІЗ: структура LTE

Таблиця 5

Характеристики протоколу LTE

| Характеристики | LTE |
|---|---|
| Частота | 1800 МГц (Band 3)<br>2600 МГц (Band 7)<br>900 МГц (Band 8) |
| Швидкість передавання | завантаження до 100 Мб/с(на практиці до 5-12 Мб/с)<br>вивантаження до 50 Мб/с(на практиці до 2,5 Мб/с) |
| Дальність | LTE-900 26 км<br>LTE-1800 13,5 км<br>LTE-2600 2,5 - 3 км |
| Розмір мережі | обмежена тільки пропускною здатністю станції LTE |
| Затримка | 10 ms |

Представлені характеристики протоколу LTE (табл. 5). Безпровідна сенсорна технологія Zigbee – стандарт передавання даних зі здатністю до самоорганізації та самовідновлення із можливостями: використання ефективних протоколів; високої сумісності пристроїв; автоматичного відновлення маршрутів (рис. 6). Функціонування: завдання головної станції ZigBee-мережі: передавання мережевих маркерів, об'єднання абонентських пристроїв в єдину мережу, керування абонентськими пристроями, зберігання інформації про стан мережі, організація передавання даних між елементами мережі, отримання живлення від електромережі, постійне перебування в режимі приймання;. завдання підлеглої станції мережі: приймання і передавання даних; визначення чи є дані, які потрібно передати; запит необхідних даних від координатора мережі, перебування у пасивному режимі тривалий час. Використання: мережа Zigbee використовується для виконання інформаційних процесів в ЦІЗ: збору даних, передавання, обробки, зберігання, архівування, захисту, представлення.

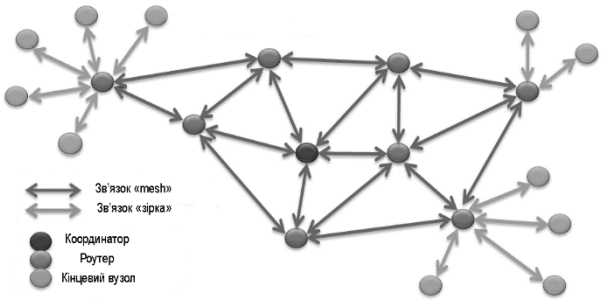



Рис. 6 Комунікаційне середовище ЦІЗ: структура Zigbee

Таблиця 6

Характеристики протоколу Zigbee

| Характеристики | Zigbee | | |
|---|---|---|---|
| Частота | 868 МГц | 915 МГц | 2,4 ГГц |
| Дальність | 1-10 м (укорочений радіус дії)<br>10-100 м (збільшений радіус дії) | | |
| Розмір стека | 4…32 Кбайт | | |
| Розмір мережі | 65536 (16-бітні адреси)<br>264 (64-бітні адреси) | | |
| Затримка | <70 ms | | |
| Переваги | самоорганізовування та самовідновлення; використання ефективних протоколів; висока сумісність пристроїв; енергозбереження, розміри мережі, відбір частотних діапазонів | | |

Представлені характеристики протоколу Zigbee (табл. 6). Цілеспрямовані загрози комунікаційному середовищу ЦІЗ на рівні: LTE, Zigbee. В наступній таблиці представлені технології безпеки для безпровідних комунікаційних систем у просторі "об'єкт – загроза – захист" (табл. 7).

Таблиця 7

LTE, Zigbee: цілеспрямовані загрози – технології безпеки

| Загрози | Захист |
|---|---|
| Снiфінг | регулярна перевірка засобів зв'язку на відсутність пристроїв прослуховування;<br>шифрування даних "in transit".<br>ідентифікація та авторизація користувачів, обладнання, даних. |
| Несанкціонований доступ до систем мережі (терміналів, шлюзів, комутаторів) | NGAV;<br>SIEM та SOAR;<br>IDS та IPS;<br>залучення розподіленої команди SOC-аналістів для налаштування та моніторингу систем безпеки;<br>логування подій;<br>шифрування даних "in transit";<br>NGFW. |
| Несанкціоноване внесення змін в конфігурацію систем | автоматичне тестування будь-яких змін до системи;<br>налаштування бекапів;<br>необхідність погодження змін з іншими членами команди. |
| Підміна довіреного об'єкта (MITM) | ідентифікація та авторизація користувачів, обладнання, даних;<br>шифрування даних в мережі. |
| Несанкціоноване проникнення в систему за допомогою шкідливого програмного забезпечення | покупка ліцензійних версії ПЗ;<br>регулярне оновлення ОС, вбудованого та купленого ПЗ;<br>застосування NGAV;<br>застосування NGFW. |

Алгоритмічно-програмна реалізація шифрування даних в кібернетичному просторі ЦІЗ. З метою захи-сту інформації в базах даних АСОІ та СППР, як інструментарію кібернетичного простору ЦІЗ, використано симетричний блоковий алгоритм AES (рис. 7), який має такі переваги: високу ефективність на будь-яких платформах; високий рівень захищеності; реалізацію в smart-картах; швидку процедуру формування ключа, підтримку різних довжин ключа з кроком 32 біта.

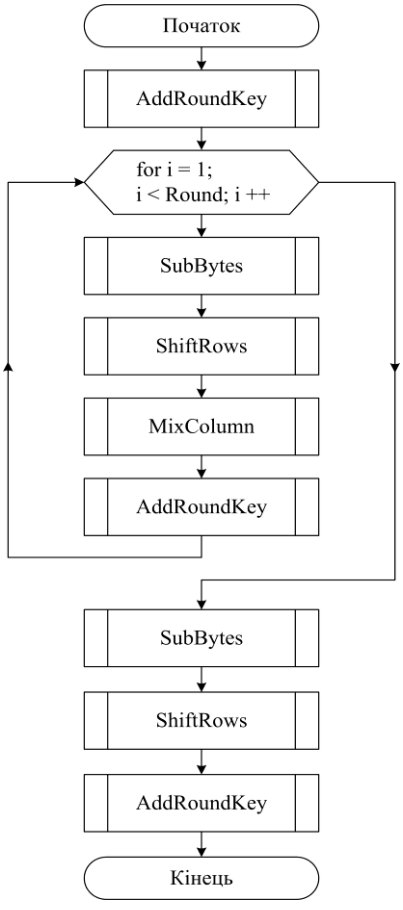



Рис. 7. Алгоритму програмної реалізації шифрування даних на основі стандарту AES

Шифрування даних в безпровідній технології зв'язку LTE реалізовано засобами мови програмування Python, серед переваг якої: об'єктно-орієнтована мова; відносно простий синтаксис; підтримка користувацьких бібліотек з відкритим кодом; створення модульних програм з графічним інтерфейсом т. і. Показано скріншоти програмної реалізації шифрування та дешифрування даних в мережі LTE ЦІЗ (рис. 8-11).

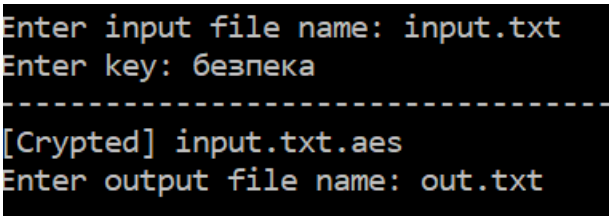



Рис. 8. Вікно програми

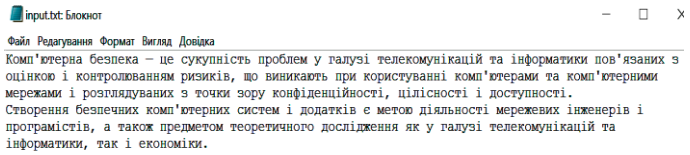



Рис. 9. Скрін вхідного тексту

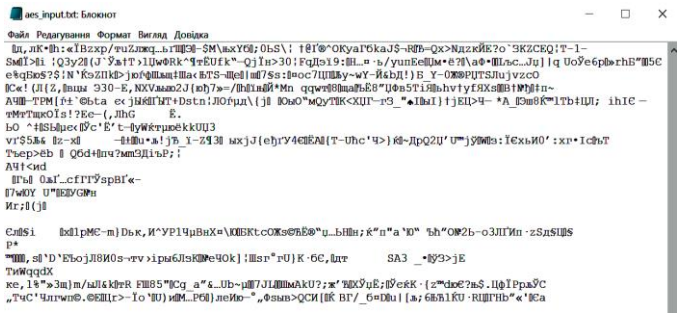



Рис. 10. Скрін шифрованого тексту

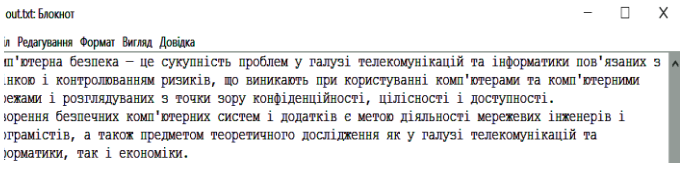



Рис.11. Скрін дешифрованого тексту

**Висновки**. В статті представлена структура кібернетичного простору та комунікаційного середовища ЦІЗ НУ Львівська політехніка відповідно на рівні: інформаційних цільових ресурсів – баз даних і баз знань; інформаційних систем – АСОІ, СППР; комунікаційних систем – LTE, Zigbee. Проаналізовано систему безпеки: інформаційних ресурсів на рівні апаратних і програмних загроз; інформаційних систем за випливу цілеспрямованих загроз в просторі "об'єкт – загроза – захист".

Розгорнуто структуру інформаційних процесів ЦІЗ на рівні фаз – сприйняття / збір / відбір; передавання; обробки; зберігання; представлення і проаналізовано систему безпеки за впливу цілеспрямованих і випадкових загроз.

Проаналізовано характеристики стандартів LTE, Zigbee і систему їх безпеки за впливу цілеспрямованих загроз. Розроблено програмну реалізацію шифрування/дешифрування інформації в кібернетичному просторі ЦІЗ на основі алгоритму AES засобами Python.

**Список літератури**

[1]. Yurchak Oleksandr. "Ukrayins'ka stratehiya Industriyi 4.0. 7 napryamiv rozvytku" [Електронний ресурс]. Режим доступу: https: // industry4-0 - ukraine. com.ua/2019/01/02/ukrainska-strategiya-industrii-4-0-7-napriankiv-rozvutku.

[2]. Стратегія кібербезпеки України. – [Електронний ресурс]. Режим доступу: https://zakon.rada.gov.ua/laws/show/447/2021#n12.

[3]. Програма EU4Digital: Кібербезпека – Схід. [Електронний ресурс]. Режим доступу: https://eufordigital.eu / uk / discover-eu / eu4digital-improving-cyber-resilience-in-the-eastern-partnership-countries/.

[4]. Бобало Ю. Я. Стратегічна безпека системи "об'єкт – інформаційна технологія": [монографія] / [Бобало Ю. Я., Дудикевич В. Б., Микитин Г. В. ]. Львів: Видавництво НУ "Львівська політехніка", 2020. 260 с.

[5]. D. Vitkus, Z.Steckevicius and N. Goranin (2019) Метод розробки бази знань автоматизованої експертної системи для аналізу ризиків інформаційної безпеки [Електронний ресурс] Режим доступу: https:// www.researchgate.net/publication/337571793_Automated_Expert_System_Knowledge_Base_Development_Method_for_Information_Security_Risk_Analysis.

[6]. A. Mousa, M. Karabatak and T. Mustafa. (2020) Загрози та виклики безпеці баз даних. [Електронний ресурс] Режим доступу: https: // ieeexplore.ieee.org/ document/9116436.

[7]. W. C. Barker, K. Scarfone, W. Fisher & M. Souppaya (2021). Профіль Рамкової концепції кібербезпеки для управління ризиками програм-вимагачів. [Електронний ресурс] Режим доступу: https:// nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8374.pdf.

[8]. K. Kumar, K. R. Ramkumar, and A. Kaur (2022) Полегшена реалізація алгоритму AES для шифрування голосових повідомлень з використанням польових програмованих вентильних матриць, Журнал Університету Короля Сауда. Комп'ютерні та інформаційні науки [Електронний ресурс]. Режим доступу: https://www.researchgate.net/publication/343674360_A_Lightweight_AES_Algorithm_Implementation_for_Encrypting _ Voice _ Messages_using_Field_Programmable_Gate_Arrays/.

**УДК: 004.054**

***Dudykevych V., Mykytyn G., Losev Z. Safety of the center's technological functions information security for higher investment***

***Abstract**. In this article, the issue of information support (CIS) of Lviv Polytechnic National University is considered, an approach to the safe functioning of the center in cyberspace and the communication environment is developed on the basis of the creation of security systems of information and communication technologies according to the concept of "object - threat" - protection". A software implementation of information encryption based on the AES algorithm by means of Python was developed in order to ensure the safe functioning of databases in the cyberspace of the Central Intelligence Agency.*

***Keywords**: intelligent transport, cyber-physical system, physical space, communication environment, cyber space, multi-level comprehensive security model, comprehensive security system, threats, security technologies, message encryption algorithm.*

**Дудикевич Валерій Богданович**, доктор технічних наук, професор, керівник Західного регіонального навчально-наукового центру захисту інформації, професор кафедри Національного університету «Львівська політехніка», Львів, Україна.

**Valerii Dudykevych**, Doctor of Technical Sciences, Professor, Head of the Western Regional Information Security Training and Research Center, Professor of Department of Lviv Polytechnic National University, Lviv, Ukraine.

**Микитин Галина Василівна**, доктор технічних наук, професор, професор кафедри Національного університету «Львівська політехніка», Львів, Україна.

**Galyna Mykytyn**, Doctor of Technical Sciences, Professor, Professor of Department of Lviv Polytechnic National University, Lviv, Ukraine.

**Лосев Захар Олександрович**, магістрант кафедри захисту інформації Національний університет «Львівська політехніка», Львів, Україна.

**Zakhar Losev**, Master's student of the Department of Information Security, Lviv Polytechnic National University, Lviv, Ukraine.

Отримано *23 січня 2023 року,* затверджено редколегією *1 квітня 2024 року*