РОЗРОБКА МЕТОДИКИ СТВОРЕННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНІЙ СИСТЕМІ У БУХГАЛТЕРІЇ ГОЛОВНОГО УПРАВЛІННЯ ДЕРЖАВНОЇ СЛУЖБИ З НАДЗВИЧАЙНИХ СИТУАЦІЙ УКРАЇНИ У ВІННИЦЬКІЙ ОБЛАСТІ

КАБАЛЮК ДМИТРО СЕРГІЙОВИЧ

- *Мета даного* дослідження полягає у створенні комплексної системи захисту інформації, у розробці комплексу взаємоузгоджених заходів, спрямованих на удосконалення і впровадження інформаційної технології, яка забезпечує обробку інформації в бухгалтерії Головного управління ДСНС України у Вінницькій області.
- *Об'єктом дослідження* є процес обробки даних у бухгалтерії Головного управління Державної служби України з надзвичайних ситуацій у Вінницькій області.
- *Предмет дослідження* – захист цілісності, конфіденційності, доступності та обробки даних, що передаються каналами зв'язку з високим рівнем загроз.

ВИДИ ІНФОРМАЦІЇ, ЯКА ЦИРКУЛЮЄ У БУХГАЛТЕРІЇ ГОЛОВНОГО УПРАВЛІННЯ ДСНС УКРАЇНИ У ВІННИЦЬКІЙ ОБЛАСТІ

- –Облікова інформації
- Звітна інформація
- Персональна данні користувачів
- Інформації виробничого та технічного характеру

ЕТАПИ ПРОВЕДЕННЯ ЕКСПЕРТИЗИ:

- аналіз документації, розробленої на етапі виконання передпроектних робіт;
- аналіз Технічного завдання на створення КСЗІ ОІД з частиною захисту від витоку технічними каналами або ТЗ на КТЗІ;
- аналіз проектної документації та матеріалів;
- аналіз нормативно-розпорядчої документації;
- аналіз документації щодо проведених випробувань;
- аналіз організаційно-розпорядчої документації;
- перевірка впровадження реалізованих у складі організаційних, фізичних та інших нетехнічних заходів захисту;
- перевірка підготовленості співробітників СЗІ, персоналу ОІД;
- перевірка (за необхідності) результатів створення та атестації комплексу ТЗІ.

ДОСЛІДЖЕННЯ РЕЗУЛЬТАТІВ ОБСТЕЖЕННЯ ОБЧИСЛЮВАЛЬНОЇ СИСТЕМИ ІТС

Під час обстеження обчислювальної системи у Головному управлінні визначено, що ІТС бухгалтерії Головного управління є багатомашинним багатокористувацьким комплексом, до складу якого входять обчислювальна система, фізичне середовище, в якому вона знаходиться і функціонує, середовище користувачів, оброблювана інформація, у тому числі й технологія її оброблення.

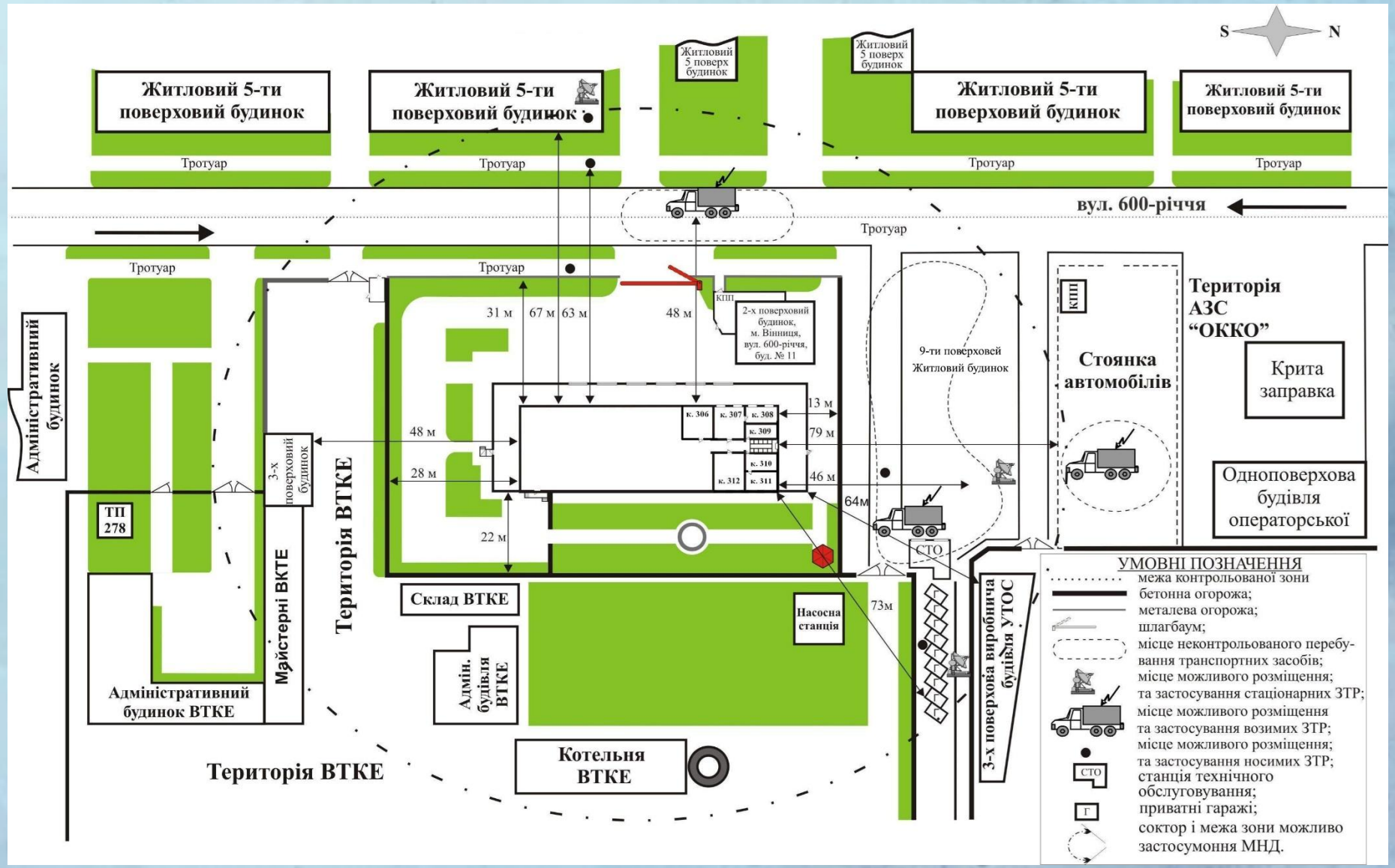
Згідно НД ТЗІ 2.5-004-99 ІТС класифікується як АС класу "З".

Обчислювальна система ІТС підрозділів складається з РС адміністратора та операторів відділу.

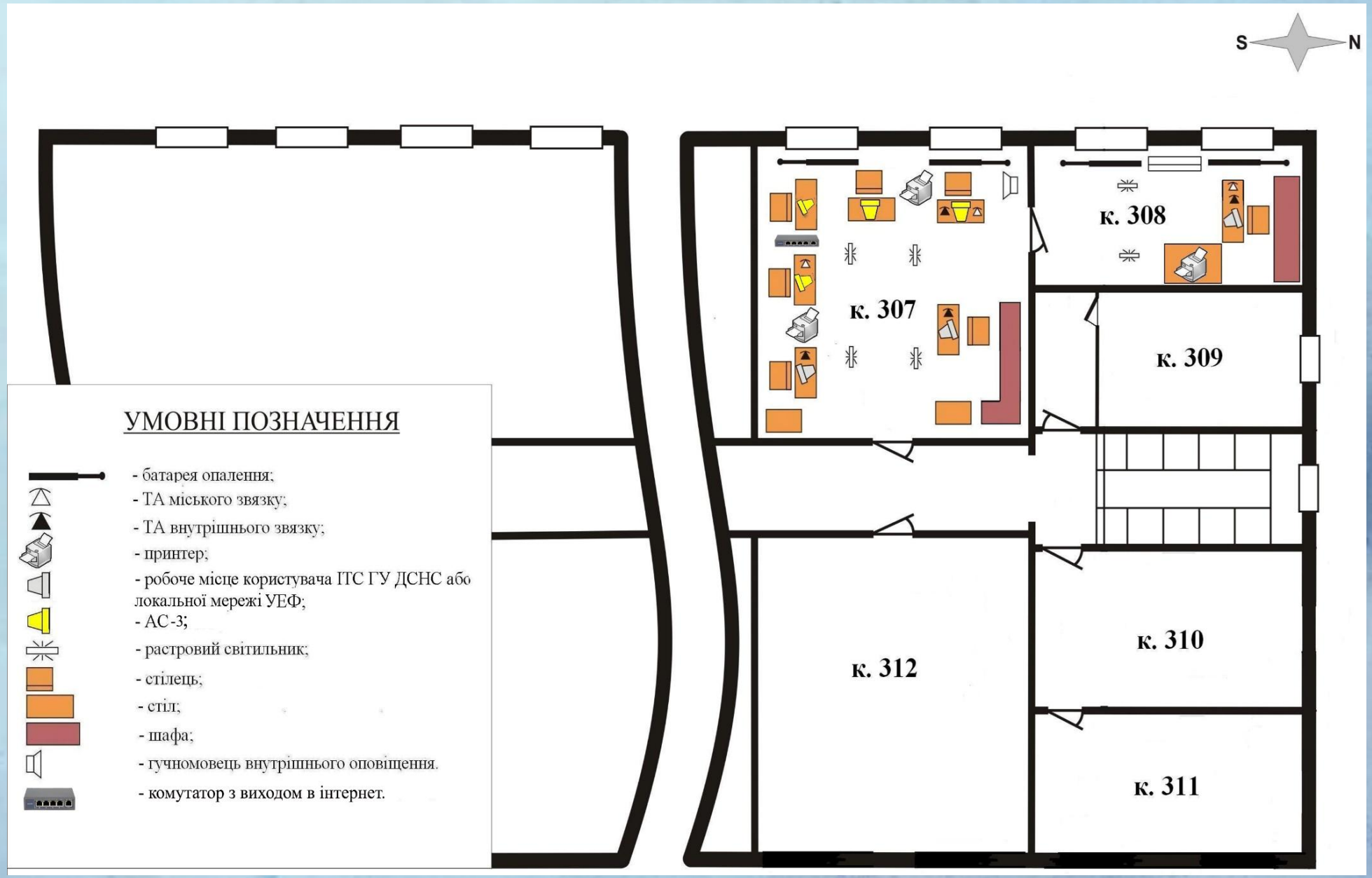
Обчислювальна система ЛОМ складається з наступних компонентів:

- комутатор ЛОМ (1 шт.);
- робочі станції користувачів ЛОМ (4 шт.).

ДОСЛІДЖЕННЯ ОБСТЕЖЕННЯ ФІЗИЧНОГО СЕРЕДОВИЩА



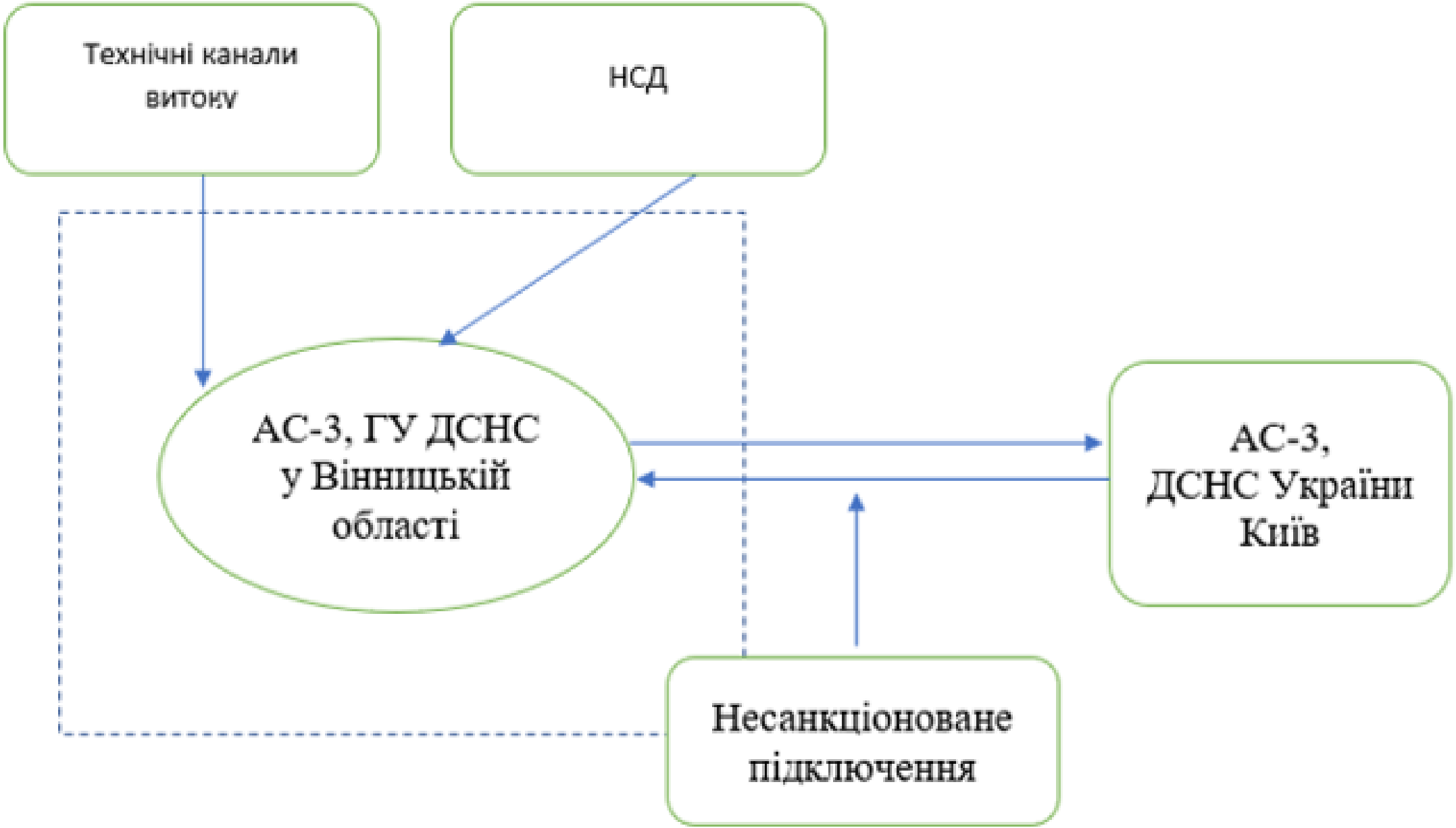
ГЕНЕРАЛЬНИЙ ПЛАН ОІД



СУКУПНІСТЬ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ

Апаратні засоби	Програмні засоби	Захисні перетворення	Організаційні засоби
Захист центрального процесора; Захист основної пам'яті; Захист зовнішньої пам'яті; Захист терміналів; Загальні методи захисту.	Ідентифікація користувача; Ідентифікація термінала; Захист файлів; Захист ОС; Допоміжні програми захисту.	Методи перестановки; Методи заміни; Адитивні методи; Добір та підготовка кадрів; Організація системи спостереження.	Будівництво та устаткування; Протипожежний захист; Збереження документів; Організація роботи в системі; Заходи захисту під час внесення змін.

Основні канали витоку інформації



ЗАХИСТ ВІД НЕСАНКЦІОНОВАНОГО ПІДКЛЮЧЕННЯ ЧЕРЕЗ МЕРЕЖУ ІНТЕРНЕТ

Між Головним управлінням ДСНС України у Вінницькій області та ДСНС України, яке знаходиться у м. Київ, через мережу інтернет постійно здійснюється передача інформації, необхідної для функціонування системи перерахунку державних коштів. Отже, одним з каналів витоку інформації є несанкціоноване підключення через мережу інтернет, оскільки між двома ОІД не створено безпечний канал передачі даних.

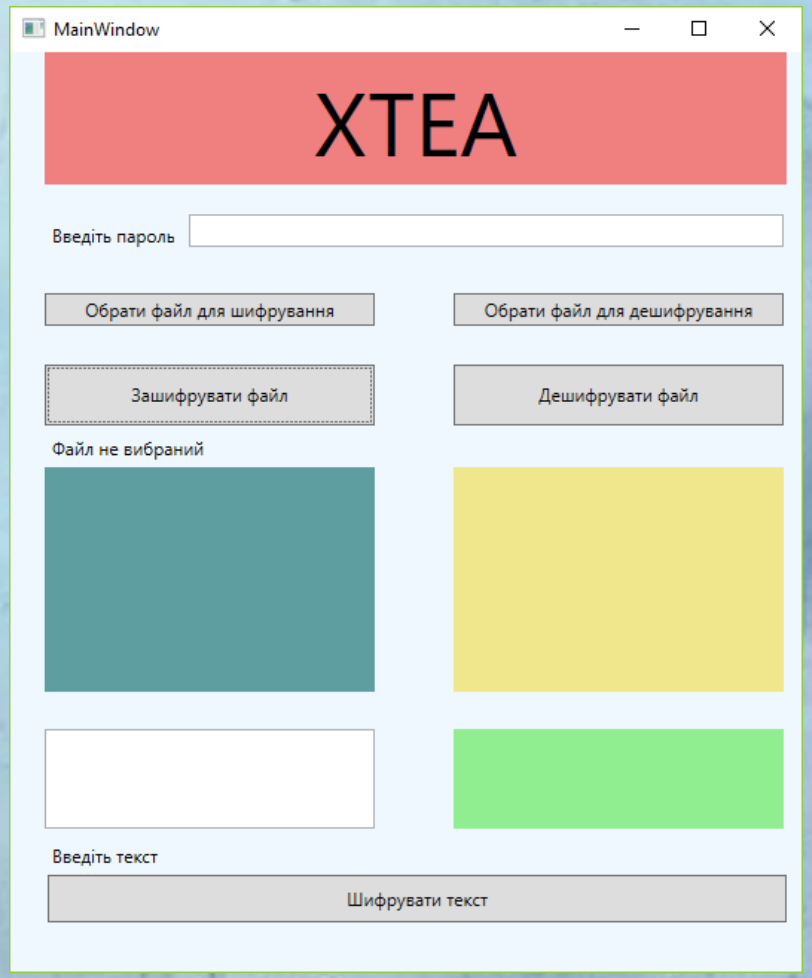
Ми пропонуємо застосування криптографічний метод захисту передачі документів від бухгалтерії Головного управління до ДСНС України і навпаки на основі розробленої програми криптографічного захисту, а саме криптографічного блокового шифру XTEA.

Реалізація роботи алгоритму

Блок програми, що забезпечує шифрування має виконувати наступні функції:	**Блок програми, що забезпечує дешифрування має виконувати наступні функції:**
1. перевірка та приведення до потрібного формату ключа, введеного користувачем; 2. доповнення вхідного повідомлення до необхідного розміру, відповідно до вимог криптографічного алгоритму XTEA; 3. формування послідовностей, що відповідають довжині блоку 64 біт та розміру підблоків 32 біт; 4. виконання 32 ітерацій шифрування схеми Фейстеля над кожним блоком даних; 5. повернення зашифрованих даних.	1. перевірка та приведення до потрібного формату ключа, введеного користувачем; 2. доповнення вхідного повідомлення до необхідного розміру; 3. формування послідовностей, що відповідають довжині блоку 64 біт та розміру підблоків 32 біт; 4. виконання 32 ітерацій дешифрування схеми Фейстеля над кожним блоком даних; 5. повернення дешифрованих даних.

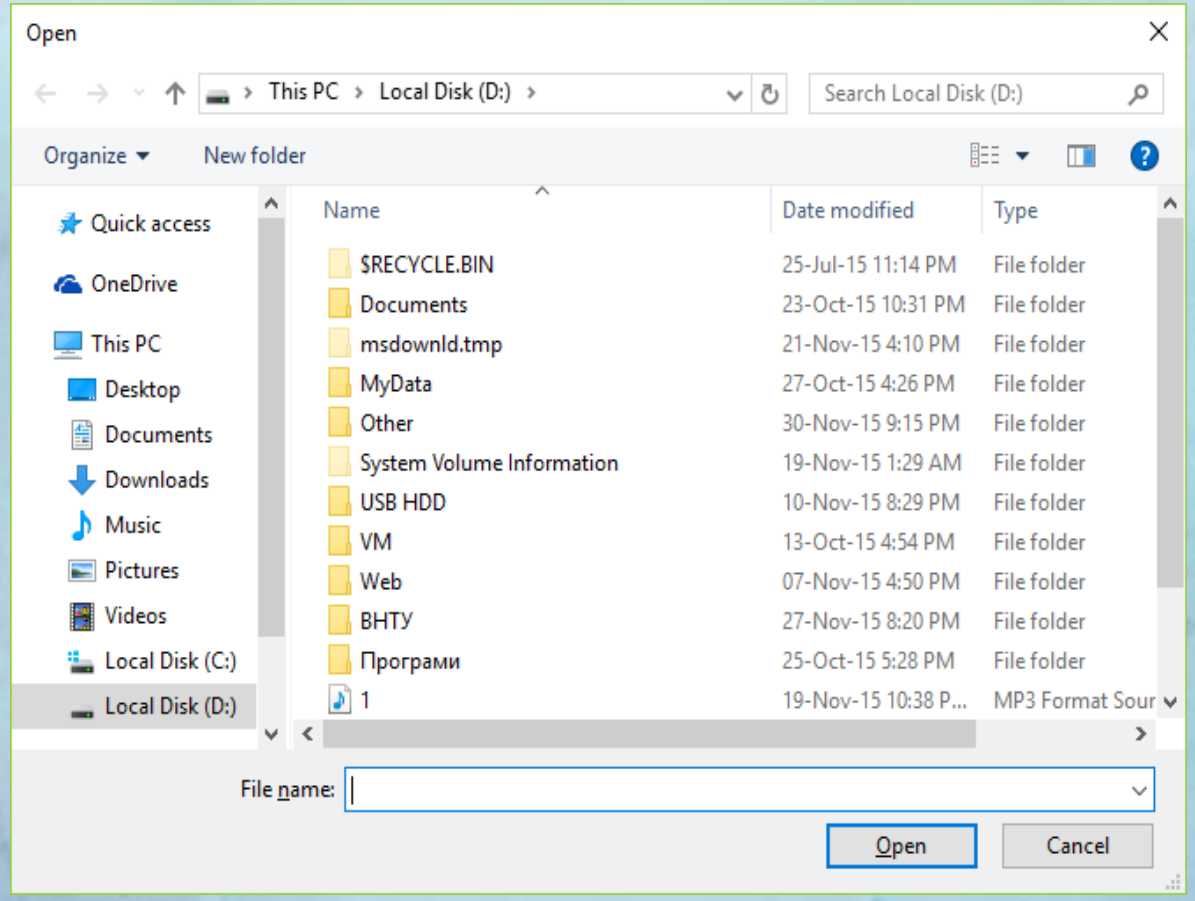
ПРАКТИЧНЕ ЗАСТОСУВАННЯ РОЗРОБЛЕНОГО ПРОГРАМНОГО КОДУ

Головне вікно програми

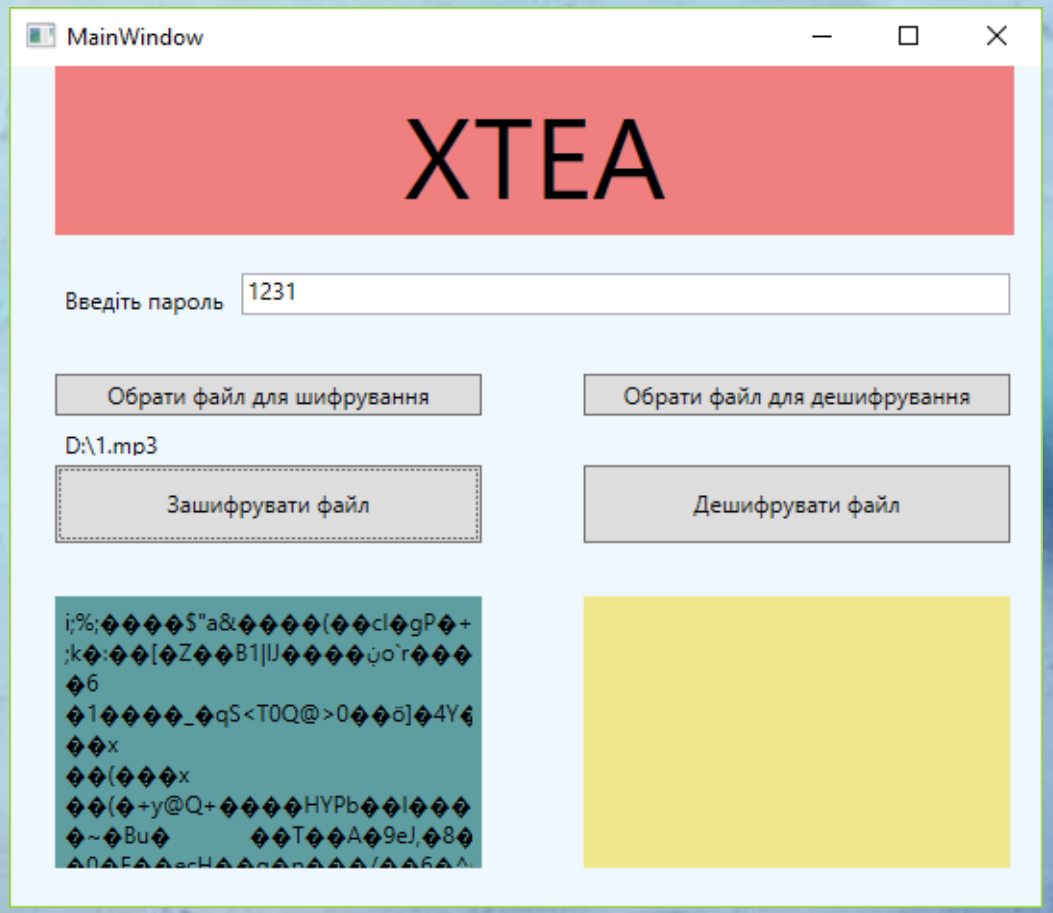


Відображення текстових повідомлень

Практичне застосування розробленого програмного коду



Вікно вибору файлу



Вікно програми після шифрування файлу

ВИСНОВКИ

- Дана робота є цінною для управління інформаційною безпекою в автоматизованих системах класу 3 в умовах передачі інформації з обмеженим доступом, що не становить державної таємниці через мережу інтернет, адже дозволяє передавати засекречену інформацію по каналах зв'язку між ДСНС України м. Київ та Головного управління ДСНС України у Вінницькій області, а також між іншими територіальними підрозділами за допомогою криптографічного захисту інформації.
- Розробка методики проведення первинної експертизи з подальшим створенням комплексної системи захисту інформації для бухгалтерії Головного управління ДСНС України у Вінницькій області, може застосовуватися у всіх підпорядкованих підрозділах ДСНС України, оскільки інформації та поставлені задачі, що обробляється у ОІД відповідають зазначеним видам у даній роботі.