Форма № Н-9.02

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ КОРАБЛЕБУДУВАННЯ
імені адмірала Макарова

Херсонська філія

Кафедра інформаційних технологій та фізико-математичних дисциплін

"Допущений до захисту"
Завідувач кафедри
д.т.н., доцент Гучек П.Й. "____"
_____ 2020 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційної роботи

на здобуття ступеня вищої освіти "магістр"

на тему:
«Дослідження технологій захисту відеоархіву від несанкціонованого доступу»

Виконав: студент VI курсу, групи 6157м спеціальності
122 - "Комп'ютерні науки", ОПП -
(шифр і назва спеціальності та освітньо-професійної програми)
"Інформаційні управляючі системи та технології"
Іванченко С.С.
(прізвище та ініціали)

Керівник к.т.н. Гайдаєнко О.В.
(прізвище та ініціали)

Рецензент Ширина С.М.
(прізвище та ініціали)

__.12 - 2020 року

Анотація

Дана робота присвячена дослідження методів захисту даних та аналіз існуючого програмного забезпечення для захисту відеоінформації від несанкціонованого доступу. Пояснювальна записка складається з вступу, чотирьох глав, висновків, списку використаної літератури.

Перша частина представляє собою дослідження методів та розробка проекту інформаційної системи, а також у рамках цієї частина виконано постановку задачі.

У рамках другої частини представлені аналіз та використання методу ієрархії для інформаційної системи.

У третій частині виконана розробка проектних рішень інформаційної системи, рішення з програмного забезпечення.

У четвертій частині представлені економічні розрахунки.

У п’ятій представлена частині охорона праці.

У шостій частині представлена охорона праці навколишнього середовища.

У висновках описується актуальність дослідження прийняття рішень для відділу постачання мережі магазину.

Робота представлена пояснювальною запискою на 106 сторінках тексту, який включає 19 рисунків, 4 таблиць.

Аннотация

Данная работа посвящена исследованию методов защиты данных и анализ сующего программного обеспечения для защиты видеоинформации от несанкционного доступа. Пояснительная записка состоит из введения, четырех глав, высновкив, списка использованной литературы.

Первая часть представляет собой исследование методов и разработка проекта информационной системы, а также в рамках этой часть выполнена постановку задачи.

В рамках второй части представлены анализ и использование метода иерархии для информационной системы.

В третьей части выполнена разработка проектных решений информационной системы, решение по программному обеспечению.

В четвертой части представлены экономические расчёты.

В пятой части представлена охрана труда.

В шестой части представлена охрана труда окружающей среды.

В выводах описывается актуальность исследования принятия решений для отдела снабжения сети магазина.

Работа представлена пояснительной запиской на 106 страницах текста, включает 19 рисунков, 4 таблиц.

Abstract

This paper is devoted to the study of data protection methods and analysis of existing software to protect video information from unauthorized access. The explanatory note consists of an introduction, four chapters, conclusions, and a list of references.

The first part is a study of methods and development of an information system project, as well as within this part the task is set.

The second part presents the analysis and use of the hierarchy method for the information system.

In the third part the development of design solutions of the information system, software solutions is performed.

The fourth part presents economic calculations.

The fifth part presents labor protection.

The sixth part presents the protection of the environment.

The conclusions describe the relevance of the decision-making study for the supply chain of the store network.

The work is presented by an explanatory note on 106 pages of text, which includes 19 figures, 4 tables.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

АРМ – автоматизоване робоче місце

БДК – база даних клієнтів

ВА – відеоархів

ВК – відеокамера

ВО – виконавче обладнання

ЗЖД – захищений журнал доступу

КЗЗ – комплекс засобів захисту

КЛ – клієнт

КМ – комутатор

КР – користувач

КТ – кабель-трос

МА – модуль аудиту

МАК – модуль автентифікації клієнтів

МВ – модуль відновлення

МВВК – модуль взаємодії з відеокамерами

МЕІ – модуль експорту та імпорту

МРД – модуль розмежування доступу

МРКД – модуль формування ключа доступу

ПА – програмний апарат

ПЗ – програмне забезпечення

ЖДС – жорсткий диск системи

СВ – система відеоспостереження

СІО – система інформаційного обміну

СР – сервер

СВК – система відеокамер

ВСТУП

Як правило для організації робіт використовуються апарати з аналоговими відеокамерами та цифровими.

В даний час пріоритетним є відеодокументування проведених робіт, але сучасні засоби надають можливість зберігання цієї інформації в незахищеному вигляді, що може спричинити за собою використання її зловмисниками. Тому данні треба зберігати на сервері у захищеному виді, і доступ до них повинні мати тільки авторизовані користувачі. Отже, існує необхідність у розробці ПЗ для захисту відеоархіву.

Метою дипломного проекту є розробка програмного забезпечення, що забезпечить захист відеоархіву охоронної системи лазерної сигналізації від несанкціонованого доступу. Для досягнення поставленої мети необхідно вирішити наступні задачі:

– описати можливі загрози інформаційній безпеці відеокомплексу охоронної системи лазерної сигналізації;
– розробити структуру програмного забезпечення для захисту;
– розробити алгоритмічне забезпечення;
– реалізувати програмне забезпечення та перевірити його працездатність.

1 ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ ДАНИХ ТА АНАЛІЗ ІСНУЮЧОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ЗАХИСТУ ВІДЕОІНФОРМАЦІЇ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

1.1 Структура відеокомплексу охоронної системи

Охоронна система (ОС) складається з системи датчиків (СД) та системи камер(СК), які з'єднані за допомогою бездротової мережі. Що забезпечує електроживлення СД та інформаційний обмін між ОС та СД.

ОС приймає керуючі сигнали від СН , які визначають маршрут руху апарату та режими роботи виконавчого обладнання (ВО).

Центральний комп'ютер (ЦК) необхідний для керування системою відеоспостереження (СВ) та ВО, а також доставку даних на СН через КТ.

Пристрої СН представлені сервером ОС , автоматизованими робочими місцями операторів (АРМ) ОС, палубними відеокамерами (ВК), відеоархівом (ВА) та комутатором (КМ). Обладнання СН та ОС з'єднано з сервером ОС за допомогою мережевого комутатора. Сервер необхіден для організації зв'язку ОС з обладнанням СН, керування апаратом, а відеоархів використовується для відеофіксації місії. АРМ призначені для керування виконавчим обладнанням ОС.

Відеоспостереження, зазвичай, організовано на базі цифрових мережевих відеокамер, що зменшить кількість необхідної апаратури та покращить інтеграцію системи відеоспостереження до системи інформаційного обміну (СІО). Систему відеоспостереження пропонується виділити в окремий сегмент мережі СІО, що зв'язаний з сервером за допомогою виділених каналів та ізольовані від інших сегментів системи. Інформаційний обмін між всіма елементами СІО забезпечується сервером з архівом. На даний елемент системи покладено завдання ретрансляції відео, яке отримано від ОС, забезпечення обміну голосовими даними між членами екіпажу, організації доступу віддалених клієнтів, які знаходяться в мережі Інтернет

до внутрішніх інформаційних ресурсів системи. Центральний сервер системи з'єднано з мережею Інтернет через маршрутизатор з функціями міжмережевого екрану. Такий підхід забезпечить захист сервера та локального сегменту СІО від мережевих атак, що націлені на зменшення доступності інформаційних ресурсів ОС локальним та віддаленим клієнтам. Інформаційний обмін з віддаленими клієнтами пропонується реалізувати з використанням технології віртуальних приватних мереж. При цьому механізми отримання доступу до інформаційних ресурсів СІО для клієнтів віддаленого та локального сегмента є ідентичними.

1.2 Аналіз загроз інформаційній безпеці відеокомплексу охоронної системи

Загрози інформаційній безпеці – це можливі випадкові або навмисні дії або події які можуть привести до порушення інформаційної безпеки і негативно впливали на систему і інформацію, яка в ній зберігається.

На сьогоднішній день існує більше ста позицій і різновидів загроз інформаційній системі. Важливо проаналізувати всі ризики за допомогою різних методик діагностики. На основі проаналізованих показників з їх деталізацією можна грамотно вибудувати систему захисту від загроз в інформаційному просторі

Класифікація вразливостей систем безпеки

Загрози інформаційної безпеки проявляються не самостійно, а через можливу взаємодію з найбільш слабкими ланками системи захисту, тобто через фактори уразливості. Загроза призводить до порушення діяльності систем на конкретному об'єкті-носії.

Основні вразливості виникають унаслідок дії наступних факторів:

– Недосконалість програмного забезпечення, апаратної платформи.

– Різні характеристики будови автоматизованих систем в інформаційному потоці.

– Частина процесів функціонування систем є неповноцінною.

– Неточність протоколів обміну інформацією та інтерфейсу.

– Складні умови експлуатації і розташування інформації.

Найчастіше джерела загрози запускаються з метою отримання незаконної вигоди внаслідок заподіяння шкоди інформації. Але можливо і випадкова дія загроз через недостатні міри захисту і масового дії загрозливого фактора.

Існує поділ вразливостей за класами, вони можуть бути:

– об'єктивними;

– випадковими;

– суб'єктивними.

Випадкові види вразливостей

Ці фактори залежать від непередбачених обставин і особливостей оточення інформаційного середовища. Їх практично неможливо передбачити в інформаційному просторі, але важливо бути готовим до їх швидкого усунення. Усунути такі неполадки можна за допомогою проведення інженерно-технічного розгляду та відповідного удару, завданого загрозі інформаційній безпеці:

1. Збої і відмови роботи систем:

– внаслідок несправності технічних засобів на різних рівнях обробки та зберігання інформації (в тому числі і тих, що відповідають за працездатність системи і за контроль доступу до неї);

– несправності і старіння окремих елементів (розмагнічування носіїв даних, таких як дискети, кабелі, з'єднувальні лінії і мікросхеми);

– збої різного програмного забезпечення, яке підтримує всі ланки в ланцюзі зберігання і обробки інформації (антивіруси, прикладні і сервісні програми);

– перебої в роботі допоміжного обладнання інформаційних систем (неполадки на рівні електропередачі).

2. Фактори, які послаблюють інформаційну безпеку:

– пошкодження комунікацій на зразок водопостачання або електропостачання, а також вентиляції, каналізації;

– несправності в роботі захисних пристроїв (паркани, перекриття в будинку, корпусу обладнання, де зберігається інформація).

Об'єктивні різновиди вразливостей

Цей вид безпосередньо залежить від технічного побудови обладнання на об'єкті, що вимагає захисту, і його характеристик. Повноцінне позбавлення від цих чинників неможливо, але їх часткове усунення досягається за допомогою інженерно-технічних прийомів, наступними способами:

1. Зміни, пов'язані з технічними засобами випромінювання:

– електромагнітні методики (побічні варіанти випромінювання і сигналів від кабельних ліній, елементів тех. засобів);

– звукові варіанти (акустичні або з додаванням вібросигналів);

– електричні (прослизання сигналів в ланцюжки електричної мережі, за наведенням на лінії і провідники, по нерівномірного розподілу струму).

2. Інформаційні керуючі:

– шкідливі ПО, нелегальні програми, технологічні виходи з програм, що об'єднується терміном «програмні закладки»;

– закладки апаратури - фактори, які впроваджуються безпосередньо в телефонні лінії, в електричні мережі або просто в приміщення.

3. Ті, що створюються особливостями об'єкта, що знаходиться під захистом:

– розташування об'єкта (видимість і відсутність контрольованої зони навколо об'єкту інформації, наявність вібро або звуковідбивальних елементів навколо об'єкта, наявність віддалених елементів об'єкта);

– організація каналів обміну інформацією (застосування радіоканалів, оренда частот або використання загальних мереж).

4. Ті, що залежать від особливостей елементів-носіїв:

– деталі, що володіють електроакустичними модифікаціями (трансформатори, телефонні пристрої, мікрофони і гучномовці, котушки індуктивності);

– речі, які підпадають під вплив електромагнітного поля (носії, мікросхеми та інші елементи).

Суб'єктивні уразливості

Цей підвид в більшості випадків являє собою результат неправильних дій співробітників на рівні розробки систем зберігання і захисту інформації. Тому усунення таких факторів можливо за допомогою методик з використанням апаратури і ПО:

1. Неточності і грубі помилки, що порушують інформаційну безпеку:

– на етапі завантаження готового програмного забезпечення або попередньої розробки алгоритмів, а також в момент його використання (можливо під час щоденної експлуатації, під час введення даних);

– на етапі управління програмами і інформаційними системами (складності в процесі навчання роботі з системою, настройки сервісів в індивідуальному порядку, під час маніпуляцій з потоками інформації);

– під час користування технічної апаратурою (на етапі включення або виключення, експлуатації пристроїв для передачі або отримання інформації).

2. Порушення роботи систем в інформаційному просторі:

– режиму захисту особистих даних (проблему створюють звільнені працівники або діючі співробітники в неробочий час, вони отримують несанкціонований доступ до системи);

– режиму збереження і захищеності (під час отримання доступу на об'єкт або до технічних пристроїв);

– під час роботи з техпристроями (можливі порушення в енергозбереженні або забезпеченні техніки);

– під час роботи з даними (перетворення інформації, її збереження, пошук і знищення даних, усунення браку і неточностей).

Ранжування вразливостей

Кожна вразливість повинна бути врахована і оцінена фахівцями. Тому важливо визначити критерії оцінки небезпеки виникнення загрози і ймовірності

поломки або обходу захисту інформації. Показники підраховуються за допомогою застосування ранжирування. Серед всіх критеріїв виділяють три основних:

– Доступність - це критерій, який враховує, наскільки зручно джерела загроз використовувати певний вид уразливості, щоб порушити інформаційну безпеку. У показник входять технічні дані носія інформації (на кшталт габаритів апаратури, її складності і вартості, а також можливості використання для злому інформаційних систем неспеціалізованих систем і пристроїв).

– Фатальність - характеристика, яка оцінює глибину впливу уразливості на можливості програмістів впоратися з наслідками створеної загрози для інформаційних систем. Якщо оцінювати тільки об'єктивні уразливості, то визначається їх інформативність - здатність передати в інше місце корисний сигнал з конфіденційними даними без його деформації

– Кількість - характеристика підрахунку деталей системи зберігання та реалізації інформації, яким притаманний будь-який вид уразливості в системі.

Кожен показник позначається символом (Коп) f, і його можна розрахувати за допомогою формули. Максимальна оцінка сукупності вразливостей - 125, це число і знаходиться в знаменнику. А в чисельнику фігурує твір з К1, К2 і К3.

1.2.1 Джерела, які загрожують інформаційній безпеці

Описуючи класифікацію загроз інформаційної безпеки, то можна виділити кілька класів. Поняття класів обов'язково, адже воно спрощує і систематизує всі фактори без винятку. В основу входять такі параметри, як:

1. Ранг навмисності здійснення втручання в інформаційну систему захисту:

– загроза, яку викликає недбалість персоналу в інформаційному вимірі;

– загроза, ініціатором якої є шахраї, і роблять вони це з метою особистої вигоди.

2. Характеристики появи:

– загроза інформаційній безпеці, яка провокується руками людини і є штучною;

– природні загрозливі фактори, непідконтрольні інформаційних систем захисту і викликає стихійне лихо.

3. Класифікація безпосередньої причини загрози. Винуватцем може бути:

– людина, яка розголошує конфіденційну інформацію, орудуючи за допомогою підкупу співробітників компанії;

– природний фактор, що приходить у вигляді катастрофи або локального лиха;

– програмне забезпечення з застосуванням спеціалізованих апаратів або впровадження шкідливого коду в тех. засоби, що порушує функціонування системи;

– випадкове видалення даних, санкціоновані програмно-апаратні фонди, відмова в роботі операційної системи.

4. Ступінь активності дії загроз на інформаційні ресурси:

– в момент оброблення даних в інформаційному просторі (дія розсилок від вірусних утиліт);

– в момент отримання нової інформації;

– незалежно від активності роботи системи зберігання інформації (в разі розкриття шифрів або криптографічного захисту інформаційних даних).

Несанкціонований доступ - один з найбільш «популярних» методів комп'ютерних правопорушень. Тобто особистість, яка здійснює несанкціонований доступ до інформації людини, порушує правила, які зафіксовані політикою безпеки. При такому доступі відкрито користуються похибками в системі захисту і проникають до ядра інформації. Некоректні настройки і установки методів захисту також збільшують можливість несанкціонованого доступу. Доступ і загроза інформаційній безпеці відбуваються як локальними методами, так і спеціальними апаратними установками.

Для відеоархіву охоронної системи загрози інформаційній безпеці поділяються на:

– копіювання інформації;

– знищення інформації;
– спотворення інформації;
– мережеві атаки;
– вивід комп’ютерної системи з ладу;
– програмна закладка.

Скопіювати інформацію зловмисник може декількома способами: отримавши доступ до інтернет трафіку, скопіювати інформацію на змінний носій отримавши доступ безпосередньо до відеосерверу, за допомогою читання ПЕМВН, викравши НЖМД з відеоархівом, а також шантажем виманити інформацію у авторизованого користувача.

Зловмисник може знищити інформацію введенням обладнання до аварійного стану або фізичним доступом до сервера. Фізичне знищення системи може бути здійснено за допомогою забезпечення підвищення напруг і виходу електричних сигналів за допустимі межі.

Інформація, що отримується відеосервером може бути спотворена несанкціонованим доступом зловмисника до сервера і засобів інформаційного обміну або викривлена через неправильну узгодженостість компонентів системи або спотворена на шляху до відеоархіву.

Деякі мережеві атаки використовуються для отримання інформації, розширення прав доступу на вузлі, а інші ж для виведення системи з ладу, щоб зменшити її доступність.

– Отримавши доступ до СІО або сервера зловмисник може впровадити в систему програму або фрагмент програми, яка дозволить здійснити несанкціонований доступ до ресурсів системи і використовувати її для своїх потреб.

1.3 Способи та засоби порушення конфіденційності інформації

1.3.1 Основні методи реалізації загроз інформаційної безпеки

До основних напрямків реалізації зловмисником інформаційних загроз на локальній, ізольованій або включеній в мережу КС можна віднести наступні:

– безпосереднє звернення до об'єктів доступу (зловмисник намагається отримати доступ до об'єктів);

– створення програмних і технічних засобів, що виконують звернення до об'єктів доступу;

– модифікація засобів захисту, що дозволяє реалізувати загрози інформаційній безпеці;

– впровадження в технічні засоби програмних або технічних механізмів, що порушують структуру і функції КС.

Отримання доступу до інформації зазвичай здійснюється зловмисником в кілька етапів. На першому етапі відбувається отримання доступу до програмних засобів, а на другому етапі вирішуються завдання впровадження програмних засобів з метою розкрадання програм і даних.

1.4 Основи протидії конфіденційності інформації

Вимоги безпеки визначають набір засобів захисту КС на всіх етапах її існування: від розробки специфікації на проектування програмних засобів до їх списання. НСД може бути попереджений або істотно ускладнений при організації наступного комплексу заходів:

- ідентифікація та аутентифікація користувачів;
- моніторинг несанкціонованих дій – аудит;
- розмежування доступу до КС;
- криптографічні методи приховування інформації;
- захист КС при роботі в мережі.

Організація надійного захисту КС неможлива, за допомогою тільки апаратно-програмних засобів. Дуже важливим є адміністративний контроль роботи КС.

Основні завдання адміністратора з підтримки засобів захисту полягають в наступному:

– постійний контроль коректності функціонування КС та її захисту;

– регулярний перегляд журналів реєстрації подій;

– Організація і підтримка адекватної політики безпеки;

– інструктування користувачів ОС про зміни в системі захисту, правильного вибору паролів і т. д;

– регулярне створення і оновлення резервних копій програм і даних;

– постійний контроль змін конфігураційних даних.

Розглянемо докладніше найбільш часто використовувані методи захисту і принципи їх дії.

1.4.1 Методи розмежування доступу

Основним способом заборони несанкціонованого доступу до ресурсів обчислювальних систем є підтвердження автентичності користувачів і розмежування доступу до інформаційних ресурсів, що включає наступні етапи:

– ідентифікація;

– встановлення автентичності (аутентифікація);

– визначення повноважень для подальшого контролю і розмежування доступу до комп'ютерних ресурсів.

Ідентифікація необхідна для вказівки комп'ютерній системі унікального ідентифікатора користувача, що звертається до неї. Ідентифікатор може являти собою будь-яку послідовність символів і повинен бути заздалегідь зареєстрований в системі адміністратора служби безпеки. В процесі реєстрації заноситься наступна інформація:

– прізвище, ім'я, по батькові (при необхідності інші характеристики користувача);

– унікальний ідентифікатор користувача;

– ім'я процедури встановлення автентичності;

– еталонна інформація для підтвердження автентичності (наприклад, пароль);

– обмеження на використовувану еталонну інформацію (наприклад, час дії пароля);

– повноваження користувача по доступу до комп'ютерних ресурсів.

Встановлення автентичності (аутентифікація) полягає в перевірці істинності повноважень користувача.

Загальна схема ідентифікації та встановлення автентичності користувача представлена на рис. 1.2.

Для особливо надійного впізнання при ідентифікації використовуються технічні засоби, що визначають індивідуальні характеристики людини (голос, відбитки пальців, структура зіниці). Однак такі методи вимагають значних витрат і тому використовуються рідко. Найбільш масово використовуваними є парольні методи перевірки автентичності користувачів. Паролі можна розділити на дві групи: прості і динамічно змінюються.

Рис 1.2 – Загальна схема ідентифікації та встановлення автентичності користувача

Простий пароль не змінюється від сеансу до сеансу протягом встановленого періоду його існування.

У другому випадку пароль змінюється за правилами, що визначаються використовуваним методом. Виділяють наступні методи реалізації динамічно змінюються паролів:

– методи модифікації простих паролів. Наприклад, випадкова вибірка символів пароля і одноразове використання паролів;

– метод "запит-відповідь", заснований на пред'явленні користувачеві випадково обираних запитів з наявного масиву;

– функціональні методи, засновані на використанні деякої функції F з динамічно змінними параметрами (дата, час, день тижня і ін.), за допомогою якої визначається пароль.

Для захисту від несанкціонованого входу в комп'ютерну систему використовуються як загальносистемні, так і спеціалізовані програмні засоби захисту.

Після ідентифікації та аутентифікації користувача система захисту повинна визначити його повноваження для подальшого контролю санкціонованого доступу до комп'ютерних ресурсів (розмежування доступу). В якості комп'ютерних ресурсів розглядаються:

– програма;
– зовнішня пам'ять (файли, каталоги, логічні диски);
– інформація, розмежована за категоріями в базах даних;
– оперативна пам'ять;
– час (пріоритет) використання процесора;
– порти введення-виведення;
– зовнішні пристрої.

Розрізняють такі види прав користувачів по доступу до ресурсів:

– загальне (повне надання ресурсу);

– функціональне або часткове;

– тимчасовий.

Найбільш поширеними способами розмежування доступу є:

– розмежування за списками (користувачів або ресурсів);

– використання матриці встановлення повноважень (рядки матриці – ідентифікатори користувачів, стовпці – ресурси комп'ютерної системи);

– розмежування за рівнями секретності і категоріям (наприклад, загальний доступ, конфіденційно, таємно);

– парольное розмежування.

1.4.2 Криптографічні методи захисту даних

Криптографічні методи захисту інформації - це спеціальні методи шифрування, кодування або іншого перетворення інформації, в результаті якого її зміст стає недоступним без пред'явлення ключа криптограми і зворотного перетворення. Криптографічний метод захисту, безумовно, самий надійний метод захисту, так як охороняється безпосередньо сама інформація, а не доступ до неї (наприклад, зашифрований файл не можна прочитати навіть у випадку крадіжки носія). Даний метод захисту реалізується у вигляді програм або пакетів програм.

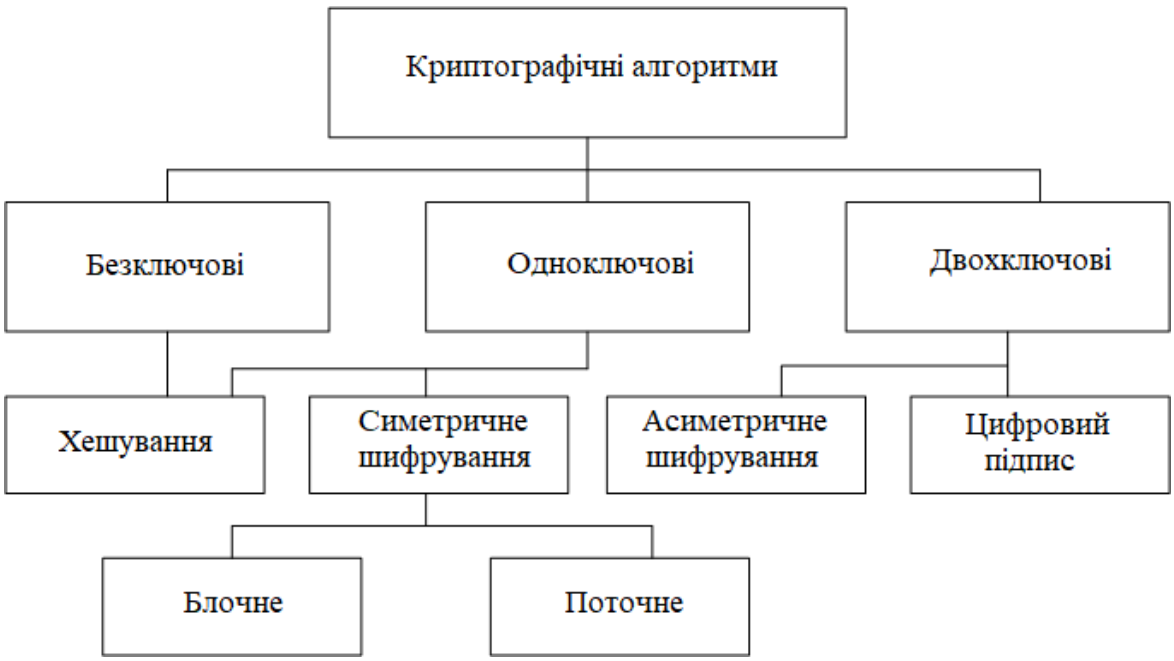

Рисунок 1.3 – Види криптографічних алгоритмів

Симетричні алгоритми шифрування – спосіб шифрування, в якому для шифрування і дешифрування застосовується один і той же криптографічний ключ. До винаходу схеми асиметричного шифрування єдиним існуючим способом було симетричне шифрування. Ключ алгоритму повинен зберігатися в секреті обома сторонами. Алгоритми шифрування і дешифрування даних широко застосовуються в комп'ютерній техніці в системах приховування конфіденційної і комерційної інформації від не коректного використання сторонніми особами. Головним принципом у них є умова, що та приймає заздалегідь знають алгоритм шифрування, а також ключ до повідомлення, без яких інформація є всього лише набір символів, що не мають сенсу. Симетричні криптоалгоритми виконують перетворення невеликого (1 біт або 32-128 біт) блоку даних в залежності від ключа таким чином, що прочитати оригінал повідомлення можна тільки знаючи цей секретний ключ.

Симетричні криптоалгоритми діляться на:

– Скремблери.
– Блокові шифри.

Скремблерами називаються програмні або апаратні реалізації алгоритму, що дозволяють шифрувати побітно безперервні потоки інформації. Сам скремблер представляє із себе набір бітів, що змінюються на кожному кроці по певному алгоритму. Після виконання кожного чергового кроку на його виході з'являється біт, що шифрує, – або 0, або 1, що накладається на поточний біт інформаційного потоку операцією XOR («побітне виключаюче АБО»). Основним недоліком алгоритмів скремблювання є їхня нестійкість до фальсифікації.

Блокові шифри в ході своєї роботи роблять перетворення блоку вхідної інформації фіксованої довжини і одержують результуючий блок того ж обсягу, але недоступний для прочитання стороннім особам, що не володіють ключем.

Класичні приклади симетричних алгоритмів шифрування:

- Проста перестановка
- Одиночна перестановка по ключу
- Подвійна перестановка
- Перестановка «Магічний квадрат»
- Проста перестановка

Проста перестановка без ключа-один з найпростіших методів шифрування. Повідомлення записується в таблицю по стовпцях. Після того, як відкритий текст записаний колонками, для утворення шифртексту він зчитується по рядках. Для використання цього шифру відправнику і одержувачу потрібно домовитися про загальний ключ у вигляді розміру таблиці. Об'єднання букв в групи не входить в ключ шифру і використовується лише для зручності запису несмислового тексту.

Одиночна перестановка по ключу

Більш практичний метод шифрування, званий одиночною перестановкою по ключу, дуже схожий на попередній. Він відрізняється лише тим, що колонки таблиці переставляються за ключовим словом, фразою або набору чисел довжиною в рядок таблиці.

Подвійна перестановка

Для додаткової скритності можна повторно шифрувати повідомлення, яке вже було зашифровано. Цей спосіб відомий під назвою подвійна перестановка. Для цього розмір другої таблиці підбирають так, щоб довжини її рядків і стовпців відрізнялися від довжин в першій таблиці. Найкраще, якщо вони будуть взаємно простими. Крім того, в першій таблиці можна переставляти стовпці, а в другому рядку. Нарешті, можна заповнювати таблицю зигзагом, змійкою, по спіралі або якимось іншим способом. Такі способи заповнення таблиці якщо і не посилюють стійкість шифру, то роблять процес шифрування набагато більш цікавим.

Перестановка «Магічний квадрат»

Магічними квадратами називаються квадратні таблиці з вписаними в їх клітини послідовними натуральними числами від 1, які дають у сумі по кожному стовпцю, кожному рядку і кожної діагоналі одне і те ж число. Подібні квадрати широко застосовувалися для вписування шифрованого тексту по наведеній в них нумерації. Якщо потім виписати вміст таблиці по рядках, то виходила шифровка перестановкою букв. На перший погляд здається, ніби магічних квадратів дуже мало. Проте, їх число дуже швидко зростає зі збільшенням розміру квадрата. Так, існує лише один магічний квадрат розміром 3 x 3, якщо не брати до уваги його повороти. Магічних квадратів 4 x 4 налічується вже 880, а число магічних квадратів розміром 5 x 5 близько 250000. Тому магічні квадрати великих розмірів могли бути доброю основою для надійної системи шифрування того часу, тому що ручний перебір всіх варіантів ключа для цього шифру був немислимий.

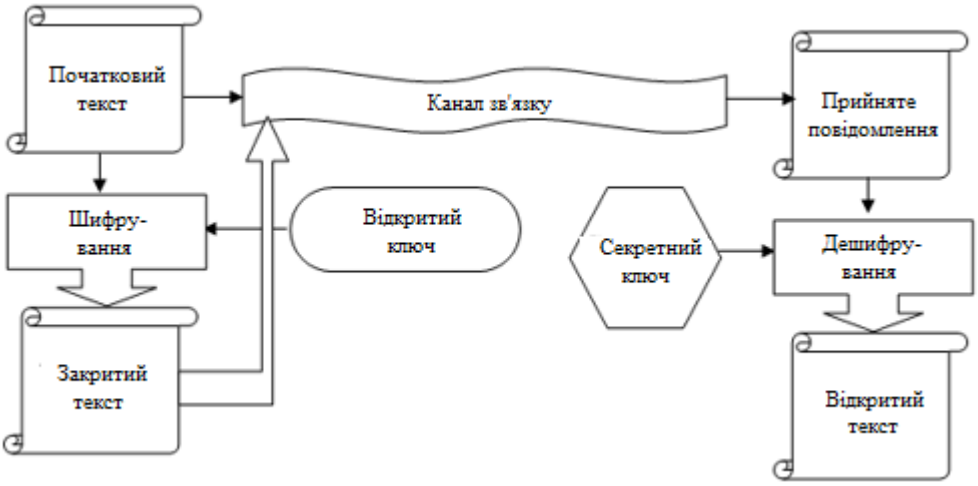

Рисунок 1.4 – Схема побудови симетричних криптосистем

До симетричних методів шифрування відносять такі алгоритми: Blowfish, DES, 3DES, CAST, AES, ГОСТ.

Алгоритм шифрування Blowfish заснований в 1993 році Брюсом Шнаєром. У загальному випадку алгоритм складається з двох етапів-розширення ключа і шифрація / дешифрація вихідних даних. Складна схема вироблення ключа сильно ускладнює атаку на алгоритм, якщо намагатися зламати її методом перебору, однак робить його непридатним для використання в системах, де ключ часто змінюється, і на кожному ключі шифрується невеликі за обсягом дані. Алгоритм найкраще підходить для систем, в яких на одному і тому ж ключі шифруються великі масиви даних.

Алгоритм шифрування DES заснований в 1975 році фірмою IBM. З 1977 по 2001 р. був Федеральним стандартом шифрування США. Симетричний алгоритм шифрування, в якому використовується один ключ, як одержувача, так і відправника, тобто цей ключ використовується як для розшифрування, так і для шифрування. DES має блоки по 64 біт і 16 циклову структуру мережі Фейстеля, для шифрування використовує ключ довжиною 56 біт. Алгоритм використовує комбінацію нелінійних S-блоки і лінійних перетворень. Основний недолік —

розмір ключа всього 56 біт, що недостатньо для сучасного рівня розвитку комп'ютерів.

Алгоритм шифрування Triple DES (3DES) — симетричний блоковий шифр, створений в 1978 році на основі алгоритму DES, з метою усунення головного недоліку останнього — малої довжини ключа 56 біт), який може бути зламаний методом повного перебору. Швидкість роботи 3DES в 3 рази нижче, ніж у DES, але криптостійкість набагато вище. 3DES є простим способом усунення недоліків DES
.

Алгоритм шифрування CAST є в певному сенсі аналогом DES. В основі цього алгоритму лежить шість S блоків з 8-бітовим входом і 32-бітовим виходом. Алгоритм складний і залежить від реалізації. Головною особливістю алгоритму CAST є те, що блоки не фіксуються. Використовуються ключі 128 і 256 біт.

Алгоритм шифрування AES (Rijndael) розроблений в 1997 році і на даний момент є Федеральним стандартом шифрування США. В основі цього алгоритму лежить симетричний блоковий шифр який працює з блоками даних довжиною 128 біт і використовує ключі довжиною 128, 192 і 256 біт. Алгоритм може працювати і з іншими довжинами блоків і ключів, але вони в стандарт не увійшли. Для шифрування в алгоритмі AES застосовуються наступні процедури перетворення даних: ExpandKey-обчислення раундних ключів для всіх раундів; SubBytes-підстановка байтів за допомогою таблиці підстановок; ShiftRows-циклічний зсув рядків у формі на різні величини; MixColumns-змішування даних всередині кожного стовпця форми; AddRoundKey-складання ключа раунду з формою.

Алгоритм шифрування ГОСТ заснований в 1989 році в СРСР і в результаті став Федеральним стандартом шифрування Російської Федерації. В основі алгоритму лежить мережа Фейстеля. Використовує 128 бітний ключ шифрування і є надійним. Швидкодія досить низька, але дозволяє збільшити швидкість роботи за рахунок можливості зміни налаштувань зі зниженням криптостійкості.

Симетрична система захисту має наступні переваги.

1. Висока швидкість і простота реалізації.

2. Для забезпечення стійкості шифру використовується мала довжина ключа.

До недоліків відноситься наступне:

1. Складність управління ключами у великій мережі.
2. Складність обміну ключами.
3. Потреба в пошуку надійного каналу для передачі ключа сторонам.
4. Неможливість використання для цифрового підпису, сертифікатів.

Для компенсації недоліків використовується комбінована схема, в якій за допомогою асиметричного шифрування передається ключ, що використовується для дешифрування. Він передається за допомогою симетричного шифрування.

Таблиця 1.1 – Огляд симетричних методів шифрування

Назва алгоритму	Розмір ключа, біт	Розмір блоку, біт	Кількість циклів	Тип (мережа)	Витрати на підбір ключа MIPS х років
Blowfish	32-448	64	16	Фейстеля	Немає даних
DES	56	64	16	Фейстеля	$5*10^2$
3DES	112/168	64	48	Фейстеля	10^{18}
CAST	40-256	64/128	12/48	Фейстеля	
AES	128/192/256	128	10/12/14	Квадрат	Немає даних
ГОСТ	256	64	32	Фейстеля	$1.84*10^{63}$

Асиметричні алгоритми шифрування – алгоритми шифрування, які використовують різні ключі для шифрування та розшифрування даних. Головне досягнення асиметричного шифрування в тому , що воно дозволяє людям, що не мають існуючої домовленості про безпеку, обмінюватися секретними повідомленнями. Необхідність відправникові й одержувачеві погоджувати таємний ключ по спеціальному захищеному каналі цілком відпала. Процедура шифрування обрана так, що вона необоротна навіть по відомому ключу шифрування. Тобто, знаючи ключ шифрування й зашифрований текст, неможливо відновити вихідне

повідомлення – прочитати його можна тільки за допомогою другого ключа – ключа дешифрування. А раз так, то ключ шифрування для відправлення листів якій-небудь особі можна взагалі не приховувати – знаючи його однаково неможливо прочитати зашифроване повідомлення. Тому, ключ шифрування називають в асиметричних системах “відкритим ключем”, а от ключ дешифрування одержувачеві повідомлень необхідно тримати в секреті – він називається “закритим ключем”. Алгоритми шифрування й дешифрування створюються так, щоб знаючи відкритий ключ, неможливо було обчислити закритий ключ.

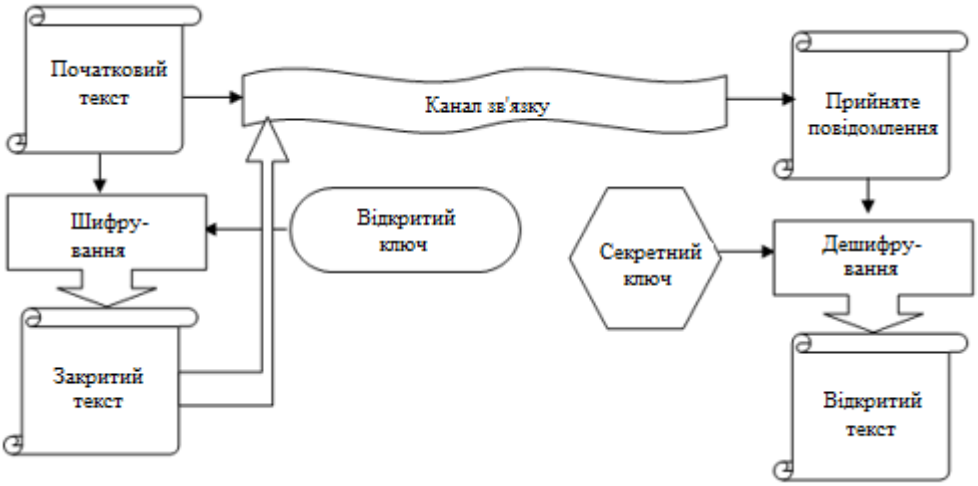

Рисунок – 1.4 Схема асиметричного алгоритму шифрування

До асиметричних відносять: RSA, El-Gamal.

Алгоритм шифрування RSA (Rivast, Shamir і Adelman, 1977 рік) припускає, що надіслане закодоване повідомлення може бути прочитане тільки адресатом. У цьому алгоритмі використовується два ключа-відкритий і закритий. Даний алгоритм привабливий також у разі, коли велике число суб'єктів повинно спілкуватися за схемою все-з усіма.

Алгоритм шифрування El-Gamal заснований в 1985 році Ель-Гамалем. Алгоритм може бути використаний для вирішення всіх трьох основних завдань: для шифрування даних, для формування цифрового підпису і для узгодження загального ключа. Крім того, можливі модифікації алгоритму для схем перевірки

пароля, докази ідентичності повідомлення й інші варіанти. Безпека цього алгоритму, так само як і алгоритму Діффі-Хеллмана, заснована на труднощі обчислення дискретних логарифмів. Цей алгоритм фактично використовує схему Діффі-Хеллмана, щоб сформувати загальний секретний ключ для абонентів, що передають один одному повідомлення, і потім повідомлення шифрується шляхом множення його на ключ.

Застосування пари відкритий-закритий ключ можна використовувати як:

1. Самостійний засіб захисту інформації.

2. Засіб розподілу ключів.

3. Засоби аутентифікації користувачів.

Має такі переваги:

1. Збереження секретного ключа в надійному місці, замість якого по відкритому каналу передається відкритий.

2. Ключ дешифрування відомий тільки одній стороні.

3. У великій асиметричній системі використовуйте меншу кількість ключів на відміну від симетричної.

У таких алгоритмах складно внести будь-які зміни. Подібна система має довгі ключі. Якщо симетричний ключ має розмір 128 Біт, то ключ RSA - 2304 Біт. Через це страждає швидкість розшифровування-вона в 2-3 рази повільніше. Для розшифровки потрібні великі обчислювальні ресурси.

Таблиця 1.2 – Асиметричні методи шифрування

Назва методу	Ключ	Метод злому	Криптостійкість, MIPS	Примітка
RSA	До 4096 біт	Факторизація великих простих чисел	2,7*1028 для ключа 1300 біт	Включений до багатьох стандартів
El-Gamal	До 4096 біт	Знаходження дискретного логарифма в кінцевому полі	При одинаковій довжині ключа криптостійкість рівна RSA	Використовується в алгоритмі цифрового підпису DSA-стандарту DSS

Криптографічна хеш-функція-особливо значущий базовий елемент, застосовуваний у багатьох криптографічних протоколах і алгоритмах. Вона, як правило, використовується для захисту інформації. Хеш-функція вилучає дані довільного об'єму, кодує їх і відправляє рядок, розмір якої має строго встановлену довжину.

Правильна криптографічна хеш-функція містить в собі такі особливо важливі характеристики:

– повинна вміти переробляти інформацію будь-якого обсягу, стискаючи дані до певного, фіксованого розміру;

– зобов'язана виключати можливість появи "колізій", тобто повторення хешу для двох абсолютно різних повідомлень;

– повинна виключати можливість відновлення початкових даних за допомогою математичних обчислень;

– повинна мати відкритий алгоритм, що надає можливість зробити аналіз криптостійкості;

– при будь-якому коригуванні вхідних даних, хеш повинен видозмінюватися;

– обробка даних не повинна вимагати значних обчислювальних ресурсів і часу.

Застосування криптографічних хеш-функцій у створенні електронного підпису

Цифровий підпис – інформація, яка захищена секретним ключем і прив'язана до вихідного тексту. Для перевірки достовірності підпису використовується відкритий ключ, за допомогою якого розшифровується підписаний текст. У тому випадку, якщо розкриті дані аналогічні вихідному тексту, підпис вважається вірною.

Застосування криптографічних хеш-функцій у створенні цифрового підпису дозволяє максимально ефективно модифікувати алгоритм. Шифрується не сам

текст повідомлення, а значення хеш-функції, присвоєні даному дайджесту. Завдяки цьому методу забезпечуються наступні характеристики:

– підвищення криптостійкості;
– зниження складності процесу;
– забезпечення сумісності.

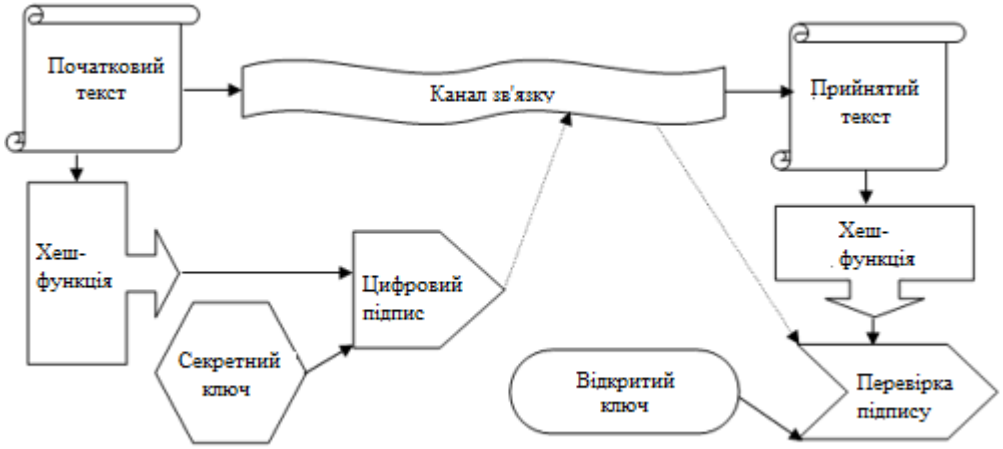

Рисунок 1.5 – Алгоритм електронного цифрового підпису

Найбільш поширені криптографічні хеш-функції:

– MD5 – один з найпоширеніших алгоритмів, що є криптографічного хеш-функцією, розмір якої становить 128 біт. Найближчим часом готується оновлення версії, так як вона вже не відповідає високим стандартам криптостійкості.

– CRC32-використовується саме для створення контрольних сум (так зване надлишкове кодування). Ця функція не є криптографічною. Є багато варіацій цього алгоритму (число після CRC означає довжину одержуваного хешу в бітах), в залежності від потрібної довжини одержуваного хеш. Функція дуже проста і нересурсоемкая. У зв'язку з цим використовується для перевірки цілісності пакетів в різних протоколах передачі даних. ГОСТ Р 34.11-2012-оновлена версія, що відрізняється високою стійкістю до спроб злому і стабільністю в роботі. Обсяг видаваного хешу може бути як 512, так і 256 біт. Як правило, застосовується в системі державного документообігу, створюючи електронні підписи.

– SHA-1 – криптографічна хеш-функція, що перетворює інформацію в рядок, довжина якої дорівнює 160 біт. Не володіє достатнім рівнем криптостійкості.

– SHA-2 – криптографічна хеш-функція, створена на основі алгоритмів SHA: 224; 256; 384; 512; 512/256; 512/224. Незважаючи на високу стійкість до злому, даний алгоритм використовується вкрай рідко. Причина-невдалий результат одного з криптоаналізів, під час якого було виявлено критичну кількість колізій (повторень хеша). Розробники мають намір створити нову криптографічну хеш-функції SHA-3, яка буде заснована на алгоритмі Keccak.

Таблиця 1.3 – Перелік та параметри хеш-функцій

Хеш-функція	Довжина значення, біт	Розмір блоку, біт	Продуктивність, Мб/с	Примітка
MD2	128		Немає даних	Виявлені колізії в спрощеній функції компресії
MD4	128	448	23.9	Виявлені колізії
MD5	128	512	6,7	Виявлені колізії в функции компресії
SHA-1	60	512	6,88	Розроблен в NIST
ГОСТ			0,9	ГОСТ

Стійкість алгоритмів шифрування

Надійність шифрувального алгоритму, часто звана його стійкістю, визначається тим, наскільки легко можна зламати шифр. Алгоритм шифрування

вважається стійким до тих пір, поки не буде доведено протилежне. Таким чином, якщо алгоритм шифрування опублікований, існує більше 5 років, і для нього не знайдено серйозних вразливостей, можна вважати, що його стійкість підходить для задач захисту секретної інформації.

Існує два типи криптографічних алгоритмів по стійкості: теоретично не розкривається (абсолютно стійкі) і ті, стійкість яких заснована на обчислювальної складності.

Щоб алгоритм вважався абсолютно стійким, він повинен відповідати таким вимогам:

– довжина ключа і довжина відкритого повідомлення повинні бути однакові;

– ключ повинен використовуватися тільки один раз;

– вибір ключа з ключового простору повинен здійснюватися равновероятно.

Дані вимоги призводять до того, що абсолютно стійкі алгоритми з практичної точки зору є важкореалізованими. В даний час відомий тільки один теоретично стійкий метод - симетричне шифрування з одноразовим блокнотом. Він заснований на застосуванні в якості ключа послідовності випадкових чисел (символів). Однак реалізувати в АС абсолютно випадковий вибір неможливо.

Все практично застосовуються сучасні алгоритми шифрування спираються на обчислювальну складність злому. Їх стійкість багато в чому визначається довжиною ключа і його непередбачуваністю - «схожістю на випадковість». Для забезпечення однієї і тієї ж ступеня стійкості симетричні методи вимагають значно меншої довжини пароля, ніж асиметричні.

Стійким вважається алгоритм, який для свого розкриття вимагає від зловмисника практично недосяжних обчислювальних ресурсів або недосяжного обсягу перехоплених зашифрованих повідомлень або часу розкриття, яке перевищує час життя, що цікавить зловмисника інформації.

1.4.3 Стенографічний метод захисту даних

Стеганографія-це метод організації зв'язку, який власне приховує саму наявність зв'язку. На відміну від криптографії, де ворог точно може визначити чи передане повідомлення зашифрованим текстом, методи стеганографії дозволяють вбудовувати секретні повідомлення у безневинні послання так, щоб неможливо було запідозрити існування вбудованого таємного послання. До неї відноситься величезна безліч секретних засобів зв'язку, таких як Невидимі чорнило, мікрофотознімки, умовне розташування знаків, таємні канали і засоби зв'язку на плаваючих частотах і т. д.

Стеганографія займає свою нішу в забезпеченні безпеки: вона не замінює, а доповнює криптографію. Приховування повідомлення методами стеганографії значно знижує ймовірність виявлення самого факту передачі повідомлення. А якщо це повідомлення до того ж зашифровано, то воно має ще один, додатковий, рівень захисту.

Стеганографічна система або стегосистема - сукупність засобів і методів, які використовуються для формування прихованого каналу передачі інформації.

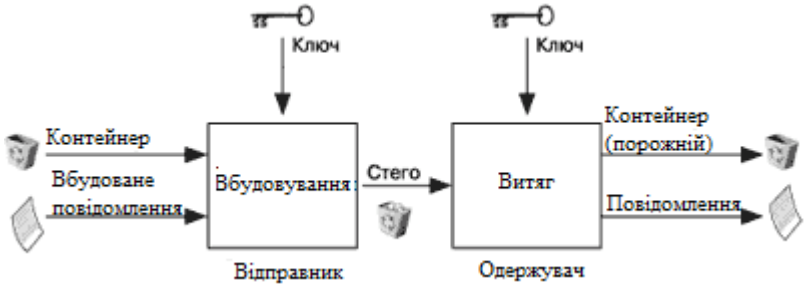

Рисунок –1.6 Узагальнена модель стегосистеми

В якості даних може використовуватися будь-яка інформація: текст, повідомлення, зображення, медіафайли і т. п.

У загальному ж випадку доцільно використовувати слово "повідомлення", так як повідомленням може бути як текст або зображення, так і, наприклад, відеодані.

Контейнер - будь-яка інформація, призначена для приховування таємних повідомлень.

Порожній контейнер - контейнер без вбудованого повідомлення; заповнений контейнер або стего - контейнер, що містить вбудовану інформацію.

Вбудоване (приховане) повідомлення-повідомлення, що вбудовується в контейнер.

Стеганографічний канал або просто стегоканал - канал передачі стего.

Стегоключ або просто ключ - секретний ключ, необхідний для приховування інформації.

За аналогією з криптографією, за типом стегоключа стегосистеми можна поділити на два типи:

– З секретним ключем.

– З відкритим ключем.

У стегосистемі з секретним ключем використовується один ключ, який повинен бути визначений або до початку обміну секретними повідомленнями, або переданий по захищеному каналу.

У стегосистемі з відкритим ключем для вбудовування та отримання повідомлення використовуються різні ключі, які розрізняються таким чином, що за допомогою обчислень неможливо вивести один ключ з іншого. Тому один ключ (відкритий) може передаватися вільно по незахищеному каналу зв'язку. Крім того, дана схема добре працює і при взаємній недовірі відправника і одержувача.

Будь-яка стегосистема повинна відповідати наступним вимогам:

– Властивості контейнера повинні бути модифіковані, щоб зміна неможливо було виявити при візуальному контролі. Ця вимога визначає якість приховування впроваджуваного повідомлення: для забезпечення безперешкодного проходження стегоповідомлення по каналу зв'язку воно жодним чином не повинно привернути увагу атакуючого.

– Стегоповідомлення має бути стійке до спотворень, в тому числі і зловмисним. В процесі передачі зображення (відео або інший контейнер) може зазнавати різні трансформації: зменшуватися або збільшуватися, перетворити в інший формат і т. д. Крім того, воно може бути стисло, в тому числі і з використанням алгоритмів стиснення з втратою даних.

– Для збереження цілісності вбудованого повідомлення необхідно використання коду з виправленням помилки.

– Для підвищення надійності вбудоване повідомлення повинно бути продубльовано.

В даний час можна виділити три тісно пов'язаних між собою і мають одні коріння напрямки додатки стеганографії: приховування даних (повідомлень), цифрові водяні знаки і заголовки.

Приховування впроваджуваних даних, які у більшості випадків мають великий обсяг, пред'являє серйозні вимоги до контейнера: розмір контейнера в кілька разів повинен перевищувати розмір вбудованих даних.

Цифрові водяні знаки використовуються для захисту авторських або майнових прав на цифрові зображення, фотографії або інші оцифровані твори мистецтва. Основними вимогами, які пред'являються до таких вбудованих даних, є надійність і стійкість до спотворень.

Цифрові водяні знаки мають невеликий об'єм, проте, з урахуванням зазначених вище вимог, для їх вбудовування використовуються більш складні методи, ніж для вбудовування просто повідомлень або заголовків.

Третє додаток, заголовки, використовується в основному для маркування зображень в електронних сховищах (бібліотеках) цифрових зображень, аудіо - та відеофайлів.

Методи

В даний час існує досить багато різних методів (і їх варіантів) вбудовування повідомлень (мається на увазі і вбудовування цифрових водяних знаків).

Методи приховування інформації

В даний час найбільш поширеним, але найменш стійким є метод заміни найменших значущих бітів або LSB-метод. Він полягає у використанні похибки дискретизації, яка завжди існує в оцифрованих зображень або аудіо - і відеофайлах. Дана похибка дорівнює найменшому значущому розряду числа, що визначає величину колірної складової елемента зображення (пікселя). Тому модифікація

молодших бітів в більшості випадків не викликає значної трансформації зображення і не виявляється візуально.

Іншим популярним методом вбудовування повідомлень є використання особливостей форматів даних, що використовують стиснення з втратою даних. Цей метод (на відміну від LSB) більш стійкий до геометричних перетворень і виявлення каналу передачі, так як є можливість в широкому діапазоні змінювати якість стисненого зображення, що робить неможливим визначення походження спотворення.

Цифрові водяні знаки

В сучасних системах формування цифрових водяних знаків використовується принцип вбудовування мітки, є вузькосмуговим сигналом, в широкому діапазоні частот маркируемого зображення. Зазначений метод реалізується за допомогою двох різних алгоритмів і їх можливих модифікацій. У першому випадку інформація ховається шляхом фазової модуляції інформаційного сигналу (несучої) з псевдовипадковою послідовністю чисел. У другому-наявний діапазон частот ділиться на кілька каналів і передача проводиться між цими каналами. Відносно вихідного зображення мітка є деяким додатковим шумом, але так як шум у сигналі присутня завжди, його незначне зростання за рахунок впровадження мітки не дає помітних на око спотворень. Крім того, мітка розсіюється по всьому вихідному зображенню, в результаті чого стає більш стійкою до вирізання.

Аналіз тенденцій розвитку технологій, що використовуються для забезпечення безпеки інформації взагалі і, зокрема, для захисту авторських прав в галузі програмного забезпечення, показує, що застосування комп'ютерної стеганографії поряд з методами, які традиційно застосовуються для захисту програмних продуктів, збільшує потужність механізмів захисту

1.5 Огляд ринку програмного забезпечення для захисту відеоінформації від несанкціонованого доступу

Bitlocker – це засіб шифрування дисків для захисту даних. Підтримувані операційні системи: Windows Vista, 7, Server 2008 R2, 8, 8.1 і 10 [13].

Алгоритми шифрування: AES 128, AES 128 Elephant diffuser, AES 256, AES 256 с Elephant diffuser.

Ключ може зберігатися в TPM або на USB-пристрої, або ж на комп'ютері.

BitLocker шифрує том, а не фізичний диск. Том може займати частину диска, а може включати в себе масив з декількох дисків. Для роботи BitLocker'у в разі шифрування системного диска потрібно два NTFS-томи, один для ОС і один для завантажувальної частини. Він повинен бути не менше 1,5 Гб, і не буде зашифрований.

TrueCrypt – це безкоштовна програма для шифрування даних. Підтримувані операційні системи: Windows XP, Vista, 7, Server 2008 R2, 8, 8.1 [16].

Підтримувані алгоритми шифрування: AES, Serpent и Twofish. Усі алгоритми шифрування використовують режим XTS.

Хеш алгоритми : RIPEMD-160, SHA-512, Whirlpool.

Відмінною особливістю TrueCrypt є можливість роботи «на льоту» (англ. - On-the-fly encryption). Завдяки цій функції можна шифрувати інформацію в реальному часі, працюючи на віртуальному зашифрованому логічному диску, який зберігається на комп'ютері у вигляді файлу. TrueCrypt може шифрувати як розділ так і цілий диск. Також програма забезпечує два рівні правдоподібного заперечення наявності шифрованих даних.

TrueCrypt має можливість призначати комбінації клавіш для монтування / розмонтування розділів, відображення і приховування вікна.

Зміна паролів і ключових файлів для тома проходить без втрати зашифрованих даних.

VeraCrypt – безкоштовний інструмент для шифрування «на льоту», форк проекту TrueCrypt. Підтримувані операційні системи:Windows XP, Vista, 7, 8, 8.1,10, Mac OS, Linux [17].

Підтримуються алгоритми шифрування: AES, Serpent, Twofish, Camellia, Kuznyechik, Cascades of ciphers.

VeraCrypt використовує режим шифрування XTS.

Хеш алгоритми: RIPEMD-160, SHA-256, SHA-512, Whirlpool, Streebog.

VeraCrypt, підтримує можливість заперечення шифрування, дозволяючи створити всередині зашифрованого томи ще один, ”прихований том”.

Файли не розшифровуються цілком - VeraCrypt розшифровує і поміщає в пам'ять тільки ту частину файлу, з якої ведеться робота в конкретний момент часу.

DiskCryptor – вільне програмне забезпечення з відкритим вихідним кодом, призначене для шифрування логічних дисків.

Підтримувані операційні системи:Windows XP, Vista, 7, 8, 8.1 [11].

Інтерфейс програми представлено на рисунку 1.5.

Підтримуються алгоритми шифрування: AES 256, Serpent, Twofish.

Хеш алгоритми: SHA-512.

Дозволяє шифрувати всі розділи дисків, включаючи системний розділ.

Ключ шифрування DiskCryptor генерується випадковим чином і зберігається в зашифрованому вигляді в першому секторі кожного тому.

Безпека криптографічного алгоритму перевіряється вбудованим тестом. Підтримує шифрування зовнішніх USB пристроїв флеш-пам’яті.

DiskCryptor має можливість призначати комбінації клавіш для монтування / розмонтування розділів.

Symantec Endpoint Encryption – це програма для прозорого шифрування диска. Підтримувані операційні системи:Windows XP, Vista, 7, 8, 8.1, 10 [15].

Підтримуються алгоритми шифрування: AES 256, AES 128.

Послідовний захист охоплює корпоративні настільні комп'ютери і сервери.

Прозоре шифрування охоплює всі дані: файли користувача, файли підкачки, системні файли, приховані файли і багато іншого.

Алгоритми PGP забезпечує високопродуктивне, надійне шифрування та використовує можливості апаратного забезпечення для збільшення швидкості шифрування.

Доступ до документів і файлів з можливістю двохфакторної аутентифікація користувачів. Централізована настройка політик безпеки в організації, управління ключами і клієнтськими додатками можлива за допомогою єдиного сервера управління.

Cyber Safe – це програма для захисту інформації. Підтримувані операційні системи:Windows XP, Vista, 7, 8, 8.1, 10 [10].

Підтримуються алгоритми шифрування: AES, ГОСТ, Blowfish, RSA.

У CyberSafe реалізована система двофакторної аутентифікації - для роботи з зашифрованими файлами потрібно не тільки знання пароля, а й наявність закритого ключа, який може зберігатися не на персональному комп'ютері, а на змінному носії.

CyberSafe надає можливість зашифровувати розділи жорсткого диску, змінні носії, а також створювати віртуальні зашифровані диски різних розмірів, а також приховувати логічні диски та зашифровані файли та папки на ПК.

При використанні CyberSafe адміністратор безпеки отримує можливість: призначити для кожної захищеної папки групу допущених до неї користувачів, провести централізовану видачу сертифікатів і ключів шифрування для співробітників компанії.

LibreCrypt – це безкоштовна програма з відкритим вихідним кодом для шифрування "на льоту". Підтримувані операційні системи:Windows XP, Vista, 7, 8, 8.1, 10 [14].

Підтримуються алгоритми шифрування: AES, Blowfish, Cast5, DES, MARS, RC6, Serpent, Twofish.

Хеш алгоритми: MD5, RIPEMD-160, SHA-256,Tiger, Whirlpool.

LibreCrypt дозволяє створювати зашифровані контейнери, які можна надалі монтувати як локальні диски. Сам контейнер можна носити з собою на знімному носії інформації.

Дозволяє шифрувати файли, диски та цілі розділи диску.

Додаткові 'файли ключів' дозволяють використовувати карту флеш-пам'яті в якості ключа.

Результати порівняння програмного забезпечення для захисту даних представлені в таблиці 1.4.

Таблиця 1.4 – Порівняльна таблиця програм шифрування

Продукт/ Показник	Bit Locker	True Crypt	Vera Crypt	Disk Cryptor	Symantec	Cyber Safe
Вартість	Безкоштовно	Безкоштовно	Безкоштовно	Безкоштовно	143$	50$
Прихова-ні кон-тейнери	-	+	+	-	-	+
Алгоритми шифрування	AES	AES, Twofish, Serpent	AES, Twofish, Serpent, Camellia	AES, Twofish, Serpent	AES	AES, RSA
Режим шифру-вання XTS	+	+	+	+	-	-
LRW	-	+	+	-	-	-
TPM	+	-	-	-	-	-
Двохфакторна автентифікація	+	+	+	+	-	+
Розмежування прав	+	-	-	-	+	+
Аудит доступу до ресурсів	+	-	-	-	+	+
Контроль цілостності контейнеру	-	+	+	-	+	-

TrueCrypt це ПЗ з відкритим вихідним кодом.28 травня 2014 року проект TrueCrypt був закритий, розробка згорнута. Всі старі версії видалені, репозиторій очищений. У вересні 2015 року було виявлено дві критичні уразливості, що дозволяють отримати права адміністратора і доступ до зашифрованих.

VeraCrypt теж ПО з відкритим вихідним кодом з'явилося як форк TrueCrypt, з реалізованими вдосконаленнями в області безпеки в порівнянні з TC. Програма схильна до ряду потенційних атак, до яких вразливе і інше програмне забезпечення шифрування дисків, наприклад, BitLocker. Для усунення цієї небезпеки розробники VeraCrypt радять використовувати ряд профілактичних рекомендацій.

BitLocker це пропрієтарне ПО, в якому відсутня можливість створювати файлові контейнери, тільки диски (флешки) цілком. Так само має ряд вразливостей, як і VeraCrypt.

CyberSafe пропрієтарне ПО. До недоліків відносяться тільки ціна і неможливість відновлення файлів при використанні прозорого шифрування у випадку апаратної проблеми (зіпсований завантажувач або пошкоджені системні файли).

Symantec Endpoint Encryption це пропрієтарне ПО. До мінусів можна віднести високу ціну і те, що ще необхідно встановлювати додаткове забезпечення (Endpoint Encryption., Symantec Drive Encryption, Symantec Endpoint Encryption (SEE), IIS 6.0).

DiskCryptor це ПЗ з відкритим вихідним кодом. З мінусів немає можливості створювати файлові криптоконтейнера і не можна створювати приховані контейнери.

Висновки по розділу 1

В даному розділі була розглянута структура відеокомплексу охоронної системи ; проведено аналіз загроз інформаційній безпеці ОС та були проаналізовані криптографічні і стенографічні методи захисту ІС.

Також розглянуто ринок програмного забезпечення для захисту відеоінформації від несанкціонованого доступу.

У ході дослідження було виявлено, що найкраще для захисту даних відеоархіву потрібно використовувати ідентифікацію і автентифікацію користувачів системи та криптографічний метод захисту інформації. Також був вибран симетричний алгоритм AES по деяким причинам:

1. На даний момент він найпопулярніший алгоритм.
2. Немає даних про взлом цього алгоритму.
3. Має високу швидкість шифрування да дешифрування великого обсягу (файли обсягом 1 ГБ шифруються та дешифруються зі швидкістю 5,3 ГБ/с, всі інші алгоритмі в середньому 989 МБ/с) і просту реалізацію.

2 ПРОЕКТУВАННЯ ІНФОРМАЦІЙНОЇ ПІДСИСТЕМИ ЗАХИСТУ ВІДЕОАРХІВУ

2.1. Вибір профілю захищеності інформації, який має забезпечувати програмне забезпечення, що розроблюється

Для визначення функціонального профілю захищеності, який має забезпечити комплекс засобів захисту (КЗЗ) згідно [5] необхідно визначити:

– категорії інформації, що оброблюватиметься;

– множину об’єктів системи, які будуть захищені КЗЗ;

– множину ролей користувачів, які можуть взаємодіяти із системою засобами КЗЗ;

– клас системи згідно [4].

Компонентами охоронної системи будуть оброблюватись файли з відеоархіву з обмеженим доступом. Витік архівних відеозаписів або їх пошкодження призведе до збитків зі сторін замовника робіт. Таким чином, до КЗЗ висуваються підвищені вимоги до забезпечення всіх базових властивостей інформації, тобто конфіденційності, цілісності та доступності.

Об’єктами відеоархіву охоронної системи є:

– автоматизовані алгоритми записів та перевірки системи;

– сервер, призначений для організації зв’язку ІД та СВК з КЗЗ;

– відеоархів використовується для відеофіксації та протоколювання.

Враховуючи специфіку системи, до якої впроваджується комплекс засобів захисту інформації, визначено наступний набір ролей користувачів:

– адміністратор – користувач, якому надані права керувати всіма елементами системи;

– адміністратор безпеки – користувач, якому надано право керувати, створювати та видаляти користувачів та змінювати атрибути доступу системи;

– користувач - якому надані права отримання відеозаписів з відеоархіву.

Виходячи з наведених вище даних, наведена зв’язка є автоматизованою системою класу «3», для якої необхідно забезпечити наступний функціональний профіль захищеності:

3.КЦД.2 = { КД-2, КА-2, КО-1, КВ-2, ЦД-1, ЦА-2, ЦО-1, ЦВ-2, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1 } [1].

Використовуючи положення [3] визначимо вимоги кожного з критеріїв захищеності, які входять до обраного профілю.

2.1.1 КА-2. Базова адміністративна конфіденційність [5]

Політика реалізації послуги повинна розповсюджуватися на наступні об’єкти захисту: файли з відеозаписами, файли бази даних системи захисту, файли ведення захищеного журналу реєстрації подій, функціональні програми обробки даних з обмеженим доступом, порти введення-виведення інформації з/на ГМД та периферійні пристрої АРМ, що входять до системи.

Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Розмежування прав необхідно здійснювати на підставі атрибутів доступу користувача і захищеного об'єкта.

Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження.

КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта.

КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного процесу через керування належністю

користувачів і процесів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес [3].

Як частина політики адміністративної конфіденційності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту.

Політика повторного використання об'єктів повинна відноситись до всіх об'єктів системи.

Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, встановлені для попереднього користувача або процесу права доступу до даного об'єкта повинні бути скасовані.

Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, вся інформація, що міститься в даному об'єкті, повинна стати недосяжною.

Політика конфіденційності повинна визначати множину об'єктів і інтерфейсних процесів, до яких вона відноситься.

Політика конфіденційності при обміні повинна визначати рівень захищеності, який забезпечується механізмами, що використовуються, і спроможність користувачів і/або процесів керувати рівнем захищеності [5].

Система повинна забезпечувати захист від безпосереднього ознайомлення з інформацією, що міститься в об'єкті, який передається.

Запити на призначення або зміну рівня захищеності повинні оброблятися системою тільки в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження.

Запити на експорт захищеного об'єкта повинні оброблятися передавальним алгоритмом на підставі атрибутів доступу інтерфейсного процесу.

Запити на імпорт захищеного об'єкта повинні оброблятися приймальним алгоритмом на підставі атрибутів доступу інтерфейсного процесу.

ЦД-1. Мінімальна довірча цілісність [3]

Політика довірчої цілісності повинна визначати множину об'єктів, до яких вона відноситься.

КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу користувача і захищеного об'єкта.

Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта.

КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право модифікувати об'єкт.

Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики довірчої цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту і імпорту.

ЦА-2. Базова адміністративна цілісність

Політика адміністративної цілісності, що реалізується КЗЗ, повинна визначати множину об'єктів ІД та СВК, до яких вона відноситься.

КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу процесу і захищеного об'єкта [9].

Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження.

КЗЗ повинен надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити конкретні процеси і/або групи процесів, які мають право модифікувати об'єкт [10].

КЗЗ повинен надавати можливість адміністратору або користувачу, який має відповідні повноваження, для кожного процесу шляхом керування належністю користувачів і процесів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право ініціювати процес [12].

Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики адміністративної цілісності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту і імпорту.

ЦО-1. Обмежений відкат [4]

Повинні існувати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкатити або відмінити певний набір (множину) операцій, виконаних над захищеним об'єктом за певний проміжок часу.

ЦВ-2: Базова цілісність при обміні

Політика цілісності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів ІД та СВК і інтерфейсних процесів, до яких вона відноситься, рівень захищеності, що забезпечується використовуваними механізмами, і спроможність користувачів і/або процесів керувати рівнем захищеності.

КЗЗ повинен забезпечувати можливість виявлення порушення цілісності інформації, що міститься в об'єкті, який передається а також фактів його видалення або дублювання.

Запити на експорт захищеного об'єкта повинні оброблятися передавальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу.

Запити на імпорт захищеного об'єкта повинні оброблятися приймальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу.

Запити на присвоєння або зміну рівня захищеності повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження [2].

ДР-1. Квоти

Політика використання ресурсів, що реалізується КЗЗ, повинна визначати множину об'єктів ІД та СВК, до яких вона відноситься.

Політика використання ресурсів повинна визначати обмеження, які можна накладати, на кількість даних об'єктів (обсяг ресурсів), що виділяються окремому користувачу.

Запити на зміну встановлених обмежень повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження.

ДВ-1. Ручне відновлення

Політика відновлення, що реалізується КЗЗ, повинна визначати множину типів відмов ІД та СВК і переривань обслуговування, після яких можливе повернення у відомий захищений стан без порушення політики безпеки. Повинні бути чітко вказані рівні відмов, у разі перевищення яких необхідна повторна інсталяція ІД та СВК.

Після відмови ІД та СВК або переривання обслуговування КЗЗ повинен перевести ІД та СВК до стану, із якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження.

Повинні існувати ручні процедури, за допомогою яких можна безпечним чином повернути ІД та СВК до нормального функціонування.

НР-2. Захищений журнал

Політика реєстрації, що реалізується КЗЗ, повинна визначати перелік подій, що реєструються.

КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє відношення до безпеки.

Журнал реєстрації повинен містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію, достатню для встановлення користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події.

КЗЗ повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування [1].

Адміністратори і користувачі, яким надані відповідні повноваження, повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації.

НИ-2. Одиночна ідентифікація і автентифікація [1]

Політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ.

Перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен автентифікувати цього користувача з використанням захищеного механізму.

КЗЗ повинен забезпечувати захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування.

НК-1. Однонаправлений достовірний канал

Політика достовірного каналу, що реалізується КЗЗ, повинна визначати механізми встановлення достовірного зв'язку між користувачем і КЗЗ.

Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації. Зв'язок з використанням даного каналу повинен ініціюватися виключно користувачем.

НО-2. Розподіл обов'язків адміністраторів

Політика розподілу обов'язків, що реалізується КЗЗ, повинна визначати ролі адміністратора і звичайного користувача і притаманні їм функції.

Політика розподілу обов'язків повинна визначати мінімум дві адміністративні ролі: адміністратора безпеки та іншого адміністратора. Функції, притаманні кожній із ролей, повинні бути мінімізовані так, щоб включати тільки ті функції, які необхідні для виконання даної ролі [1].

Користувач повинен мати можливість виступати в певній ролі тільки після того, як він виконає певні дії, що підтверджують прийняття їм цієї ролі.

НЦ-2. КЗЗ з гарантованою цілісністю

Політика цілісності КЗЗ повинна визначати домен КЗЗ та інші домени, а також механізми захисту, що використовуються для реалізації розподілення доменів.

КЗЗ повинен підтримувати домен для свого власного виконання з метою захисту від зовнішніх впливів і несанкціонованої модифікації і/або втрати керування [1].

Повинні бути описані обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ і всі запити на доступ до захищених об'єктів контролюються КЗЗ.

НТ-2. Самотестування при старті

Політика самотестування, що реалізується КЗЗ, повинна описувати властивості ІД та СВК і реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ [2].

КЗЗ має бути здатним виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій. Тести повинні виконуватися за запитом користувача, що має відповідні повноваження при ініціалізації КЗЗ [3].

НВ-1: Автентифікація вузла

Політика ідентифікації і автентифікація при обміні, що реалізується КЗЗ, повинна визначати множину атрибутів КЗЗ і процедури, які необхідні для взаємної ідентифікації при ініціалізації обміну даними з іншим КЗЗ [11].

КЗЗ, перш ніж почати обмін даними з іншим КЗЗ, повинен ідентифікувати і автентифікувати цей КЗЗ с використанням захищеного механізму

Підтвердження ідентичності має виконуватися на підставі затвердженого протоколу автентифікації.

2.2 Узагальнена структура програмного забезпечення для захисту відеоархіву охоронної підводної системи від несанкціонованого доступу

Розробляти програмне забезпечення (ПЗ) охоронної фірми пропонується за модульним принципом. Узагальнену структуру ПЗ проекту «Гідрограф» зображено на рисеуre. 2.1 [13].

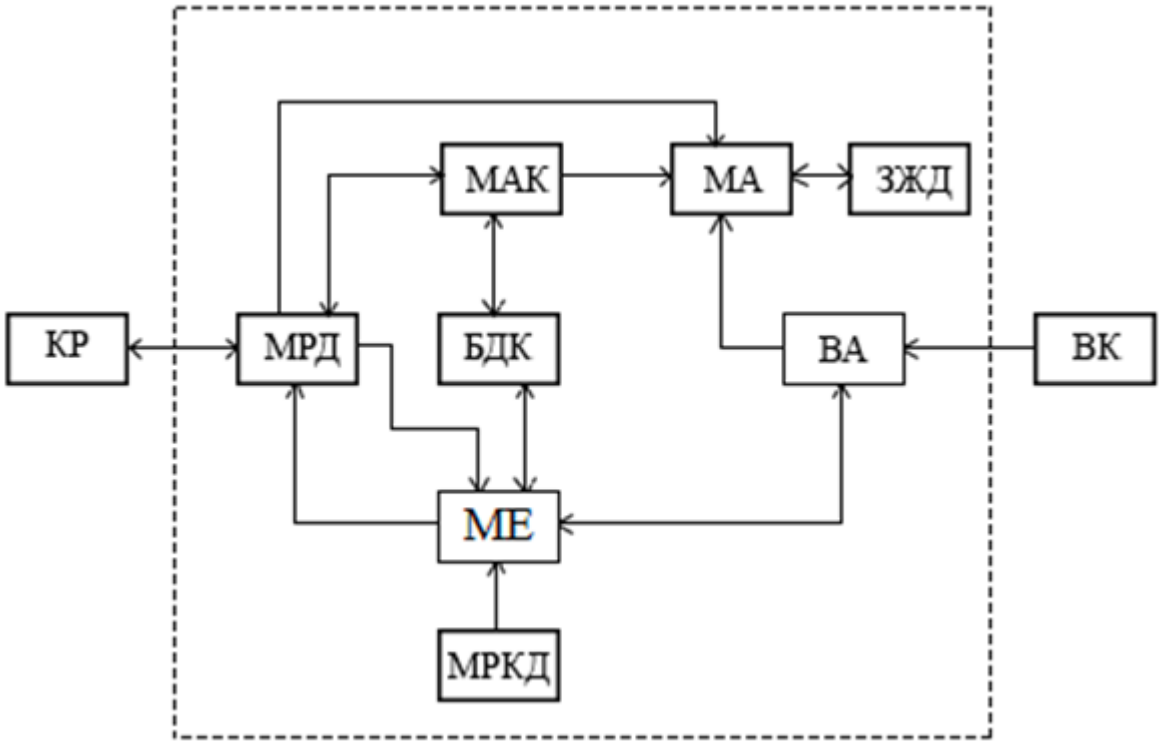

Рисунок 2.1 – Структура ПЗ для захисту відеоархіву КЗЗ

Користувач звертаючись до програмного забезпечення, тим самим надсилає сигнал до модулю розмежування доступу (МРД), який звертається до модулю автентифікації клієнтів (МАК), що бере інформацію з бази даних клієнтів (БДК) та вирішує про надання користувачу права доступу до даних з відеоархіву.

Після отримання відповідних прав доступу користувача модуль експорту/імпорту (МЕІ) отримує дані з відеоархіву, ключову інформацію з БДК та виконує операцію експорту файлів і надає метод розшифровки користувачу. При цьому дані про спробу доступу до ресурсів записуються модулем аудиту (МА) до захищеного журналу доступу (ЗЖД). Дані, які зберігаються у відеоархіві можуть бути записані адміністратором шляхом захоплення відео сигналу від відеокомплексу ПА [5].

Широко поширеними механізмами вирішення завдань забезпечення безпеки є розробка методів і засобів, що дозволяють одній стороні переконатися в ідентичності іншого боку.

На даний момент актуальні протоколи автентифікації:

– RADIUS;

– SSH;

– EAP-TLS.

RADIUS (Remote Authentication Dial-In User Service) – це мережевий протокол, призначений для забезпечення централізованої авторизації та обліку користувачів, які підключаються до різних мережевих служб. RADIUS це клієнт-серверний протокол, що працює на прикладному рівні, і може використовувати як транспорт як TCP так і UDP [7].

SSH (Security Shell) - це мережевий протокол, що забезпечує захищену авторизацію, з'єднання і безпечна передача даних між хостами мережі, шляхом шифрування трафіку, що проходить через нього з можливою компресією даних.

EAP (Extensible Authentication Protocol) – це протокол, що забезпечує підтримку додаткових схем перевірки автентичності, які називаються типами EAP. До даних схем відносять токен-карти, одноразові паролі, перевірка справжності відкритого ключа і сертифікати. Схема перевірки автентичності EAP називається типом EAP. Для успішної перевірки автентичності клієнт віддаленого доступу і пристрій перевірки автентичності повинні підтримувати один і той же тип EAP [7].

У даному програмному забезпеченні пропонується використати метод шифрування AES.

AES (Advanced Encryptin Standart) – симетричний алгоритм блочного шифрування; базується на принципах нової мережі підстановок-перестановок.

Має нову архітектуру SQUARE (КВАДРАТ), для якої характерним є:

– блок, який шифрується представляється у виді двомірного байтового масиву;

– шифрування за один раунд усього блоку даних;

– виконання криптографічних перетворень, як над окремими байтами масиву, так і над його рядками і стовпцями.

Це забезпечує дифузію даних одночасно в двох напрямках –по рядках і стовпцях. Архітектура SQUARE властива, крім шифру AES, шифрам SQUARE,CRYPTON.

Загальні характеристики AES:

– AES зашифровує і розшифровує 128-бітові блоки даних;

– AES дозволяє використовувати три різних ключа довжиною 128, 192 або 256 біт (в залежності від довжини ключа версії шифру AES-позначають 128, AES-192 або AES-256);

– від розміру ключа залежить число раундів шифрування: довжина 128 біт - 10 раундів; 192 довжина біта - 12 раундів; 256 біт довжина - 14 раундів;

– всі раунди, крім останнього, ідентичні [8].

2.2.1 Подання даних у криптоалгоритмі AES

Основним елементом, яким оперує алгоритм AES, є байт – послідовність 8 біт, що оброблюються як єдине ціле. Для формування байтів 128 бітів блоку відкритого тексту, вихідного блоку шифротексту та ключа шифру поділяються на групи з 8-ми біт, які стоять так, щоб в цілому вийшов масив байтів. На рисунку 2.2 [10] представлена прийнята нумерація в межах кожного байту.

№ бита на вході	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	…
№ байта	0								1								2								…
№ бита в байте	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	…

Рисунок 2.2 – Нумерація в межах кожного байту [10]

Задавати значення байту зручно в шістанадцятирічній системі числення. Для цього байт ділиться на дві групи з 4-х біт: група старших біт у байті представляється першим шістнадцятирічним символом, а група молодших біт – другим. Наприклад, для байту 10101100 отримаємо [10]:

10101100 = 1010 1100 = AC.

Позначимо

in0, in1,…,

in15 – 16 байт блоку відкритого тексту;

k0, k1,…, k15 – 16 байт ключа шифру;

– 16 байт блоку шифротексту.

Вхідними даними для операцій шифрування є масив з 16 байтів in0, in1,…, in15. Перед початком шифрування байти цього масиву розміщаються послідовно у стовпці матриці InputBlock (зверху вниз). Усередині алгоритму операції виконуються над матрицею байт, яка називається матрицею станів State або просто станом. Звісно значення матриці OutputBlock є виходом алгоритму та перетворюється у послідовність байтів шифротексту out0, out1,…, out15. Аналогічно у стовпці матриці InputKey попадають і 16 байтів k0,k1,...,k15 ключа шифру. Розмірність усіх матриць – 4 x 4 [6].

Схематично таке представлення зображено на рисунку 2.3 [14].

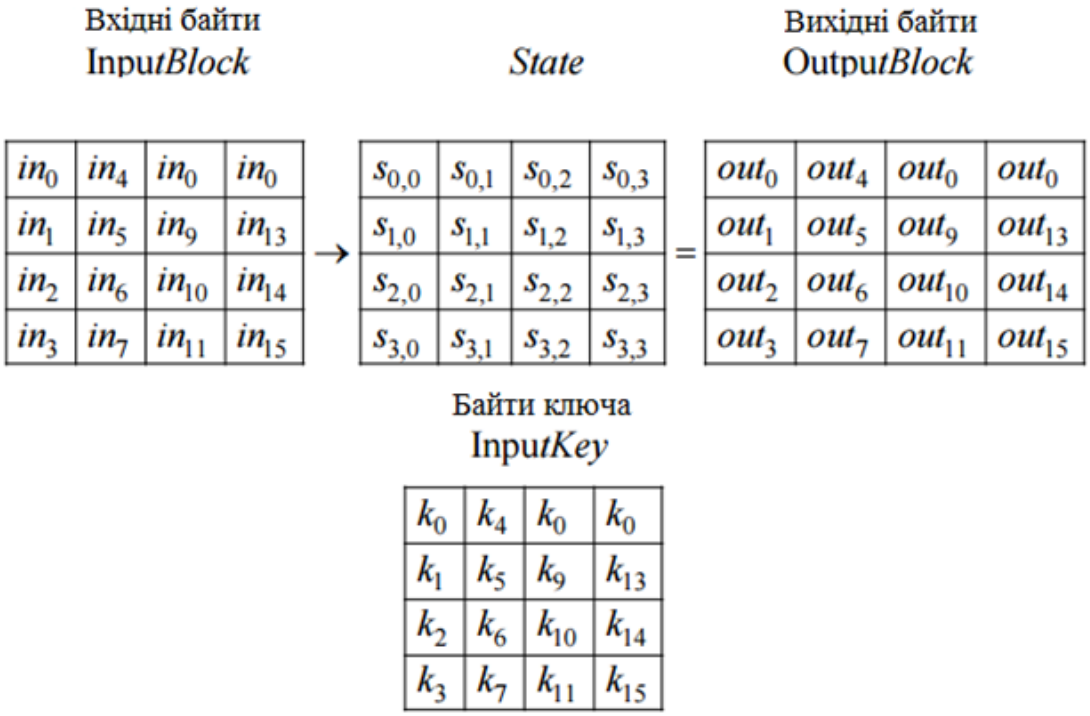

Рисунок 2.3 – Матриця станів [12]

Чотири байти у кожному стовпці матриці станів або ключа можливо розглядати як одне 32-х бітове слово. Тому матриця станів – це масив з 4 слів w0,w1,w2,w3, де

$$w_0 = s_{0,0}\, s_{1,0}\, s_{2,0}\, s_{3,0};$$
$$w_1 = s_{0,1}\, s_{1,1}\, s_{2,1}\, s_{3,1};$$
$$w_2 = s_{0,2}\, s_{1,2}\, s_{2,2}\, s_{3,2};$$
$$w_3 = s_{0,3}\, s_{1,3}\, s_{2,3}\, s_{3,3}.$$

Рисунок 2.4 – Масив з 4 слів w0,w1,w2,w3 [11]

Матриця, що надходить на вхід кожного раунду називається матрицею InputState, а на виході створюється матриця OutputState. На вході першого раунду InputState=InputBlock , а на виході останнього раунду OutputState= OutputBlock.

2.2.2 Загальна структура AES

AES-128 ключ шифру складається з 128 бітів, поділених на 16 байтів k0, k1, …, k15 та записується в стовпці матриці InputKey. Кожний стовпець матриці InputKey створює слово, тобто фактично ключ шифру – це чотири слова w0, w1, w2, w3 , де w0=k0k1k2k3, w1=k4k5k6k7 и т.д [13].

Рисунок 2.5 – Ключі раундів [14]

З цих слів за допомогою спеціального алгоритму, утворюється послідовність з 44 слів: w0,w1,w2,...,w43 (кожне слово по 32 биту). На кожний раунд шифрування подаються по чотири слова цієї послідовності. Вони будуть грати роль раундового ключа.

Схема перетворення даних зображена на рисунку 2.6 [17].

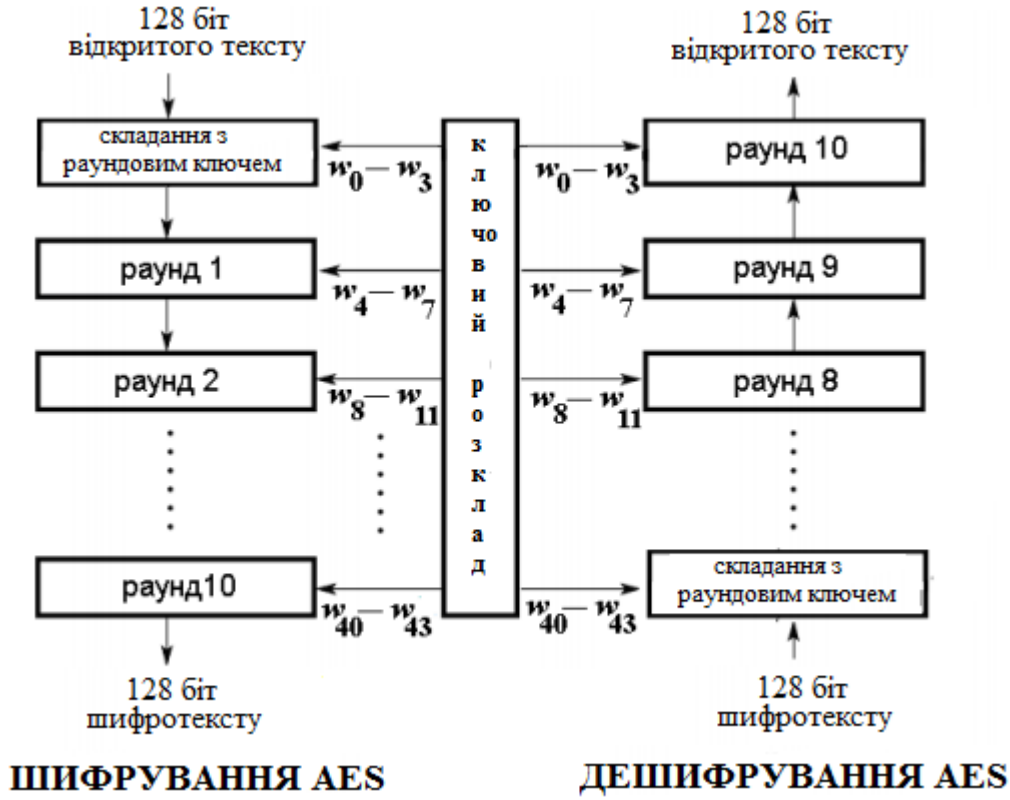

Рисунок 2.6 – Схема перетворення даних

Перед першим раундом виконується операція AddRoundKey (підсумування по модулю 2 с початковим ключем шифру). Перетворення, виконувані в одному раунді позначають

Round (State, RoundKey),

де змінна State – матриця, що описує дані на вході раунду і на його виході після шифрування; змінна RoundKey – матриця, яка містить раундовий ключ.

Раунд складається з 4-х різних перетворень [16]:

– SubBytes – побайтова підстановка в S-боксі з фіксованою таблицею замін;

– ShiftRows – побайтовий зсув рядка матриці State на різну кількість байтів;

– MixColumns – перемішування байтів в стовпцях;

– AddRoundKey – складання з раундовим ключем (операція XOR).

Останній раунд відрізняється від попередніх тим, що не задіє функцію MixColumns.

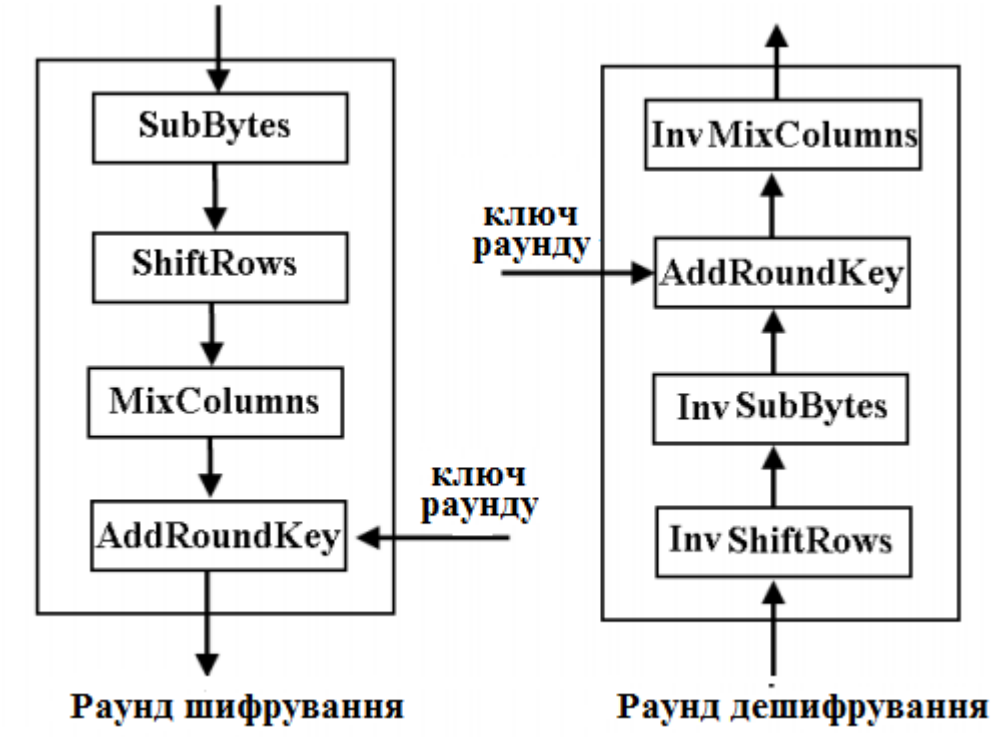

Рисунок 2.7 – Раунди шифрування та дешифрування

При дешифруванні у кожному раунді виконуються зворотні операції: InvShiftRows, InvSubBytes, AddRoundKey и InvMixColumns. Порядок виконання операцій при шифруванні та дешифруванні різний.

Для трьох варіантів ключів AES повний перебір вимагає , або операцій відповідно. Навіть найменша з цих числа свідчить, що атака з використанням перебір ключі сьогодні не має практичного значення.

2.3 Алгоритмічне забезпечення розробки

Блок-схема головного алгоритму ПЗ зображена на рис. 2.8 [15].

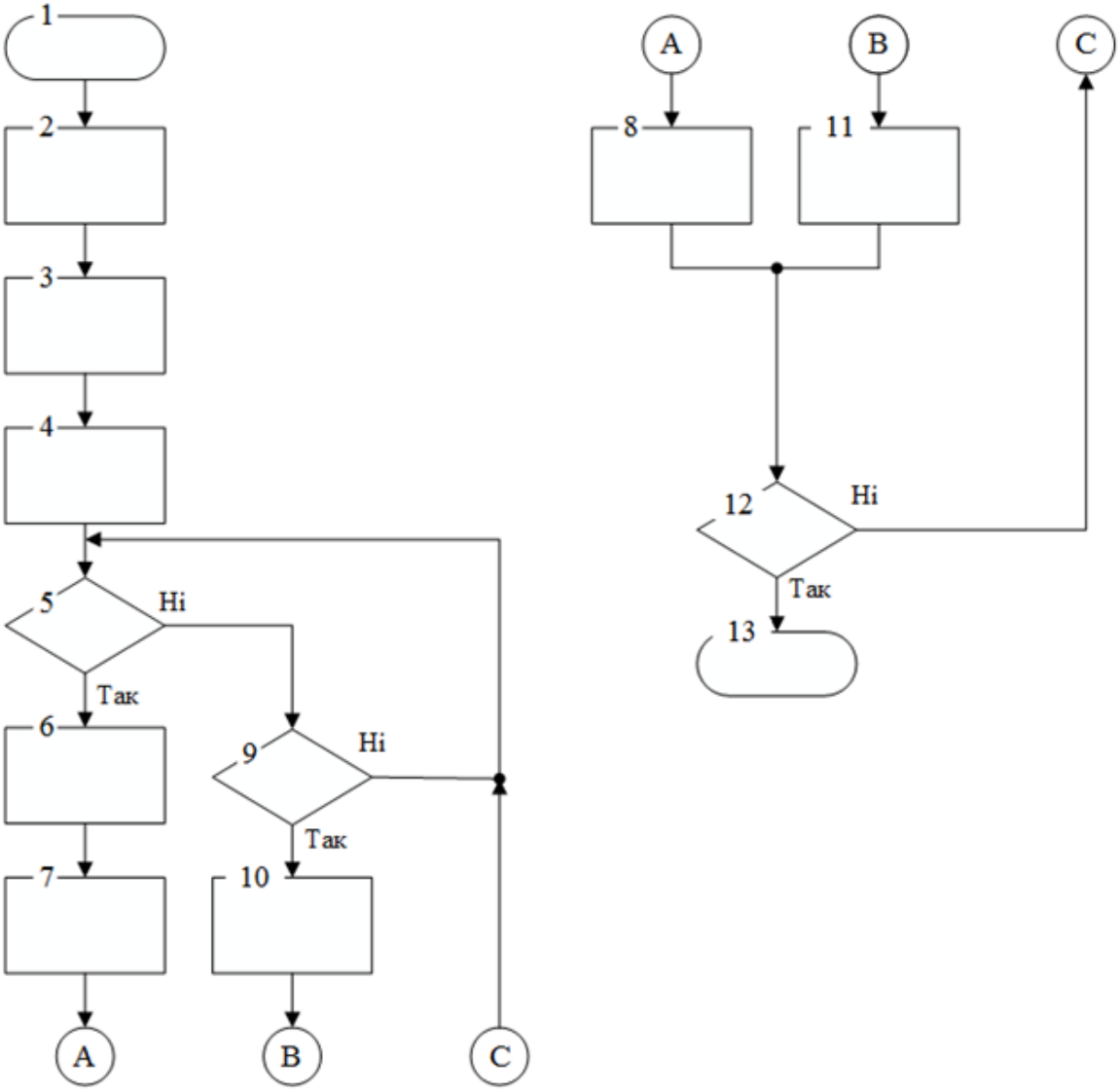

Рисунок 2.8 – Блок-схема головного алгоритму ПЗ

Опис блоків алгоритму:

1) Початок;
2) З’єднання з сервером;
3) Авторизація;
4) Реєстрація події у ЗЖД;
5) Отримано запит на експорт файлів?;
6) Експорт відеофайлу;
7) Обмін ключами шифрування з клієнтом;
8) Реєстрація події у ЗЖД;

9) Запит дії на імпорт;
10) Шифрування відеофайлу;
11) Реєстрація події у ЗЖД;
12) Завершити роботу;
13) Кінець.

Після початку роботи система очікує запитів клієнтів на з’єднання з сервером (блок 2) КЗЗ. Далі проходить авторизація користувача (блок 3). Результати процесу авторизації користувача записуються до захищеного журналу доступу (блок 4) [11].

Наступним кроком надсилається запит на експорт відеофайлу (блок 6). Якщо запит вдалий то проходить експорт відеофайлу (блок 6) та проходить обмін ключами шифрування з клієнтом (блок 7), а також реєструється подія у ЗЖД (блок 8) про виконані дії. У другому випадку проходить запит дії на імпорт відеофайлів (блок 9). При вдалій спробі починається шифрування відеофайлу (блок 10) та виконується реєстрація події у ЗЖД (блок 11). У негативному випадку запит на дію починається з блоку 5 [13].

Далі виконується запит на завершення роботи (блок 13), якщо він позитивний то програмне забезпечення завершує сеанс роботи з даним користувачем. У іншому випадку запит на дію починається з блоку 5.

Блок-схема алгоритму авторизації користувача зображена на рисунку 2.9 [16].

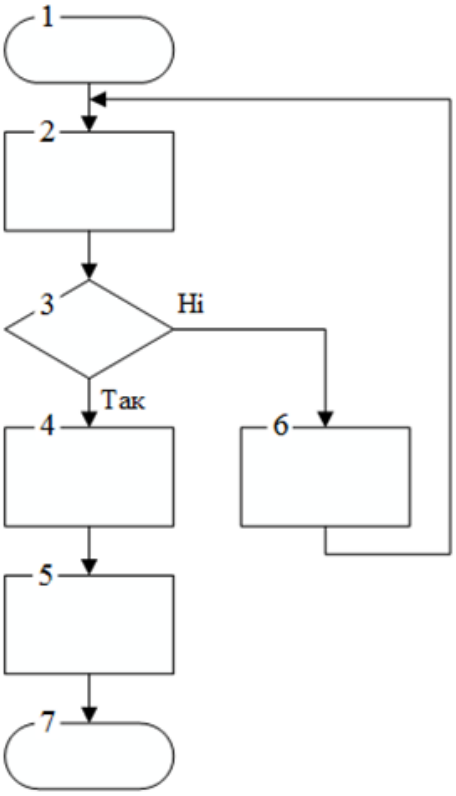

Рисунок 2.9 – Блок-схема авторизації користувача ПЗ

Опис блоків алгоритму:

1. Вхід.
2. Введення логіну та паролю.
3. Існує користувач у БДК?
4. Реєстрація події у ЗЖД.
5. Створення тимчасової БД з правами доступу.
6. Реєстрація події у ЗЖД.
7. Вихід.

Після входу до функції користувач вводить логін та пароль (блок 2). Система надсилає запит чи є дані про користувача у БДК (блок 3). У разі співпадання події реєструються у ЗЖД (блок 4). Створюється тимчасова база даних (блок 5), де зберігаються права доступу користувача до закінчення сеансу [17].

Якщо дані про користувача не співпадали з БДК, то система повертає запит на дію до блоку 2 [18].

Висновки до розділу 2

Виходячи з компонентів КЗЗ, об’єктів відеоархіву та специфіки системи був вибраний профіль захищеності 3.КЦД.2. Також було розроблено узагальнену структуру ПЗ для захисту відеоархіву КЗЗ охоронної системи від несанкціонованого доступу.

3 РЕАЛІЗАЦІЯ ІНФОРМАЦІЙНОЇ ПІДСИСТЕМИ ЗАХИСТУ ВІДЕОАРХІВУ

3.1 Вихідний код програмного модуля захисту відеоматеріалів від несанкціонованого доступу

Метод Encrypt реалізує шифрування відеофайлу методом шифрування AES. Програмний код наведений нижче.

```
public byte[] Encrypt(byte[] key, byte[] secret_message, byte[] iv)
    {
        using (Aes aes = new AesCryptoServiceProvider())
        {
            aes.Key = key;
            aes.IV = iv;

            using (MemoryStream ms = new MemoryStream())
            {
                using (CryptoStream cs = new CryptoStream(ms, aes.CreateEncryptor(), CryptoStreamMode.Write))
                {
                    cs.Write(secret_message, 0, secret_message.Length);
                    cs.Close();
                    return ms.ToArray();
                }
            }
        }
    }
```

Метод Decrypt реалізує дешифрування відеофайлу. Програмний код наведений нижче.

```
public byte[] Decrypt(byte[] key, byte[] encrypted_message, byte[] iv)
    {
        using (Aes aes = new AesCryptoServiceProvider())
        {
            aes.Key = key;
            aes.IV = iv;

            using (MemoryStream ms = new MemoryStream())
            {
                using (CryptoStream cs = new CryptoStream(ms, aes.CreateDecryptor(),
CryptoStreamMode.Write))
                {
                    cs.Write(encrypted_message, 0, encrypted_message.Length);
                    return ms.ToArray();
                }
            }
        }
    }
```

3.2 Вихідний код програмного модуля резервування та відновлення видалених відеоматеріалів

Метод Data_Base реалізує роботу модуля бази даних клієнту. Метод Create_Table забезпечує створення таблиці бази даних. Метод Add_in_Table дозволяє додавати нових користувачів у БДК. Метод Read_from_Table забезпечує зчитування даних з БДК. Програмний код наведений нижче.

```
        public Data_Base(string dbName)
        {
            baseName = dbName;

            if (!File.Exists(baseName))
            {
                SQLiteConnection.CreateFile(baseName);
                m_Connection = new SQLiteConnection(string.Format("DataSource={0}",
baseName));
                m_Connection.Open();
                Create_Table("User_Table", "id_user integer primary key autoincrement, login
char[100], password char[100], user_type char[100]");
                Add_in_Table("User_Table", "login, password, user_type", "'admin', 'admin',
'admin'");
            }
            else
            {
                m_Connection = new SQLiteConnection(string.Format("DataSource={0}",
baseName));
                m_Connection.Open();
            }

        }

        public void Dispose()
        {
            m_Connection.Close();
        }

        private void Create_Table(string Name_Table, string Parameters_Table)
        {
            using (SQLiteCommand command = new SQLiteCommand(m_Connection))
            {
```

```
                command.CommandText = "CREATE TABLE " + Name_Table + " (" +
Parameters_Table + " );";
                command.ExecuteNonQuery();
            }
        }

        public void Add_in_Table(string Name_Table, string Table_Param, string Values)
        {
            using (SQLiteCommand command = new SQLiteCommand(m_Connection))
            {
                command.CommandText = "INSERT INTO " + Name_Table + " ( " + Table_Param +
" ) " + " VALUES ( " + Values + " );";
                command.ExecuteNonQuery();
            }
        }

        public SQLiteDataReader Read_from_Table(string Name_Table, string Read_Param)
        {
            using (SQLiteCommand command = new SQLiteCommand(m_Connection))
            {
                command.CommandText = "SELECT " + Read_Param + " from " + Name_Table + "
;";
                return command.ExecuteReader();
            }
        }
```

У наступному коді реалізовано автентифікацію користувача.

```
public partial class Form1 : Form
    {
        string login, password;
        byte[] key;
        Data_Base db = new Data_Base("User.db");
```

```
        Form2 f2;
        Form3 f3;

        public Form1()
        {
            f2 = new Form2(this, db);
            f3 = new Form3(this);
            InitializeComponent();
        }


        private void button1_Click(object sender, EventArgs e)
        {
            login = LoginTB.Text;
            LoginTB.Clear();
            password = PasswordTB.Text;
            PasswordTB.Clear();

            if(login != "" && password != "")
            {
                SQLiteDataReader data_red = db.Read_from_Table("User_Table WHERE login ='" +
login + "'", "*");
                foreach (DbDataRecord record in data_red)
                {
                    if (Int32.Parse(record["id_user"].ToString()) != 0)
                    {
                        Hide();
                        key = SHA256.Create().ComputeHash(
Encoding.UTF8.GetBytes(string.Concat(login, password)));
                        if (record["user_type"].ToString() == "admin")
                        {
                            f2.SetKey(key);
                            f2.ShowDialog();
                        }
```

```
                if (record["user_type"].ToString() == "user")
                {
                    f3.SetKey(key);
                    f3.ShowDialog();
                }
            }
            else
            {
                MessageBox.Show("Невірний логін чи пароль!");
            }
        }
    }


    }
  }
public partial class Form2 : Form
  {
    Form1 f1;
    Form4 f4 = new Form4();
    string NULogin, NUPass, NUUser_Type, FileName;
    long FileSize = 0;
    Int32 Count = 0, Ost = 0;
    Data_Base db;
    byte[] key;
    Thread EncryptedThread;

    public Form2(Form1 f, Data_Base dbObject)
    {
      f1 = f;
      db = dbObject;
      EncryptedThread = new Thread(AddVideo);
      InitializeComponent();
    }
```

```
        public void SetKey(byte[] k)
        {
            key = k;
        }

        private void button2_Click(object sender, EventArgs e)
        {
            f4.ShowDialog();
        }

        private void Form2_Closing(object sender, FormClosingEventArgs e)
        {
            Hide();
            f1.Show();
        }

        private void button1_Click(object sender, EventArgs e)
        {
            NULogin = RegTBLogin.Text;
            NUPass = RegTBPass.Text;
            NUUser_Type = RegTBUT.Text;
            db.Add_in_Table("User_Table", "login, password, user_type", "'" + NULogin + "', '" +
NUPass + "', '" + NUUser_Type + "'");
            MessageBox.Show("Реєстрація успішна");
        }

        private void button3_Click(object sender, EventArgs e)
        {
            if (openFileDialog1.ShowDialog() == DialogResult.OK)
            {
                FileName = openFileDialog1.FileName;
                EncryptedThread.Start();
            }
```

```
}
```

Метод AddVideo() реалілує імпорт відео у відеоархів. Програмний код наведений нижче.

```
private void AddVideo()
{
   byte[] encrypted_message;
   byte[] iv;
   int Block_Size = 512;

   using (FileStream file1 = new FileStream(FileName, FileMode.Open))
   {
      using (FileStream file2 = new FileStream("D:\\testVideo.mp4", FileMode.Create))
      {

         FileSize = file1.Length;
         Ost = (Int32)FileSize % Block_Size;
         Count = (Int32)(FileSize - Ost) / Block_Size;

         using (BinaryReader reader = new BinaryReader(file1))
         {
            using (BinaryWriter writer = new BinaryWriter(file2))
            {
               using (Crypto cr = new Crypto())
               {
                  using (Aes aes = new AesCryptoServiceProvider())
                  {
                     iv = aes.IV;
                  }
                  byte[] buf1 = new byte[Block_Size];
                  byte[] buf2 = new byte[Ost];

                  writer.Write(iv);

                  for (int i = 0; i < Count; i++)
```

```
                    {
                        reader.Read(buf1, 0, Block_Size);
                        encrypted_message = cr.Encrypt(key, buf1, iv);
                        writer.Write(encrypted_message, 0, encrypted_message.Length);
                    }
                    //reader.Read(buf2, 0, Ost);
                    //encrypted_message = cr.Encrypt(key, buf2, iv);
                    //writer.Write(encrypted_message, 0, encrypted_message.Length);
                }
            }
        }

    }
    MessageBox.Show("Відео додано до архіву!");
}

}
```

Метод Form4() описує роботу з захищеним журналом доступа. Програмний код наведений нижче.

```
public partial class Form4 : Form
    {
        public Form4()
        {
            InitializeComponent();
            //dataGridView1.Columns.Add("colTime", "Дата\Час");
            //dataGridView1.Columns.Add("colUser", "Користувач");
            //dataGridView1.Columns.Add("colEvent", "Подія");
            dataGridView1.Rows.Add("12.06.17 17:23", "Admin", "Додання файлу
'Випробування1.avi'.");
            dataGridView1.Rows.Add("13.06.17 10:48", "Admin", "Додання файлу
'Випробування2.avi'.");
```

```
            dataGridView1.Rows.Add("14.06.17 19:15", "Admin", "Реєстрація користувача
'User'");
            dataGridView1.Rows.Add("14.06.17 20:05", "User", "Копіювання файлу
'Випробування1.avi'.");
        }

    }
    }
```

3.3 Перевірка працездатності програмного забезпечення для захисту відеоархіву

На початку виконання програма видає діалог авторизації користувача. Далі з’являється головне вікно.

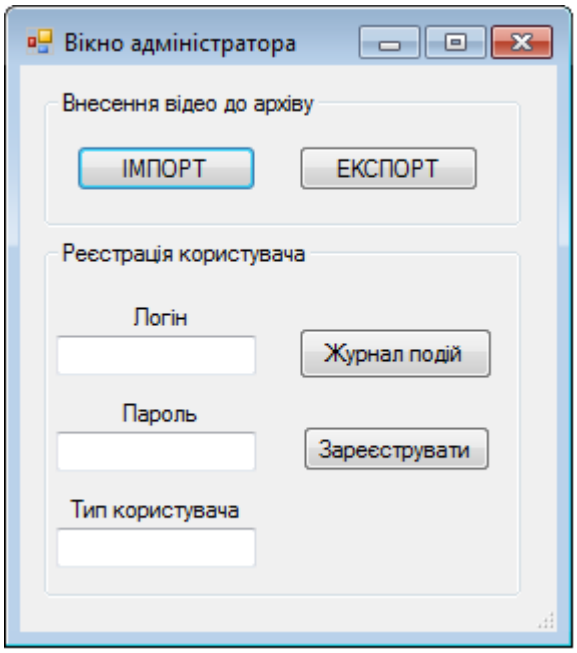

Рисунок 3.1 – Вікно адміністратора

У вікні адміністратора доступними є кнопки ІМПОРТУ та ЕКСПОРТУ файлів, журнал подій та розділ реєстрації користувача. Кнопки ІМПОРТУ та ЕКСПОРТУ надають можливість виклику підпорядкованого вікна для вибору

відеофайлів, зображено на рисунку 3.2. Розділ реєстрації користувача доступний тільки для адміністратора, для звичайного користувача поле буде пустим.

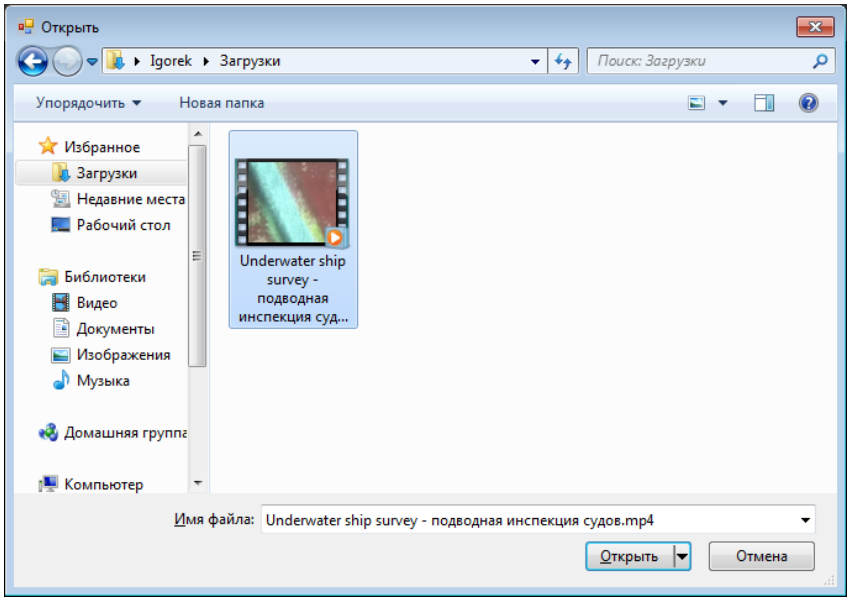

Рисунок 3.2 – Вибір файлу для імпорту у відеоархів

Кнопка Журнал подій визиває однойменну форму, де відображується інформація про виконувані дії з відеоархівом та базою даних, зображено на рисунку 3.3.

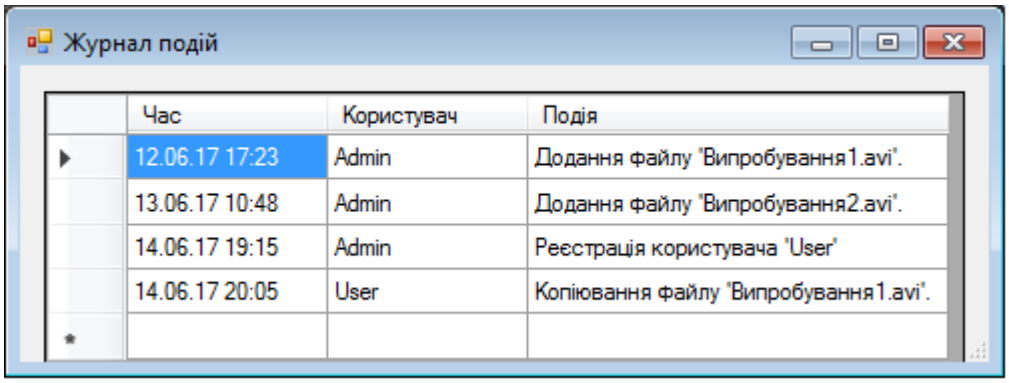

Рисунок 3.3 – Вікно журналу подій

При успішному імпорті файлів з’являється повідомлення про завершення операції, зображено на рисунку 3.4.

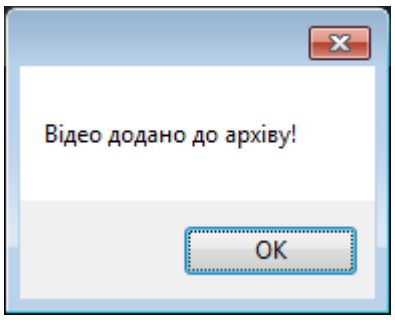

Рисунок 3.4 – Повідомлення про успішний імпорт файлу

Висновки до розділу 3

Було розглянуто вихідний код програмних модулів захисту відеоматеріалів від несанкціонованого доступу. Також була проведена перевірка працездатності програмного забезпечення.

4 РОЗРАХУНОК ЕКОНОМІЧНОГО ЕФЕКТУ ОБҐРУНТУВАННЯ РОЗРОБКИ

4.1 Вступ до проблеми

Інформаційні системи широко використовуються багатьма організаціями України різної форми власності. Ці системи розповсюджуються все більше і більше, змінюючись відповідно до вимог замовників та модернізуючись з плином часу.

Створення інформаційної системи вимагає одноразових витрат на її розробку та придбання необхідних технічних засобів, а також поточних витрат, пов’язаних з функціонуванням підсистеми. Економічний ефект від експлуатації системи визначається з урахуванням витрат на її експлуатацію. Відношення економічного ефекту до витрат на створення системи характеризує економічну ефективність капітальних вкладень. Економічні показники визначаються за діючими на момент розрахунку цінами, тарифами та ставками заробітної плати.

4.2 Розрахунок вартості створення автоматизованої системи

Загальні витрати (на проектування, реалізацію та впровадження системи)

$$З = Сп\text{-}р + Стз + Спз + Свпр,$$

де Сп-р – витрати на проектування і реалізацію;

Стз – витрати на придбання або модернізацію обчислювальної техніки, периферійних пристроїв, засобів зв'язку, допоміжного устаткування та оргтехніки (з урахуванням витрат на транспортування, монтаж, налагодження і запуск), виробничо-господарського інвентарю;

Спз – витрати на придбання та інсталяцію програмного забезпечення (ПЗ), необхідного для розробки;

Свпр – витрати на впровадження системи (навчання персоналу тощо).

Витрати на проектування та реалізацію розраховуються за формулою

$$Сп\text{-}р = Сз + Свід + См + Сн,$$

де З С – заробітна плата розробників;

ВІД С – відрахування на соціальні заходи (відповідно до чинного законодавства ВІД С становить 47,5% від фонду оплати праці);

М С - експлуатація та амортизація, $См=З_{експл}+З_{амор}$;

Н С – накладні витрати у розмірі 50-150% від витрат на оплату праці (охоплюють оплату праці управлінського персоналу з нарахуваннями; оплату службових відряджень; оплату консультаційно-інформаційних послуг; оплату ремонту і техобслуговування основних фондів, крім персональних комп'ютерів (ПК)).

1) Розробка підсистеми вимагає 6 місяців (експертна оцінка, яка базується на досвіді розробки систем такого класу). Заробітна платня розробників за місяць дорівнює 12000 грн (відповідно до сучасних розцінок та попиту на спеціалістів такого профілю). Кількість розробників – одна людина.

профілю). Кількість розробників – одна людина.

$$Сз = 1 * 12000 * 6 = 72000 \text{ грн.}$$

$$Свід = 72000 * 0,475 = 34200 \text{ грн.}$$

2) витрати на амортизацію ЕОМ, на якій виконується розробка:

$$З_{амор} = (Ц_{еом}/Т_{сл}) \cdot (Т_{разр}/12),$$

де $Ц_{еом} = 6000$ грн. – балансова вартість ЕОМ;

$Т_{сл} = 5$ років – термін служби ЕОМ;

$Т_{разр} = 0,5$ року – час, необхідний для розробки системи, виражений в місяцях, і тому ділиться на 12, щоб одержати число років.

$$З_{амор} = (6000/5) \cdot 0,5 = 600 \text{ (грн.)};$$

3) витрати на експлуатацію ЕОМ, на якій виконується розробка, полягають в оплаті споживаної нею електричної енергії:

$$З_{експл} = P_{ЭВМ} \cdot T_{разр} \cdot N_{рд} \cdot N_{рч} \cdot Э_{ст},$$

де $P_{ЭВМ} = 0,4$ кВт/год – потужність ЕОМ;

$T_{разр} =$ 6 міс. – тривалість розробки;

$N_{рд} = 21$ день – число робочих днів у місяці;

$N_{рч} = 8$ годин – число годин у робочому дні;

$Э_{ст} =$ 0,3073 грн – вартість 1 кВт електроенергії.

$$З_{експл} = 0,4 \cdot 6 \cdot 21 \cdot 8 \cdot 0,3073 = 123,90 \text{ (грн);}$$

$$С_м = 600 + 123,90 = 723,90 \text{ (грн.)}$$

$$С_н = 72000 * 0,3 = 21600 \text{ (грн.)}$$

$$С_{п-р} = 72000 + 34200 + 723,90 + 21600 = 128\,523,90 \text{ (грн.)}$$

Витрати на програмне забезпечення не закладаються у даний кошторис оскільки в роботі системи планується використовувати безкоштовне ПЗ відкритими вихідними кодами. Витрати на апаратне забезпечення складають 19981 грн (придбання серверу та комутаційного обладнання і матеріалів). До витрат на впровадження системи можна віднести витрати вартість навчання кадрів, витрати на монтаж і настроювання мережі, вартіст устаткування, вартість програмного забезпечення. Витрати на впровадження системи приведені в таблиці 4.1.

Таблиця 4.1 – Витрати на провадження системи

№	Найменування інвестицій	Сума, грн.
1	Вартість устаткування	19981
2	Вартість програмного забезпечення	-
3	Вартість підготовки кадрів	500
4	Монтаж і настроювання локальної мережі	300
Разом на впровадження системи		*20781*

Таким чином, загальні витрати на проектування, реалізацію та впровадження системи складають

$$З = Сп\text{-}р + Стз + Спз + Свпр = 128\ 523{,}90 + 20781 = 149304{,}90 \text{ (грн)}.$$

Витрати на створення та експлуатацію системи в перший рік експлуатації

$$Зсе = З + Зер,$$

де Зер – експлуатаційні витрати на технічне забезпечення за рік.

$$Зер = АОБ + Зм + Зе,$$

де АОБ – амортизаційні відрахування на устаткування;

Зм – витрати на основні і допоміжні матеріали;

Зе – витрати на електроенергію.

Амортизаційні відрахування на устаткування складають 60% балансової вартості в рік (за чинним законодавством)

$$А_{об} = 20781 * 0{,}6 = 12468{,}6 \text{ грн.}$$

В масштабі підприємства річні витрати на основні та допоміжні матеріали (гнучкі диски, папір тощо) визначаються в розмірі 3% вартості основного устаткування

$$З_м = 20781 * 0{,}03 = 623{,}43 \text{ грн.}$$

Річний обсяг робіт ПК у нормо-годинах

$$ФМ = 253{,}3 * Т_С,$$

де $Т_С$ – середнє місячне завантаження устаткування (близько 5 годин);

253,3 – середня кількість робочих днів у році.

$$Фм = 253{,}3 * 5 = 1266{,}5 \text{ годин.}$$

Витрати на електроенергію під час 1266,5 годин роботи устаткування в рік при потужності ЕОМ 0,4 кВт/год та ціні 0,3073 грн за 1 кВт електроенергії складуть

$$Зе = 1266{,}5 * 0{,}3073 * 0{,}4 = 155{,}68 \text{ грн.}$$

Отже, у перший рік витрати на створення та експлуатацію системи складуть

$$Зсе = 149304{,}90 + 13247{,}71 = 162552{,}61 \text{ грн.}$$

4.3 Розрахунок економічної ефективності

Економічна ефективність використання розподіленої інформаційної системи на базі технології хмарних обчислень полягає у наступному:

– зменшення часу на обслуговування системи за рахунок її відмовостійкост та автоматичного масштабування;
– можливість надання користувачам обчислювальних потужносте в оренду.

Це зменшення відбудеться за рахунок зменшення складності користування системою, збільшення надійності, стабільності та рівня безпеки. Визначимо, що це зменшення складе 50% від сучасного.

Однак, не піддається прямій грошовій оцінці зменшення кількості помилкових та необережних рішень, підвищення оперативності керування, поліпшення організації роботи та своєчасне отримання необхідної інформації про пріоритетність варіантів рішень тощо.

Використання даної системи дозволяє вивільнити 0,2 робочого часу. Так як з системою працює 10 робітників, то система умовно вивільнить 2 робітників.

Визначимо пряму економічну ефективність, ґрунтуючись на тому, що впровадження системи вивільнить 2 робітників.

Річна платня за рахунок вивільнення робочого часу складе

$$\Delta Cn = 12000*2*12 - 13247,71 = 274752,29 \text{ грн.}$$

Річний економічний ефект розраховується за наступною формулою:

$$Э_{год} = \Delta C_n - E_n \cdot k$$

де E_n – нормативний коефіцієнт економічної ефективності капітальних вкладень у галузь і для обчислювальної техніки приймається 0,5;

k – додаткові капітальні вкладення з урахуванням витрат на проектування, створення і функціонування системи.

$$Эгод = 274\,752,29 – 0,5 * 162\,552,61 = 193\,475,98 \text{ (грн).}$$

Строк окупності підсистеми

$$T = k / {}_n\Delta C,$$

тобто

$$T = 162\,552,61 / 274\,752,29 = 0,6 \text{ (року).}$$

Таким чином, витрати на створення розподіленої інформаційної систем окупляться протягом 0,6 року.

5 ОХОРОНА ПРАЦІ

Охорона праці – це система правових, соціально-економічних, організаційно технічних, санітарно-гігієнічних і лікувально-профілактичних заходів і засобів, спрямованих на збереження життя, здоров'я й працездатності людини в процесі трудової діяльності (Закон України "Про охорону праці").

Головною метою охорони праці є створення на кожному робочому місці безпечних умов праці, безпечної експлуатації обладнання, зменшення або повна нейтралізація дії шкідливих і небезпечних виробничих факторів на організм людини і, як наслідок, зниження виробничого травматизму та професійних захворювань.

Дія закону про охорону праці поширюється на всіх юридичних та фізичних осіб, які відповідно до законодавства використовують найману працю, та на всіх працюючих.

Якщо міжнародним договором, згода на обов'язковість якого надана Верховною Радою України, встановлено інші норми, ніж ті, що передбачені законодавством України про охорону праці, застосовуються норми міжнародного договору.

Державна політика в галузі охорони праці визначається відповідно до Конституції України (254к/96-ВР) Верховною Радою України і спрямована на створення належних, безпечних і здорових умов праці, запобігання нещасним випадкам та професійним захворюванням.

Державна політика в галузі охорони праці базується на принципах:

– пріоритету життя і здоров'я працівників, повної відповідальності роботодавця за створення належних, безпечних і здорових умов праці;

– підвищення рівня промислової безпеки шляхом забезпечення суцільного технічного контролю за станом виробництв, технологій та продукції, а також сприяння підприємствам у створенні безпечних та нешкідливих умов праці;

– комплексного розв'язання завдань охорони праці на основі загальнодержавної, галузевих, регіональних програм з цього питання та з урахуванням інших напрямів економічної і соціальної політики, досягнень в галузі науки і техніки та охорони довкілля;

– соціального захисту працівників, повного відшкодування шкоди особам, які потерпіли від нещасних випадків на виробництві та професійних захворювань;

– встановлення єдиних вимог з охорони праці для всіх підприємств та суб'єктів підприємницької діяльності незалежно від форм власності та видів діяльності;

– адаптації трудових процесів до можливостей працівника з урахуванням його здоров'я та психологічного стану;

– використання економічних методів управління охороною праці, участі держави у фінансуванні заходів щодо охорони праці, залучення добровільних внесків та інших надходжень на ці цілі, отримання яких не суперечить законодавству;

– інформування населення, проведення навчання, професійної підготовки і підвищення кваліфікації працівників з питань охорони праці;

– забезпечення координації діяльності органів державної влади, установ, організацій, об'єднань громадян, що розв'язують проблеми охорони здоров'я, гігієни та безпеки праці, а також співробітництва і проведення консультацій між роботодавцями та працівниками (їх представниками), між усіма соціальними групами під час прийняття рішень з охорони праці на місцевому та державному рівнях;

– використання світового досвіду організації роботи щодо поліпшення умов і підвищення безпеки праці на основі міжнародного співробітництва.

– Державне управління охороною праці в Україні здійснюють:

– Кабінет Міністрів України;

– центральний орган виконавчої влади, що реалізує державну політику у сфері охорони праці;

– міністерства та інші центральні органи виконавчої влади.

5.1 Аналіз небезпечних та шкідливих факторів, що впливають на людину при розробці програмного забезпечення та його експлуатації

5.1.1 Аналіз шкідливого впливу на користувача ПК

На користувачів персональних комп’ютерів (ПК) впливають наступні фактори виробничого середовища:

- електронебезпечність;
- шум;
- освітленість;
- пожежна небезпечність;
- статична електрика;
- електромагнітні поля і випромінювання;
- пил (вентиляція);
- робоче середовище.

5.1.2 Мікроклімат

У результаті життєдіяльності людей змінюються фізичні властивості і хімічний склад повітря закритих приміщень. У видихуваному людьми повітрі кількість CO2 збільшується з 0,04 до 4,4 %. У погано вентильованих приміщеннях з'являються неприємні заходи, які можуть бути результатом розкладання органічних речовин на поверхні шкіри, білизни й одягу людину, вогкості стін, кухонних приміщень, убиралень і т.д. Навіть короткочасне перебування в такій атмосфері знижує працездатність, погіршує загальне самопочуття, може викликати поява головного болю, нудоту, блювоту.

5.1.3 Пожежонебезпека

Найчастіше зустрічаються термічні ураження шкіри, рідше — термічні і

хімічні опіки порожнини рота і дихальних шляхів, ще рідше — опіки стравоходу і шлунку.

Термічні опіки шкіри розділяють на 4 ступені:

- I ступінь (легкий) — вражається тільки зовнішній шар шкіри виявляється розлитою червоністю, набряком шкіри і сильним пекучим болем в місці ураження;
- II ступінь — вражається як епідерміс, так і шари шкіри під ним, почервоніння і набряк шкіри виражені значніше і супроводяться утворенням міхурів, заповнених прозорою рідиною, яка потім швидко каламутніє;
- III А ступінь — частковий некроз шкіри із збереженням острівців епітелію, з яких за сприятливих умов можлива самостійна епітелізація;
- III Б ступінь — некроз шкіри на всю її глибину;
- IV ступінь — обвуглювання, ураження не тільки шкіри, але і тканин, що знаходяться під нею.

Поверхневі опіки площею до 10% поверхні тіла і глибокі до 5% поверхні протікають як місцеві ураження. Опіки більшої площі викликають специфічні зміни у всьому організмі і розглядаються як опікова хвороба. При важких опіках - більше 8–10% тіла або поверхневих опіках більше 10–15% поверхні розвивається опіковий шок.

5.2 Заходи з техніки безпеки

На робочому місці оператора повинні бути створені умови для високопродуктивної праці. Оператор зазнає значне навантаження, як фізичне (сидяче положення, навантаження на очі), так і розумове, що приводить до зниження його працездатності до кінця робочого дня.

Для зниження шкідливого впливу комп'ютера на людину необхідно дотримуватись визначених вимог до умов роботи і робочого місця; комп'ютер

також повинен відповідати гігієнічним вимогам. Крім того, необхідно строго дотримуватись режиму роботи на комп'ютері. Розглянемо докладніше ці вимоги.

Кожен комп'ютер повинен мати сертифікат республіканського центра санепіднагляду, сертифікат відповідності ГОСТу, технічний паспорт і т.ін. При перевірці рекомендується звертати увагу на наступні параметри: розмір екрана по діагоналі - 31 см, частота кадрового розгорнення ≥ 70 Гц, розбірливість зображення, яскравість знака, фарбування знака (при монохромному зображенні рекомендується жовто-зелений колір знаків на темному тлі, при кольоровому - не більш 7 кольорів одночасно), відсутність геометричних перекручувань. Корпус комп'ютера, клавіатура й інші блоки і пристрої повинні мати матову поверхню (без блискучих деталей, здатних створювати відблиски). З метою захисту від електромагнітних і електростатичних полів треба використовувати екранні фільтри, спеціальні екрани, інші засоби індивідуального захисту, що пройшли іспити і мають відповідний гігієнічний сертифікат.

До приміщення, у якому розміщається комп'ютер, пред'являються такі вимоги: об'єм приміщення повинний бути не менш 24 м3 (на один комп'ютер), вікна приміщення повинні бути орієнтовані на північ, північний схід. Віконні прорізи повинні бути обладнані регульованими пристроями типу жалюзі, зовнішніх козирків і т.ін.

Для підлоги рекомендується поливинилхлоридне антистатичне покриття (без килимів). Аналогічні рекомендації для стін (панелі), дверей. Вище панелей елательні звуковбирні матеріали для зниження рівня шуму. Рекомендується також застосовувати сучасну техніку, тому що на ній установлені звуковбирні пристрої.

Для обробки приміщень не можна використовувати матеріали, що виділяють шкідливі хімічні речовини: ДСП, шпалери що миються, плівкові, рулонні синтетичні матеріали, шаруватий паперовий пластик. Штори повинні бути з щільних натуральних тканин, вони не повинні пропускати світло.

Оптимальні параметри мікроклімату: температура – 19..21 оС, відносна вологість повітря – 55..65 %. Систематично перед початком роботи необхідно

наскрізне провітрювання і вологе прибирання. Це забезпечить якісний склад повітря в приміщенні. Якщо дозволяють погодні умови , працювати краще при відкритих вікнах, а для підвищення вологості повітря використовувати зволожувачі або установити ємності з водою поблизу опалювальних приладів. Зміст шкідливих хімічних речовин у повітрі приміщення з ЕОМ не повинен перевищувати середньодобових концентрацій для атмосферного повітря.

До робочого місця вимоги наступні: відстань від вікна не менш 0,8..1 м. Світильники розташовуються ліворуч від комп'ютера, паралельно лінії зору. Освітлення може бути природним, штучним (при закритих шторах), а також змішаним. Штучне освітлення повинне здійснюватися системою загального рівномірного освітлення. (Рекомендуються люмінесцентні лампи денного кольоророзподілу). Освітленість на поверхні столу в зоні розміщення робочого документа повинна бути 30-50 лк. Допускається установка світильників місцевого освітлення для підсвічування документів. У них можна застосовувати лампи накалювання. Для комп'ютера потрібний спеціальний одномісний стіл (один стіл для розміщення комп'ютера, інший – для клавіатури). Крісло або стілець повинні регулюватися по висоті («вертушка»), кути лопаток повинні торкатися спинки стільця. Робоча поза – пряма, злегка нахил уперед. Оптимальна відстань від екрана до очей 0,6 м – 0,7 м. Рівень очей повинний приходиться на центр екрана або 2/3 його висоти.

Режим роботи на комп'ютері при дотриманні всіх гігієнічних вимог – не більш 5 – 6 годин для дорослого, при цьому через кожні 20..30 хвилин потрібно робити перерви на 5 – 10 хвилин, щоб зняти зорове стомлення, статичну електрику, зробити комплекс фізичних вправ, що поліпшують функціональні стани центральної нервової системи, дихальної системи, мозкового кровообігу і ліквідують застійні явища нижньої половини тіла, ніг, плечового пояса. Два рази в рік необхідний контроль зору.

Роботу необхідно організувати таким чином, щоб найбільш складні задачі вирішувалися з 11:00 до 16:00 – у період найбільшої активності людини, а не на

початку дня, коли оператор ще не досяг максимальної активності, і не наприкінці дня, коли вже розвивається стомлення. Оскільки робота оператора не пов'язана з рішенням великих логічних задач і досить одноманітна, то рекомендується по можливості чередувати види діяльності.

5.2.1 Електрична безпека

Широке застосування електрики змушує приділяти велику увагу питанням електричної безпеки. Вплив струму може привести до електричної травми, тобто ушкодженню організму електричним струмом, чи електричною дугою. Винятково важливе значення для запобігання електричного травматизму має правильна організація обслуговування діючих електричних установок, яка установлена “Правилами технічної експлуатації електроустановок споживачів” і “Правилами установки електрообладнання”. Лабораторія відноситься до категорії приміщень без підвищеної небезпеки.

Для запобігання електротравматизму необхідно застосовувати найбільш дешевий і ефективний спосіб захисту, яким є захисне заземлення. Принцип дії заземлення полягає в багаторазовому зменшенні струму, що протікає через людину у випадку витоку струму.

5.2.2 Захист від шуму

- Захист від шуму на робочому місці здійснюється наступними методами:
- зменшення шуму;
- застосування засобів колективного захисту
- застосування засобів індивідуального захисту;
- раціональне планування приміщень;
- акустична обробка приміщень.

Для боротьби із шумом необхідно застосовувати наступні заходи:

- збільшення звукоізоляції конструкцій, що огороджують приміщення;

- ущільнення по периметру дверей, що перекривають проходи;
- зменшення впливу джерел шуму шляхом застосування прокладок з еластичних матеріалів, звукових екранів.

5.2.3 Вентиляція

Однією з необхідних умов здорової і високопродуктивної праці є забезпечення чистоти повітря і нормальних метеорологічних умов у робочій зоні приміщень, тобто просторі висотою до 2 м над рівнем підлоги чи площадки, де знаходяться робочі місця.

Атмосферне повітря у своєму складі містить (% за обсягом): азоту – 78,08; кисню – 20,95; аргону, неону й інших інертних газів – 0,93; вуглекислого газу – 0,03; інших газів – 0,01. Повітря такого складу найбільш сприятливе для дихання.

У приміщенні необхідно забезпечити прилив свіжого повітря, кількість якого визначається техніко-економічним розрахунком і вибором схеми вентиляції.

Вентиляція – організований повітрообмін, що полягає у видаленні з робочого приміщення забрудненого повітря і подачі замість нього свіжого зовнішнього чи очищеного повітря. У залежності від призначення, вентиляція буває: приточна; витяжна.

Необхідно приділити увагу обмеженню кількості пилу в повітрі, тому що це безпосередньо впливає на надійність і ресурс експлуатації устаткування.

5.2.4 Пожежна безпека

Запобігання пожежі досягається виключенням утворення запального середовища і джерел загоряння. Пожежний захист реалізується:

- застосуванням незапальних речовин і матеріалів;
- обмеженням поширення пожежі;
- створенням умов для евакуації людей;
- застосування протидимового захисту;
- застосування пожежної сигналізації.

Для ліквідації пожеж застосовуються наступні засоби пожежогасіння:

- внутрішні пожежні водоводи;
- вогнегасники ручні і пересувні;
- сухий пісок;
- азбестові ковдри.

Пожежні крани встановлюють у коридорах і нішах на висоті 1,35 м, де також знаходяться пожежний рукав з пожежним стволом. Застосовуються пінні вогнегасники ОХП–10, ОХВП–10 і ручні вуглекислотні вогнегасники ОУ–2, ОУ–5, ОУ–8. Ручні вогнегасники встановлюють у приміщенні з розрахунку один вогнегасник на 40 – 50 м2 площі, але не менше двох у приміщенні.

5.2.5 Статична електрика

Для запобігання утворенню і захисту від статичної електрики необхідно використовувати нейтралізатори й зволожувачі, а підлоги повинні мати антистатичне покриття. Захист повинен проводиться відповідно до санітарно-гігієнічних норм напруженості електростатичного поля - рівень напруженості не повинен перевищувати 20 кВ/м в продовж години.

Висновки до розділу 4

В даному розділі нами були проведен аналіз небезпечних та шкідливих факторів, що впливають на людину при розробці програмного забезпечення та його експлуатації. Також були приведині рекомендації при роботі на ПК:

– при роботі з ПК необхідно робити 15-хвилинні перерви через кожних 2 години, а при інтенсивній роботі – через 1 годину і навіть півгодини;

– під час роботи на ПК необхідно слідкувати, щоб лінія руки в області зап’ястя залишалась прямою, зап’ястя були розслаблені, а пальці трохи зігнуті; не напружуйте руки, зігніть їх у ліктях приблизно під прямим кутом;

– підлокітники робочого місця повинні бути опорою для рук як при роботі з клавіатурою, так і користуванні мишею (при цьому клавіатура і миша повинні

розміщуватися так, щоб до них не потрібно було тягнутися);

– під час роботи сидіти прямо чи з нахиленим корпусом вперед, намагаючись зберегти природній згин тіла в поясниці;

– регулярно робити вправи для очей;

– поверхня стола, клавіатури і корпуси ПК повинні бути одного кольору;

– у приміщенні, де встановлено ПК, необхідно підтримувати відносну вологість повітря не нижче 40% з метою зменшення шкідливого впливу електростатичного поля;

рекомендується відсунути все обладнання ПК (і взагалі все, що включено в електричну мережу) на 60 – 90 см від робочо місця.

6 ОХОРОНА НАВКОЛИШНЬОГО СЕРЕДОВИЩА

6.1 Вступ до проблеми

Охорона навколишнього середовища здійснюється різними, у тому числі й правовими, засобами. При цьому в правових формах захищаються переважно всі компоненти, які утворюють природне середовище.

Сучасними головними нормативно-правовими актами що регулюють основи організації охорони навколишнього природного середовища, є Закони України «Про охорону навколишнього природного середовища» від 25 червня 1991 р., «Про охорону атмосферного повітря» від 16 жовтня 1992 р., «Про природно-заповідний фонд України» від 16 червня 1992 р., «Про тваринний світ» від 3 березня 1993 р., «Про карантин рослин» від 30 червня 1993 р та інші. До того ж деякі відносини у сфері використання і охорони навколишнього природного середовища врегульовані кодексами (земельним, водним, лісовим, про надра), а також Законами України «Про плату за землю» від 3 липня 1992 р., «Про ветеринарну медицину» від 25 червня 1992 р. Важливе значення у вирішенні цього питання має затверджений Постановою Верховної Ради «Порядок обмеження, тимчасової заборони (зупинення) чи припинення діяльності підприємств, установ, організацій і об'єктів у разі порушення ними законодавства про охорону навколишнього природного середовища».

Різновидами права природокористування є: право землекористування, право водокористування, право лісокористування, право користуватися надрами, право користуватися тваринним світом, право користування природно-заповідним фондом. Право природокористування це процесі раціонального використання людиною природних ресурсів для задоволення різних потреб та інтересів. Найважливішими принципами природокористування є його цільовий характер, плановість і тривалість, ліцензування, врахування надзвичайного значення у житті

суспільства тощо. При цьому виділяють такі групи природокористування, як право загального і спеціального використання землі, вод, лісів, надр, тваринного світу та інших природних ресурсів. Суб'єктами права загального користування природними ресурсами можуть бути, згідно з Законом України «Про охорону навколишнього природного середовища», усі громадяни для задоволення найрізноманітніших потреб і інтересів. Воно здійснюється громадянами безкоштовно і безліцензійно, тобто для цього не потрібен відповідний дозвіл уповноважених органів і осіб. Загальним є, наприклад, використання парків, скверів, водойм, лісів, збір дикорослих ягід, грибів, горіхів і т. ін. Право загального природокористування закріплене у ст. 13 Конституції України: «Кожний громадянин має право користуватися природними об'єктами права власності народу відповідно до закону». Похідним від загального природокористування є спеціальне використання природних ресурсів. На відміну від першого, це використання конкретних природних ресурсів, що здійснюється громадянами, підприємствами, установами і організаціями у випадках, коли відповідна, визначена у законодавстві частина природних ресурсів передається їм для використання. Як правило, така передача має вартість і визначена в часі. Надання природних ресурсів відбувається на основі спеціальних дозволів державних актів на право постійного користування.

Крім прав суб'єктів, як природокористувачів, сучасною юридичною наукою сформовані й інтенсивно розвиваються екологічні права і обов'язки. Так, у Конституції України записано, що «кожен має право на безпечне для життя і здоров'я довкілля та на відшкодування завданої порушенням цього права шкоди. Кожному гарантується право вільного доступу до інформації про стан довкілля, про якість харчових продуктів і предметів побуту, а також право на її поширення». Аналогічні формулювання є й у Законі України «Про охорону навколишнього природного середовища», бо це право одне з основних прав людини. Цьому праву відповідає обов'язок держави забезпечувати здійснення санітарно-гігієнічних заходів, спрямованих на поліпшення та оздоровлення навколишнього природного середовища. Усі екологічні права громадян захищаються і відновлюються у

судовому порядку. Поряд з правами Закон України «Про охорону навколишнього природного середовища» передбачає і певні обов'язки громадян. Так, незалежно від того, є громадяни природокористувачами, чи ні, вони зобов'язані берегти природу, раціонально використовувати її запаси, не завдавати шкоди. Крім того, Закон України «Про охорону навколишнього природного середовища» покладає на громадян і підприємства, установи й організації, як суб'єктів спеціального використання природних ресурсів, спеціальні обов'язки. Так, плата за спеціальне природокористування встановлюється на основі нормативів плати і лімітів використання природних ресурсів. Ці нормативи визначаються з урахуванням розповсюдження природних ресурсів, їх якості, можливості використання, місцезнаходження, можливості переробки і зберігання відходів. До того ж суб'єкти спеціального природокористування зобов'язані сплачувати певні кошти за забруднення навколишнього природного середовища, що встановлюються за викиди у атмосферу забруднюючих речовин; скидання забруднюючих речовин на поверхню води, у територіальні і морські води, а також під землю.

Контроль у сфері природо-використання і охорони навколишнього природного середовища здійснюється шляхом перевірки, нагляду, обстеження, інвентаризації та експертиз. Він може здійснюватись як уповноваженими державними органами, так і громадськими формуваннями. Державний контроль покладається на Ради народних депутатів, державні адміністрації та Міністерство охорони навколишнього природного середовища і його органи на місцях.

До основних пріоритетів охорони довкілля та раціонального використання природних ресурсів належать:

– гарантування екологічної безпеки ядерних об'єктів і радіаційного захисту населення та довкілля, зведення до мінімуму шкідливого вплив наслідків аварії на Чорнобильській АЕС;
– поліпшення екологічного стану басейнів рік України та якості питної води;
– стабілізація та поліпшення екологічного стану в містах і промислових центрах Донецько-Придніпровського регіону;

– будівництво нових та реконструкція діючих потужностей комунальних очисних каналізаційних споруд;
– запобігання забрудненню Чорного та Азовського морів і поліпшення їх екологічного стану;
– формування збалансованої системи природокористування та адекватна структурна перебудова виробничого потенціалу економіки, екологізація технологій у промисловості, енергетиці, будівництві, сільському господарстві, на транспорті;
– збереження біологічного та ландшафтного різноманіття, заповідна справа.

Для досягнення цього передбачається вирішення таких завдань:

1. Зменшення до мінімуму рівня радіаційного забруднення;

2. Захист повітряного басейну від забруднення, насамперед у великих містах і промислових центрах;

3. Захист і збереження земельних ресурсів від забруднення, виснаження і нераціонального використання;

4. Збереження і розширення територій з природним станом ландшафту, посилення природоохоронної діяльності на заповідних і рекреаційних територіях;

5. Ппідвищення стійкості та екологічних функцій лісів;

6. Знешкодження, утилізація та захоронення промислових та побутових відходів;

7. Запобігання забрудненню морських і внутрішніх вод, зменшення та припинення скиду забруднених стічних вод у водні об'єкти, захист підземних вод від забруднення;

8. Збереження та відродження малих річок, здійснення управління водними ресурсами на основі басейнового принципу;

9. Завершення створення державної системи моніторингу навколишнього природного середовища;

10.Створення системи прогнозування, запобігання та оперативних дій у разі надзвичайних ситуацій природного і природно-техногенного походження;

11.Забезпечення екологічного супроводу процесу конверсії військово-промислового комплексу;

12.Здійснення заходів щодо екологічного контролю за діяльністю Збройних Сил України;

13.Розробка механізмів реалізації схем природокористування;

14.впровадження дійових економічних складових впливу на систему природокористування;

15.створення системи екологічної освіти, виховання та інформування.

6.2 Забруднення навколишнього середовища підприємством з розробки програмного забезпечення

Основними чинниками забруднення навколишнього середовища фірмою є лише використання автотранспорту. Бо підприємство окрім забруднення повітряного середовища не забруднює ні водне, ні ґрунтове.

В сучасних умовах автомобільний транспорт стає найбільш значним джерелом забруднення атмосферного повітря, особливо великих міст.

Відомо, що атмосферне повітря міст постійно забруднюється і за всіма параметрами докорінно відрізняється від повноцінного природного повітря. Міські поселення характеризуються найвищими рівнями антропогенних навантажень на навколишнє середовище, в результаті чого воно деформується, набуває якісно нових рис, аж до зміни мікрокліматичних факторів і фізико- хімічних властивостей середовища, зокрема повітряного басейну. Метеорологічні спостереження свідчать, що температура повітря в межах міських територій у середньому на декілька градусів вища, ніж у приміських районах. Над містами, особливо великими, частіше випадають атмосферні опади, бувають густі тумани, а також смоги – густі тумани, змішані з димом, кіптявою та вихлопними газами. Прозорість атмосфери в містах менша, ніж за її межами і в сільській місцевості. Тумани, а також

запиленість повітря помітно зменшують проникнення до земної поверхні сонячних променів.

Однак за рахунок автомобільних викидів якість атмосферного повітря містах погіршилась.

Прогресуючому забрудненню атмосфери в містах сприяє висока питома вага автомобілів, адже зростання кількості автотранспортних засобів супроводжується збільшенням об'ємів забруднюючих речовин із вихлопних труб. Останнім часом у міському повітрі виріс об'єм оксидів вуглецю, вуглеводнів, оксидів азоту, сажі. Але найбільшу небезпеку, окрім оксидів азоту,складають сірчані та свинцеві сполуки. Їх вміст у міському повітрі значною мірою виріс. Місто не пристосоване до такої кількості автотранспорту. Довжина пробігу без зупинок між світлофорами становить лише 400–600 м., внаслідок цього середня швидкість руху вдень у центрі міста і на великих автошляхах знижується до 12–20 км/год, а це збільшує витрати палива в 3–4 рази. Відповідно збільшуються й викиди забруднюючих речовин. Автотранспорт також призводить до специфічних форм забруднення повітря. При русі стираються шини і тисячі тонн гуми у вигляді пилу потрапляє в повітря. Автомобільний транспорт не тільки забруднює повітря продуктами згорання палива, він сприяє зростаючому надходженню свинцю в навколишнє середовище. В Україні поки ще використовують бензин із вмістом свинцю 0,36 г/л, тоді як в Англії, Німеччині та США – 0,013–0,15.

6.3 Розробка заходів щодо зменшення забруднення

Природоохоронною є будь-яка діяльність, спрямована на збереження якості навколишнього середовища на рівні, що забезпечує стійкість біосфери. До неї відноситься як великомасштабна, здійснювана на загальнодержавному рівні діяльність по збереженню еталонних зразків недоторканої природи ізбереженню розмаїтості видів на Землі, організації наукових досліджень, підготовці фахівців-екологів і вихованню населення, так і діяльність окремих підприємств по

очищенню від шкідливих речовин стічних вод і відхідних газів, зниженню норм використання природних ресурсів і т.д. Така діяльність здійснюється в основному інженерними методами.

Існують два основних напрямки природоохоронної діяльності підприємств. Перший – очищення шкідливих викидів. Цей шлях «у чистому вигляді» малоефективний, тому що з його допомогою далеко не завжди вдається цілком припинити надходження шкідливих речовин у біосферу. До того ж скорочення рівня забруднення одного компонента навколишнього середовища веде до посилення рівня забруднення іншого [8].

І, наприклад, встановлення вологих фільтрів при газоочищенні дозволяє коротити забруднення повітря, але веде до ще більшого забруднення води. Уловлені з відхідних газів і зливальних вод речовини часто отруюють значні земельні площі.

Використання очисних споруд, навіть найефективніших, різко скорочує рівень забруднення навколишнього середовища, однак не вирішує цієї проблеми цілком, оскільки в процесі функціонування цих установок теж виробляються відходи, хоча й у меншому обсязі, але, як правило, з підвищеною концентрацією шкідливих речовин. Нарешті, робота більшої частини очисних споруджень вимагає значних енергетичних витрат, що, у свою чергу, теж небезпечно для навколишнього середовища.

Крім того, забруднювачі, на знешкодження яких йдуть величезні засоби, являють собою речовини, на які уже витрачена праця і які за рідкісним винятком можна було б використовувати в народному господарстві.

Для досягнення високих еколого-економічних результатів необхідно процес очищення шкідливих викидів сполучити з процесом утилізації уловлених речовин, що уможливить об'єднання першого напрямку з другим.

Другий напрямок – усунення самих причин забруднення, що вимагає розробки маловідходних, а в перспективі і безвідхідних технологій виробництва, які

дозволяли б комплексно використовувати вихідну сировину й утилізувати максимум шкідливих для біосфери речовин [8].

Однак далеко не для усіх виробництв знайдені прийнятні техніко- економічні рішення по різкому скороченню кількості відходів, що утворюються, і їх утилізації, тому на даний час доводиться працювати в обох зазначених напрямках.

Піклуючись про удосконалювання інженерної охорони навколишньої природного середовища, треба пам'ятати, що ніякі очисні спорудження і безвідхідні технології не зможуть відновити стійкість біосфери, якщо будуть перевищені припустимі (граничні) значення скорочення природних, не перетворених людиною природних систем, у чому виявляється чинність закону незамінності біосфери.

Таким порогом може виявитися використання більш 1% енергетики біосфери і глибоке перетворення більш 10% природних територій (правила одного і десяти відсотків). Тому технічні досягнення не знімають необхідності рішення проблем зміни пріоритетів суспільного розвитку, стабілізації народонаселення, створення достатнього числа заповідних територій і інших, розглянутих раніше.

Основними напрямками робіт в галузі захисту атмосфери від забруднення викидами автотранспорту є:

а) створення і розширення виробництва автомобілів з високоекономічними і малотоксичними двигунами, у тому числі подальша дизелізація автомобілів;

б) розвиток робіт зі створення і впровадження ефективних систем нейтралізації відпрацьованих газів;

в) зниження токсичності моторних палив;

г) розвиток робіт з раціональної організації руху автотранспорту в містах, удосконаленню дорожнього будівництва з метою забезпечення невпинного руху на автомагістралях.

ВИСНОВОК

В дипломній роботі досліджено методи захисту відеоархіву та визначено що використання симетричного алгоритму для шифрування відеоархіву підходить найбільше. Коефіцієнт захищеності складає 89%. Проаналізовано загрози інформаційній безпеці відеокомплексу охоронної фірми. Розглянуто ринок програмного забезпечення захисту відеоінформації від несанкціонованого доступу.

Спроектована та реалізована інформаційна підсистема для захисту відеоархіву від несанкціонованого доступу. Розроблено алгоритмічне та програмне забезпечення для захисту відеоархіву від несанкціонованого доступу. Запропонований програмний комплекс реалізує отримання, зберігання та захист передавання відеоінформації користувачам. Конфіденційність інформації забезпечується за рахунок шифрування її з використанням симетричного алгоритму.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу, затверджений наказом ДСТСЗІ СБ України від 28.04.1999 № 22.

2. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації автоматизованій системі.

3. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України.

4. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу Зі Зміною №1, затвердженою наказом Адміністрації Держспецзв'язку від 15.10.2008 № 172.

5. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.

6. Блинцов В.С. Привязные подводные системы – К.: Наукова думка, 1998. – 232 с.

7. Блінцов О.В. Прив'язна підводна система з централізованим інформаційним обміном. // VIII міжнародна науково-технічна конференція «Гіротехнології, навігація, керування рухом та конструювання космічно-авіаційної техніки»: Зб. доп.: У 4 ч. – К.: НТУУ «КПІ», 2011. – Ч. ІІІ. – С. 12-19.

8. Жидецький В.Ц. Основи охорони праці. Підручник. – Вид. 5-е, доповнене. – Львів: Афіша,. 2000р. 350 с.

9. Жидецький В.Ц. Охорона праці користувачів комп'ютерів. Навчальний посібник. – Вид. 2-е доп. Львів: Афіша, 2001. – 176 с

10. Мельников В. Захист інформації в комп'ютерних системах. М.: Фінанси і статистика, Електронінформ, 1997 – 368 с.

11. BitLocker URL: https://technet.microsoft.com/ru-ru/library/dd835565(v=ws.10).aspx.

12. CyberSafe URL: http://cybersafesoft.com/rus/.

13. DiskCryptor URL: https://diskcryptor.net/.

14. LibreCrypt URL: https://github.com/t-d-k/LibreCrypt.

15. Symantec EE URL: https://www.symantec.com/products/information-protection/encryption/endpoint-encryption.

16. TrueCrypt URL: https://truecrypt.ch/.

17. VeraCrypt URL: https://veracrypt.codeplex.com/.