Харківський національний університет імені В.Н. Каразіна

Факультет комп’ютерних наук

Безпека інформаційних систем і технологій

«Допущено до захисту»

Зав.кафедрою БІСТ

Сватовський І.І.

«07» червня 2023р.

Пояснювальна записка

до кваліфікаційної роботи бакалавра

спеціальність: 125 Кібербезпека

на тему: «Дослідження методів забезпечення конфіденційності інформації, яка отримується та зберігається в системі відеоспостереження»

оцінка « » Керівник Сватовський І.І.
(прізвище та ініціали/підпис)

Голова ЕК Рецензент Бакуменко Н.С
(прізвище та ініціали/підпис)

Лемешко О.В._____ Виконавець студент групи КБ-42

Левченко Д.О.
(прізвище та ініціали/підпис)

Харків – 2023

РЕФЕРАТ

Обсяг роботи – 17907, кількість додатків – 1, кількість джерел - 80

Мета:

виявлення та розробка ефективних методів та технологій, які можуть допомогти у забезпеченні конфіденційності та безпеки інформації, яка отримується та зберігається в системі.

Методи дослідження - аналіз літературних джерел та законодавства, аналіз потенційних загроз та вразливостей

Результати роботи та їх новизна - аналіз потенційних загроз та вразливостей системи відеоспостереження вказує на необхідність застосування комплексних заходів забезпечення безпеки, включаючи використання сучасних алгоритмів шифрування, контролю доступу та аудиту дій користувачів.

Рекомендації щодо використання результатів роботи:

a) При проектуванні та встановленні систем відеоспостереження, необхідно передбачати та застосовувати ефективні методи забезпечення конфіденційності, такі як шифрування, маскування, анонімізація та обмеження доступу до інформації.

b) Необхідно регулярно проводити аудит систем відеоспостереження та оцінювати їх безпеку, щоб вчасно виявляти та усувати вразливості, а також покращувати захист даних.

c) При зберіганні та обробці даних, отриманих в системі відеоспостереження, необхідно дотримуватись вимог законодавства щодо захисту персональних даних, зокрема, даних, які містяться на відеозаписах.

Значущість роботи та висновки - результати дослідження методів забезпечення конфіденційності інформації, яка отримується та зберігається в системі відеоспостереження, є дуже важливими в контексті захисту особистих даних та приватності користувачів систем відеоспостереження. Зокрема, було досліджено різні методи захисту інформації, такі як шифрування, маскування, анонімізація та обмеження доступу до інформації, та оцінено їх ефективність в контексті захисту конфіденційності даних. Було встановлено, що використання цих методів може значно покращити рівень захисту даних в системах відеоспостереження.

Перелік ключових слів - конфіденційність даних, система відеоспостереження, захист персональних даних, безпека даних, захисні методи, захист інформації.

ABSTRACT

Volume of work - 17907, number of applications - 1, number of sources - 80

Purpose:

identifying and developing effective methods and technologies that can help ensure the confidentiality and security of information received and stored in the system.

Research methods - analysis of literary sources and legislation, analysis of potential threats and vulnerabilities

The results of the work and their novelty - the analysis of potential threats and vulnerabilities of the video surveillance system indicates the need to apply comprehensive security measures, including the use of modern encryption algorithms, access control and auditing of user actions.

Recommendations regarding the use of work results:

a) When designing and installing video surveillance systems, it is necessary to foresee and apply effective methods of ensuring privacy, such as encryption, masking, anonymization and limiting access to information.

b) It is necessary to conduct regular audits of video surveillance systems and assess their security in order to timely identify and eliminate vulnerabilities, as well as improve data protection.

c) When storing and processing data received in the video surveillance system, it is necessary to comply with the requirements of the law on the protection of personal data, in particular, data contained in video recordings.

Significance of the work and conclusions - the results of the study of the methods of ensuring the confidentiality of the information received and stored in the video surveillance system are very important in the context of the protection of personal data and the privacy of users of video surveillance systems. In particular, various methods of information protection, such as encryption, masking, anonymization, and limiting access to information, were investigated and their effectiveness in the context of data privacy protection was evaluated. It was established that the use of these methods can significantly improve the level of data protection in video surveillance systems.

List of keywords - data privacy, video surveillance system, personal data protection, data security, protective methods, information protection.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ ТА СИМВОЛІВ

VPN	-	Virtual private network
UPS	-	Uninterruptible power supply
GDPR	-	General Data Protection Regulation
HIPAA	-	Health Insurance Portability and Accountability Act
ISO	-	International Organization for Standardization
TRA	-	Threat and Risk Assessment
SSL	-	Secure Sockets Layer
TLS	-	Transport Layer Security
IoT	-	Internet of things
SQL	-	Structured Query Language
DDoS	-	Denial-of-service attack
MFA	-	Multi-factor authentication
AES	-	Advanced Encryption Standard
DES	-	Data Encryption Standard
RSA	-	Rivest-Shamir-Adleman

ВСТУП

В сучасному світі обмін інформацією став неодмінною частиною життя як приватних осіб, так і компаній. Збільшення кількості даних, які зберігаються та передаються через різні системи, зробило безпеку цих даних надзвичайно важливою. Інформація, яка не забезпечена належним рівнем конфіденційності, може бути підвергнута крадіжці, порушенню приватності, або використана проти власника цієї інформації. У зв'язку з цим, дослідження методів забезпечення конфіденційності інформації, яка отримується та зберігається в системі, є актуальною та важливою темою в галузі інформаційної безпеки. Ці методи включають у себе різноманітні технічні та організаційні заходи, такі як шифрування даних, контроль доступу, аудит безпеки та інші. У цьому дослідженні буде розглянуто різні методи забезпечення конфіденційності інформації та їх застосування в системах зберігання та передачі даних. Метою дослідження є виявлення найефективніших методів забезпечення конфіденційності інформації та їх відповідність вимогам сучасного ринку інформаційних технологій. У сучасному світі, коли великі обсяги інформації зберігаються в електронному вигляді та передаються через різні мережі, важливо забезпечити конфіденційність цих даних. Компанії, які займаються зберіганням та обробкою конфіденційної інформації, повинні бути впевнені в тому, що ці дані не потраплять в руки неправомірних осіб. Тому, забезпечення конфіденційності інформації в системі є надзвичайно важливим завданням для бізнесу та організацій. Для цього використовуються різноманітні методи, такі як шифрування даних, контроль доступу, аудит безпеки та інші. Шифрування даних є одним з найпоширеніших методів забезпечення конфіденційності інформації. Воно дозволяє перетворити дані в такий формат, який може бути розшифрований лише з використанням спеціального ключа. Контроль доступу передбачає встановлення правил, що регулюють доступ до конфіденційної

інформації. Аудит безпеки включає в себе моніторинг та аналіз поведінки користувачів системи, що дозволяє виявити та запобігти можливим порушенням безпеки. Дослідження методів забезпечення конфіденційності інформації допоможе зрозуміти, які методи є найбільш ефективними та відповідають вимогам сучасного ринку інформаційних технологій. Таке дослідження може бути корисним як для приватних компаній, так і для державних органів, що займаються зберіганням та обробкою конфіденційної інформації. Дослідження методів забезпечення конфіденційності інформації також включає в себе вивчення технічних аспектів захисту інформації, таких як захист від вірусів, хакерських атак та інших загроз. Крім того, це дослідження може допомогти встановити найбільш ефективні процедури безпеки, такі як резервне копіювання даних та відновлення інформації в разі її втрати чи пошкодження. Для успішного застосування методів забезпечення конфіденційності інформації, необхідно також забезпечити належне навчання та підтримку персоналу, що використовує систему. Це означає проведення навчання щодо правил безпеки та поширення знань про можливі загрози та способи їх запобігання. Нарешті, важливо розуміти, що забезпечення конфіденційності інформації є постійним процесом, який потребує постійного вдосконалення та оновлення. З'являються нові методи атак та загрози, які вимагають нових методів захисту, тому необхідно відслідковувати та аналізувати останні тренди в галузі безпеки інформації та підлаштовувати свої методи захисту відповідно до нових вимог і стандартів.

Актуальність: дослідження методів забезпечення конфіденційності інформації, яка отримується та зберігається в системі, є вельми високою в наш час, оскільки зростає кількість загроз кібербезпеці, пов'язаних зі зламами, витоками даних, шахрайством, шпигунством та іншими видами кібератак. Інформаційні системи стали невід'ємною частиною більшості сфер діяльності, інформація, що зберігається в цих системах, може бути вкрадена, знищена або пошкоджена, що може спричинити серйозні проблеми для підприємств, установ та окремих осіб.

Підвищення рівня кібербезпеки стало однією з головних тем для дослідження в останні роки. Дослідження методів забезпечення конфіденційності інформації, яка отримується та зберігається в системі, дозволяє розробляти нові технології та методики, які допоможуть зменшити ризики порушення безпеки інформації та забезпечити її надійний захист. Окрім того, у зв'язку зі стрімким розвитком технологій, що використовуються для зберігання та обробки інформації, виникає необхідність постійного вдосконалення методів захисту від нових загроз. Також, з поширенням обміну даними через мережу Інтернет, виникає необхідність в захисті конфіденційності інформації від зловмисників з усього світу. Також, у зв'язку зі збільшенням кількості кібератак та кіберзлочинності, більшість країн світу почали розробляти та приймати законодавство, яке регулює захист інформації. Дослідження методів забезпечення конфіденційності інформації є важливим кроком для розробки та вдосконалення законодавчих актів у галузі кібербезпеки. Також, зростає попит на спеціалістів у галузі кібербезпеки, які мають знання та досвід у захисті інформації від кібератак та використання сучасних методів та технологій захисту. Дослідження методів забезпечення конфіденційності інформації допомагає підготувати таких фахівців та забезпечує їх кваліфіковану підготовку для вирішення складних завдань в галузі кібербезпеки. Отже, актуальність дослідження методів забезпечення конфіденційності інформації, яка отримується та зберігається в системі, надзвичайно висока в наш час і важлива для забезпечення безпеки та захисту інформації в сучасному світі. Дослідження методів забезпечення конфіденційності інформації має важливе значення для бізнесу, організацій та держав. У сучасних умовах, коли більшість даних зберігається в електронному вигляді, їх захист від кібератак та крадіжок стає дедалі важливішим завданням. В разі втрати або пошкодження важливої інформації може зазнати значної шкоди не лише сама компанія, а й її клієнти, партнери та співробітники. Дослідження методів забезпечення конфіденційності інформації також допомагає розвивати нові технології та

підходи до захисту даних. Наприклад, блокчейн технологія дозволяє забезпечити безпеку даних, зберігаючи їх у розподіленій системі, що ускладнює доступ до них для зловмисників. Також дослідження методів шифрування, двофакторної автентифікації, контролю доступу та інших заходів захисту інформації є надзвичайно важливим для розробки нових систем безпеки. Крім того, дослідження методів забезпечення конфіденційності інформації також стає важливим для захисту особистої інформації користувачів в Інтернеті, так як більшість людей надає свої дані в мережі. Для захисту приватної інформації користувачів в Інтернеті також необхідно розробляти нові методи та технології, які забезпечать конфіденційність даних та запобігатимуть їх використанню в кіберзлочинності.

Мета:

виявлення та розробка ефективних методів та технологій, які можуть допомогти у забезпеченні конфіденційності та безпеки інформації, яка отримується та зберігається в системі.

Основні завдання роботи:

1) Огляд існуючих методів забезпечення конфіденційності в системах відеоспостереження. Це включає аналіз протоколів шифрування, методів контролю доступу та інших методів забезпечення конфіденційності.
2) Вивчення специфіки збору та зберігання відеоінформації. Це включає розуміння того, як відео може бути записано, збережено, передано та використано в майбутньому.
3) Аналіз потенційних загроз безпеці відеоінформації. Це включає вивчення методів зламу протоколів шифрування, виявлення іншого шкідливого програмного забезпечення, зловживання дозволами користувачів та інших методів, які можуть загрожувати конфіденційності відеоінформації.

Об'єктом дослідження є – система відеоспостереження

Предметом дослідження є – методи конфіденційності та їх аналіз та пов'язаних аспектів у об'єкті дослідження

1 ТЕОРЕТИЧНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ІНФОРМАЦІЇ

1.1 Дослідження основних понять та термінів

Дослідження методів забезпечення конфіденційності інформації, яка отримується та зберігається в системі відеоспостереження включає такі поняття і терміни:

a) Конфіденційність - це властивість інформації, яка обмежує доступ до неї лише авторизованих осіб або систем.
b) Шифрування - це процес перетворення звичайного тексту на криптографічно стійкий формат за допомогою алгоритмів шифрування.
c) Дешифрування - це процес перетворення зашифрованого тексту на звичайний текст за допомогою ключа шифрування.
d) Аутентифікація - це процес перевірки ідентифікаційних даних користувача, які він надає для доступу до системи.
e) Авторизація - це процес надання доступу до системи користувачеві з певними привілеями та обмеженнями.
f) Криптографічний ключ - це послідовність символів, яку використовують для шифрування та дешифрування інформації.
g) Цифровий підпис - це електронний еквівалент ручного підпису, який забезпечує автентичність та цілісність документа.
h) Протокол SSL/TLS - це протокол забезпечення захищеної передачі даних через мережу Інтернет за допомогою шифрування.
i) Пароль - це секретний код, який використовується для авторизації користувача в системі.

j) Безпека інформації - це процес захисту інформації від несанкціонованого доступу, використання, модифікації та знищення.

Дослідження методів забезпечення конфіденційності інформації, яка отримується та зберігається в системі відеоспостереження є важливим процесом в забезпеченні безпеки та захисту приватності осіб. Системи відеоспостереження використовуються в багатьох сферах, таких як науково-дослідна робота, охорона, промисловість, медицина, комерційний та муніципальний сектори. Забезпечення конфіденційності інформації в системах відеоспостереження є надзвичайно важливим, оскільки вони можуть містити конфіденційні дані, такі як особисті дані, фінансову інформацію, комерційну та державну інформацію. Для забезпечення конфіденційності інформації в системах відеоспостереження використовуються різні методи, такі як шифрування даних, автентифікація та авторизація користувачів, захист мережевих з'єднань за допомогою SSL/TLS-протоколів, використання сильних паролів, а також захист збереження даних за допомогою криптографічних алгоритмів. У сучасному світі, де застосовуються системи відеоспостереження в різних сферах діяльності, забезпечення конфіденційності та захисту приватності стають все більш актуальними питаннями. Наприклад, у сфері медицини, відеоспостереження може бути застосовано для моніторингу пацієнтів, але ці дані мають бути оброблені та збережені з дотриманням всіх правил конфіденційності та приватності. Захист відеоданих може забезпечуватись за допомогою різних методів. Одним з найпоширеніших методів є шифрування, що передбачає перетворення вхідних даних у форму, що неможлива для розуміння без знання спеціального ключа. Шифрування може бути застосовано як для зберігання відеоданих, так і для їх передачі по мережі. Іншим методом є автентифікація та авторизація користувачів. Це дозволяє забезпечити доступ лише авторизованим користувачам та встановити різні рівні доступу в залежності від потреб користувача. Для захисту мережевих з'єднань застосовуються SSL/TLS-протоколи, які забезпечують захищені канали зв'язку

між різними пристроями. Крім того, захист відеоданих може бути забезпечено за допомогою використання сильних паролів та криптографічних алгоритмів для зберігання даних. У деяких випадках може бути корисним використання псевдоанонімізації даних, що дозволяє зберегти корисну інформацію, але при цьому знизити ризик викриття особистих даних. При цьому, інформація може бути використана для різних цілей, наприклад, для аналізу трафіку, розробки нових алгоритмів та технологій, тощо. Додатковою мірою захисту може бути використання мультифакторної аутентифікації, що дозволяє підвищити рівень безпеки захищеного доступу. Це може бути здійснено, наприклад, за допомогою використання біометричних технологій, таких як відбитки пальців, розпізнавання обличчя або голосу. Усі ці методи можуть бути застосовані окремо або в комбінації для забезпечення найвищого рівня захисту конфіденційної інформації, яка отримується та зберігається в системі відеоспостереження. Важливо також пам'ятати про дотримання вимог законодавства щодо захисту особистих даних та конфіденційності. Окрім зазначених методів забезпечення конфіденційності інформації, яка отримується та зберігається в системі відеоспостереження, можна використовувати й інші заходи захисту. Наприклад, можна використовувати шифрування даних, що передаються між пристроями в системі відеоспостереження. Шифрування дозволяє захистити дані від несанкціонованого доступу та перехоплення. Для шифрування можуть використовуватись різні алгоритми, наприклад, AES, DES, RSA, тощо. Також можна використовувати системи виявлення вторгнень (IDS) та системи запобігання вторгнень (IPS), що дозволяють виявити та запобігти несанкціонованому доступу до системи відеоспостереження. IDS та IPS можуть бути реалізовані як програмні або апаратні рішення. Однак, важливо пам'ятати, що забезпечення конфіденційності даних в системі відеоспостереження повинно бути збалансоване з іншими цілями, такими як забезпечення безпеки та ефективності відеоспостереження. Наприклад, використання шифрування може збільшити обсяг обробки даних та затримати відповідь системи. Тому,

важливо забезпечити адекватний рівень захисту даних, що не обмежуватиме ефективність відеоспостереження та інших функцій системи. Ще одним методом забезпечення конфіденційності даних в системі відеоспостереження є розподіл доступу до даних. Цей метод передбачає, що доступ до даних в системі відеоспостереження буде мають лише користувачі з необхідними правами доступу. Для цього можна використовувати систему авторизації та аутентифікації користувачів, яка дозволяє забезпечити відповідність між ідентифікатором користувача та його правами доступу до даних в системі. Крім того, можна використовувати фізичні методи забезпечення конфіденційності, наприклад, захищені приміщення, у яких знаходяться сервери з даними системи відеоспостереження. У таких приміщеннях можна використовувати системи контролю доступу, які дозволяють забезпечити доступ до приміщення лише авторизованим користувачам. Нарешті, важливо забезпечити регулярне оновлення програмного забезпечення системи відеоспостереження, в тому числі оновлення заходів забезпечення конфіденційності. Оновлення дозволяють усувати виявлені уразливості, які можуть бути використані зловмисниками для несанкціонованого доступу до даних в системі відеоспостереження. Загалом, забезпечення конфіденційності даних в системі відеоспостереження є важливим завданням, що вимагає комплексного підходу та застосування різних методів захисту. Такий підхід дозволяє забезпечити високий рівень захисту даних від несанкціонованого доступу та зберегти ефективність та безпеку відеоспостереження. Ще одним методом забезпечення конфіденційності даних в системі відеоспостереження є застосування шифрування. Шифрування може використовуватись для захисту даних під час їх передачі по мережі та під час їх зберігання на серверах системи відеоспостереження. Існують різні методи шифрування, включаючи симетричне та асиметричне шифрування. Симетричне шифрування використовує один ключ для шифрування та розшифрування даних, тоді як асиметричне шифрування використовує два ключі - публічний та приватний. Публічний ключ використовується для шифрування даних, тоді як

приватний ключ використовується для їх розшифрування. Застосування шифрування дозволяє забезпечити захист даних від перехоплення та несанкціонованого доступу до них. Це особливо важливо для систем відеоспостереження, де даними можуть бути зображення людей, їх поведінка та інша конфіденційна інформація. Також, важливо забезпечити захист даних від вірусів та інших шкідливих програм. Для цього можна використовувати антивірусне програмне забезпечення, яке дозволяє виявляти та блокувати шкідливі програми. Нарешті, важливим аспектом забезпечення конфіденційності даних в системі відеоспостереження є навчання користувачів та персоналу системи. Користувачі та персонал системи повинні бути свідомі ризиків несанкціонованого доступу до даних та знати, як правильно використовувати систему та її інструменти для забезпечення конфіденційності даних. Загалом, забезпечення конфіденційності даних в системі відеоспостереження є важливим завданням для забезпечення безпеки та приватності людей. При розробці та експлуатації системи відеоспостереження необхідно враховувати потенційні загрози та використовувати заходи забезпечення конфіденційності даних, такі як аутентифікація, авторизація, шифрування та контроль доступу. Крім того, при зборі та обробці даних в системі відеоспостереження необхідно дотримуватись вимог законодавства щодо захисту персональних даних та приватності осіб. Для цього можна використовувати різноманітні інструменти, наприклад, забезпечувати анонімізацію даних, зменшення роздільної здатності зображення, встановлювати правила зберігання та видалення даних. Для забезпечення конфіденційності даних в системі відеоспостереження можуть використовуватись різні методи та технології. Один з них - шифрування даних. Шифрування може бути застосоване як при збереженні даних на пристрої, так і при передачі їх по мережі. Шифрування забезпечує захист від несанкціонованого доступу до даних шляхом перетворення зрозумілого тексту в нечитабельний формат, що може бути розшифрований тільки за допомогою

відповідного ключа. Іншим методом забезпечення конфіденційності даних в системі відеоспостереження є встановлення систем контролю доступу. Система контролю доступу дозволяє встановлювати обмеження на доступ до даних та обладнання системи відеоспостереження для окремих користувачів або груп користувачів. Це може бути реалізовано, наприклад, шляхом використання різних рівнів доступу для різних користувачів, аутентифікації користувачів за допомогою паролів або ідентифікаційних карток. Також для забезпечення конфіденційності даних можуть використовуватись різні методи анонімізації даних, такі як зменшення роздільної здатності зображення або заміна обличчя людей на зображенні на замінники. Це дозволяє зберігати дані відображення, не втрачаючи важливої інформації, але зменшуючи ризик порушення приватності людей.

1.2 Аналіз методів забезпечення конфіденційності інформації

Існує безліч методів забезпечення конфіденційності інформації, і кожен з них має свої переваги та недоліки. Ось деякі з найбільш поширених методів:

1) Шифрування - це процес перетворення зрозумілої інформації в кодований вигляд, що забезпечує її конфіденційність. Він забезпечує високий рівень безпеки, оскільки навіть якщо зловмисник зможе отримати доступ до зашифрованої інформації, він не зможе розшифрувати її без відповідного ключа. Однак шифрування може бути досить трудомістким і вимагати значних ресурсів.
2) Хешування - це процес перетворення будь-якої вхідної інформації в унікальний вихідний код фіксованої довжини. Хеші можуть використовуватися для збереження конфіденційної інформації, такої як паролі, без збереження самої інформації. Це забезпечує високий рівень безпеки, оскільки навіть якщо зловмисник зможе отримати доступ до хешу, він не зможе отримати оригінальну інформацію.

Однак хешування не може бути зворотним процесом, тому оригінальна інформація не може бути відновлена з хешу.

3) Політики доступу до інформації - це система, що встановлює правила доступу до інформації в залежності від рівня довіри та потреб користувачів. Цей метод забезпечує високий рівень конфіденційності, оскільки користувачі отримують доступ лише до необхідної для їх роботи інформації. Однак система політик доступу може бути досить складною у налаштуванні та вимагати регулярного аудиту.
4) Фізичні методи - це методи, що включають у себе фізичний захист інформації, такий як захист приміщень, контроль доступу та маркування конфіденційної інформації. Цей метод забезпечує високий рівень безпеки, оскільки фізичний захист є складним для обходу для зловмисників. Однак фізичні методи можуть бути досить дорогими та складними у впровадженні.

Забезпечення конфіденційності інформації є важливою задачею для будь-якої організації, незалежно від її розміру та спеціалізації. Існує декілька основних причин, чому організації повинні забезпечувати конфіденційність своєї інформації:

1) Збереження конкурентної переваги: у бізнесі конфіденційність є важливим фактором, який допомагає зберегти конкурентну перевагу та захистити інтелектуальну власність організації.
2) Захист від крадіжки даних: конфіденційна інформація може бути цінною метою для зловмисників, які можуть використовувати її для вчинення крадіжок ідентифікаційних даних, фінансових даних та інших видів шахрайства.
3) Захист від витоку інформації: витік конфіденційної інформації може призвести до серйозних наслідків для організації, таких як втрата довіри клієнтів, фінансові втрати та порушення репутації.

Для забезпечення конфіденційності інформації організації можуть використовувати не тільки технічні та організаційні методи, але й навчання персоналу. Важливо, щоб кожен працівник розумів значення конфіденційності інформації та знав, як правильно зберігати та обробляти конфіденційну інформацію. Іншим викликом є забезпечення конфіденційності в хмарному середовищі. Захист даних у хмарних сервісах може бути складнішим, оскільки дані зберігаються на серверах, які знаходяться за межами контролю організації. Для забезпечення конфіденційності в хмарному середовищі можуть використовуватися різні методи, такі як шифрування даних та двофакторна аутентифікація. Крім того, важливо забезпечувати конфіденційність під час передачі даних, особливо через відкриті мережі, такі як Інтернет. Для забезпечення конфіденційності під час передачі даних можуть використовуватися різні методи, такі як використання протоколів шифрування та віртуальних приватних мереж. Одним із важливих аспектів забезпечення конфіденційності є захист від внутрішнього зловживання. Внутрішній загрози можуть виникнути в результаті дій співробітників організації, які мають доступ до конфіденційної інформації. Для забезпечення захисту від внутрішніх загроз можуть використовуватися методи, такі як обмеження доступу до конфіденційної інформації, моніторинг дій співробітників та інші. Окрім того, важливо забезпечувати конфіденційність відносно зовнішніх сторін, таких як партнери та клієнти організації. Для цього можуть використовуватися різні методи, такі як підписання нерозголошування, що гарантує, що конфіденційна інформація не буде передана третім сторонам без дозволу організації. Окрім технічних заходів, важливо також забезпечити конфіденційність шляхом підвищення свідомості співробітників організації. Розуміння значення конфіденційності та правил поведінки щодо конфіденційної інформації може бути важливим фактором у забезпеченні її безпеки. Усі ці методи та підходи до забезпечення конфіденційності є важливими і мають свої переваги та недоліки. Вибір методів залежить від конкретних потреб та характеристик організації.

Однак, незалежно від того, які методи застосовуються, забезпечення конфіденційності є важливим елементом у збереженні довіри клієнтів та забезпеченні успішної діяльності організації. Дотримання принципів конфіденційності також може допомогти у запобіганні правових проблем та штрафів, пов'язаних з порушенням прав на захист персональних даних. Крім того, в сучасному світі дефіцит довіри є серйозною проблемою, особливо в сфері електронної комунікації та віртуальної взаємодії. Забезпечення конфіденційності може допомогти підвищити рівень довіри споживачів та клієнтів до організації, що може позитивно позначитися на її репутації та успішності. Один з головних викликів забезпечення конфіденційності інформації полягає в тому, що сучасні технології зробили її збереження значно складнішим завданням, ніж раніше. З одного боку, інформація може бути збережена на серверах та базах даних, що розташовані у різних країнах світу, що ускладнює контроль за її зберіганням та передачею. З іншого боку, зростає кількість загроз, які можуть стати причиною витоку конфіденційної інформації, таких як кібератаки, шахрайство, внутрішні проблеми безпеки, помилки персоналу та багато інших. Тому для забезпечення конфіденційності інформації необхідно використовувати комплексний підхід, який включає у себе як технічні заходи, так і правові та організаційні. Серед технічних методів можна відзначити шифрування даних, захист мереж та систем від злому, використання механізмів аутентифікації, контроль доступу та моніторинг системи безпеки. Організаційні заходи включають в себе розробку політики конфіденційності, навчання персоналу, забезпечення фізичної безпеки приміщень, контроль за зберіганням документів та інформації. Правові заходи включають в себе використання захисту прав на інтелектуальну власність, законодавчі заходи щодо захисту персональних даних, контроль за відповідністю різних нормативних актів та правил. Отже, забезпечення конфіденційності інформації є складним процесом, який потребує комплексного підходу та співпраці всіх сторін, що займаються збереженням та обробкою інформації. Важливо не

тільки забезпечити захист від потенційних загроз, але й вчасно реагувати на події та проблеми, що можуть виникнути. Для цього важливо мати ефективну систему моніторингу та відстеження потенційних загроз і проблем. Крім того, у світі постійно змінюються технології та підходи до збереження та обробки інформації, тому необхідно постійно оновлювати знання та компетенції спеціалістів у цій сфері. Тільки так можна забезпечити ефективний та надійний захист конфіденційної інформації, що є важливим для успішного функціонування підприємств та організацій. Для забезпечення конфіденційності інформації важливо також мати чітко визначені правила та процедури її обробки та збереження. Це може включати у себе вимоги до паролів та їх частоти зміни, регулярну перевірку наявності вразливостей у системі, заборону використання простих паролів та збереження інформації на захищених серверах з обмеженим доступом. Також важливо мати план надзвичайних ситуацій та процедури реагування на них, щоб в разі потенційної загрози швидко та ефективно забезпечити захист інформації та зменшити можливі наслідки. У сучасному світі, де інформація є одним з найцінніших активів, захист конфіденційної інформації є надзвичайно важливим завданням. Недостатня увага до цього питання може призвести до витоку конфіденційної інформації, що може спричинити серйозні наслідки для підприємств та організацій, а також порушити довіру клієнтів та партнерів. Тому, захист конфіденційної інформації повинен бути на першому місці для будь-якої організації або підприємства. Однією з найважливіших складових захисту конфіденційної інформації є культура безпеки в організації. Це означає, що всі співробітники повинні бути свідомі ризиків та вміти захищати конфіденційну інформацію, яку вони обробляють. Це може включати у себе навчання співробітників правилам безпеки та створення культури, в якій захист конфіденційної інформації є нормою поведінки та відповідальністю кожного співробітника. Для забезпечення безпеки інформації також можуть використовуватися різноманітні технології, які забезпечують захист від

потенційних загроз. Наприклад, це можуть бути криптографічні алгоритми, що дозволяють захистити дані від несанкціонованого доступу, або системи перевірки автентичності, які забезпечують, що доступ до інформації має лише авторизована особа. У сучасному світі, коли обробка та передача інформації відбувається з використанням різноманітних технологій та мереж, захист конфіденційної інформації є важливим завданням. Для забезпечення безпеки інформації необхідно використовувати комплексний підхід, який включає в себе як технічні, так і організаційні заходи.

Висновки до першого розділу

У розділі 1 було проведено аналіз теоретичних аспектів забезпечення конфіденційності інформації в системах відеоспостереження. Були визначені основні поняття та терміни, пов'язані з цією темою, проаналізовано різні методи забезпечення конфіденційності та порівняно їх ефективність. В результаті проведеного дослідження було зроблено висновок, що забезпечення конфіденційності інформації в системах відеоспостереження є актуальною проблемою, яка потребує вирішення. Різні методи забезпечення конфіденційності мають свої переваги та недоліки, і вибір конкретного методу повинен залежати від потреб користувачів системи відеоспостереження та вимог до захисту конфіденційної інформації. Для подальшого дослідження рекомендується розглянути можливість комбінування різних методів забезпечення конфіденційності, щоб отримати максимальний ефект захисту інформації. Також слід розглянути можливість використання новітніх технологій, таких як штучний інтелект та машинне навчання, для поліпшення забезпечення конфіденційності в системах відеоспостереження.

2 МЕТОДИ ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ІНФОРМАЦІЇ В СИСТЕМАХ ВІДЕОСПОСТЕРЕЖЕННЯ

2.1 Аналіз переваг та недоліків кожного з методів

У сучасному світі системи відеоспостереження стали необхідним елементом безпеки, адже вони дозволяють зафіксувати події та рухи на визначеній території. Однак, збір та обробка відеоданих можуть створювати загрозу конфіденційності та приватності людей. Тому, забезпечення конфіденційності інформації в системах відеоспостереження є дуже важливою задачею. Розглянемо деякі методи забезпечення конфіденційності інформації в системах відеоспостереження та їх переваги та недоліки.

1) Замаскування чутливих зон

Цей метод полягає у замаскуванні зон, де можуть знаходитись чутливі дані, такі як особисті дані про людей або конфіденційні дані. Це можна зробити шляхом додавання чорних полів або блоків, що перекривають чутливі зони на відео. Цей метод є простим та ефективним, але він може призвести до обмежень у покритті території та ускладнення аналізу відеоданих.

2) Шифрування відеоданих

Цей метод полягає в застосуванні шифрування для захисту відеоданих від несанкціонованого доступу. Відеодані можна шифрувати під час передачі їх з камер до центрального сервера, або зберігання їх на сервері. Шифрування відеоданих забезпечує високий рівень захисту даних, але воно може збільшувати витрати на обробку відеоданих та знижувати швидкість передачі даних.

3) Псевдоанонімізація даних

Цей метод полягає в зміні даних про людей на фейкові дані, що не можуть бути пов'язані з реальними даними. Наприклад, можна замінити обличчя людини на схожі фотографії або замінити номер автомобіля на випадковий номер. Цей метод забезпечує високий рівень конфіденційності та приватності даних, але він може знижувати точність відеоаналізу та ускладнювати процес ідентифікації.

4) Використання системи доступу за принципом "необхідний доступ"

Цей метод полягає в обмеженні доступу до відеоданих тільки для осіб, які мають необхідний доступ до цих даних. Така система забезпечує високий рівень захисту від несанкціонованого доступу до відеоданих, але вона може бути менш ефективною при використанні систем відеоспостереження з масштабним покриттям.

Недоліки та переваги вищезазначених методів забезпечення конфіденційності інформації в системах відеоспостереження можуть бути такі:

- Замаскування чутливих зон: Простий та ефективний метод, але може обмежувати зону покриття та ускладнювати аналіз відеоданих.
- Шифрування відеоданих: Забезпечує високий рівень захисту від несанкціонованого доступу до відеоданих, але може збільшувати витрати на обробку відеоданих та знижувати швидкість передачі даних.
- Псевдоанонімізація даних: Забезпечує високий рівень конфіденційності та приватності даних, але може знижувати точність відеоаналізу та ускладнювати процес ідентифікації.

У кожного методу є свої переваги та недоліки, тому при виборі методу забезпечення конфіденційності важливо враховувати конкретні потреби та вимоги системи відеоспостереження. Наприклад, якщо система відеоспостереження використовується в приміщенні з високим рівнем доступу, то кращим вибором буде метод доступу за принципом "необхідний доступ". У

разі, якщо система відеоспостереження використовується в публічному місці, де важливо захистити конфіденційні дані, метод шифрування відеоданих може бути кращим варіантом. Крім того, важливо забезпечити правильну конфігурацію та моніторинг системи відеоспостереження, щоб забезпечити високий рівень захисту даних. Також необхідно враховувати законодавчі вимоги до збору та зберігання особистих даних, оскільки недотримання цих вимог може призвести до серйозних правових наслідків. Для забезпечення конфіденційності інформації в системах відеоспостереження можна також використовувати методи обробки даних. Наприклад, можна застосовувати методи анонімізації, при яких інформація про конкретну особу замінюється на інші дані, які не можуть бути пов'язані з особою. Таким чином, зменшується ризик розголошення конфіденційної інформації. Також можна використовувати методи маскування, при яких частини зображення, що містять конфіденційну інформацію, замінюються на інші дані або приховуються за допомогою спеціальних фільтрів. Метод маскування може бути корисним у випадках, коли важливо забезпечити конфіденційність зображення, наприклад, при відображенні інформації про платіжні картки або інші особисті дані. Недоліками методів забезпечення конфіденційності можуть бути підвищені витрати на їх впровадження та обслуговування. Наприклад, метод шифрування вимагає додаткового обладнання та програмного забезпечення для шифрування та розшифрування даних, що може збільшити загальні витрати на систему відеоспостереження. Крім того, методи забезпечення конфіденційності можуть зменшити якість відео та ускладнити процес обробки та аналізу даних, що може призвести до втрати важливої інформації. Також важливим елементом забезпечення конфіденційності інформації в системах відеоспостереження є забезпечення цілісності та доступності даних. Цілісність даних означає, що дані залишаються незмінними та невикривленими протягом всього періоду їх зберігання, а доступність даних означає, що дані можуть бути доступними та користуватися ними у необхідний момент. Для забезпечення цілісності та

доступності даних можуть використовуватися різні методи, такі як резервне копіювання даних, регулярна перевірка стану системи та забезпечення її стійкості до можливих атак. Важливо також враховувати можливі ризики, пов'язані з використанням обладнання та програмного забезпечення, які можуть призвести до втрати даних або порушення їх цілісності. Для забезпечення конфіденційності інформації в системах відеоспостереження також важливо використовувати методи шифрування даних. Шифрування даних дозволяє захистити їх від несанкціонованого доступу та забезпечити їх конфіденційність. Шифрування може бути застосовано для захисту як даних, що передаються по мережі, так і даних, що зберігаються на серверах. Для підтримки ефективного функціонування системи відеоспостереження та забезпечення безперебійності роботи важливо забезпечити необхідні ресурси, такі як достатній рівень пропускної здатності мережі, достатньої потужності серверів та міцності обладнання. Також важливо забезпечити регулярне оновлення програмного забезпечення та обладнання для запобігання можливих вразливостей та захисту системи від нових загроз. Одним з найбільших викликів для забезпечення конфіденційності інформації в системах відеоспостереження є баланс між захистом даних та захистом прав людей на приватність. У багатьох країнах існують законодавчі норми та регуляції, що регулюють використання систем відеоспостереження та обмежують їхнє застосування, щоб забезпечити права та свободи людей. Такі обмеження можуть впливати на можливість використання систем відеоспостереження в різних випадках та вимагати відповідного рівня контролю та дотримання правил. Одним зі способів забезпечення конфіденційності інформації в системах відеоспостереження є шифрування даних. Шифрування дозволяє захистити передачу даних між камерами відеоспостереження та сервером від несанкціонованого доступу. Це забезпечує захист від перехоплення чутливої інформації, такої як відеозаписи, від зловмисників. Також можуть використовуватись інші методи, такі як маскування та затемнення зон, щоб забезпечити приватність індивідів, які

перебувають в зоні відеоспостереження. Наприклад, зони, де присутні чутливі дані, такі як PIN-коди, можуть бути затемнені, щоб забезпечити їхню конфіденційність. Недоліками таких методів можуть бути складність їх впровадження та високі витрати на установку та підтримку системи. Також можуть виникати труднощі з визначенням дійсного рівня захисту, оскільки ці методи не завжди є абсолютно ефективними та можуть піддаватись атакам. Однак, враховуючи ризики та вимоги, що ставляться до систем відеоспостереження, використання цих методів захисту може допомогти забезпечити конфіденційність даних та захист. Для того, щоб забезпечити оптимальний рівень захисту конфіденційної інформації, слід враховувати потенційні загрози та ризики. Наприклад, при проектуванні систем відеоспостереження слід враховувати потенційні місця атак, такі як підключення до системи підроблених камер або хакерські атаки на сервер, який зберігає відеодані. Крім того, слід забезпечити відповідний рівень захисту для обробки та зберігання конфіденційної інформації. Також важливо розробляти та впроваджувати процедури забезпечення безпеки для протидії загрозам внутрішнього та зовнішнього характеру, таким як зловмисні дії персоналу, крадіжки, втрати даних або випадкові помилки. Наприклад, можна встановити систему відеоспостереження на території, що охороняється, віддаленість від якої дозволить зменшити ризик несанкціонованого доступу. Крім того, слід забезпечити відповідний рівень обізнаності та навчання персоналу, який працює з системою відеоспостереження. Це допоможе підвищити рівень свідомості щодо загроз, які можуть бути пов'язані зі зберіганням та обробкою конфіденційної інформації, а також до того, як краще захистити цю інформацію від можливих атак. Додатково, важливо враховувати етичні та правові аспекти використання систем відеоспостереження з метою захисту конфіденційної інформації. Наприклад, при зберіганні та обробці персональних даних (таких як зображення облич, відбитки пальців тощо) слід дотримуватися відповідних правил, встановлених законодавством, та забезпечувати доступ до такої

інформації лише за відповідних умов та з дозволу власника даних. У загальному, забезпечення конфіденційності інформації в системах відеоспостереження - це складний та важливий процес, який вимагає постійного вдосконалення та оновлення системи захисту, а також уважного врахування етичних та правових аспектів використання таких систем. Тому, для досягнення максимального рівня конфіденційності інформації в системах відеоспостереження необхідно використовувати комплексний підхід, що включає в себе не лише методи шифрування та анонімізації даних, але й правильно налаштовану систему доступу до інформації та захист від зловмисних атак. Також важливо забезпечувати постійний моніторинг системи та регулярне оновлення її захисту для запобігання вразливостей та викривлення конфіденційної інформації.

2.2 Дослідження найбільш ефективного методу забезпечення конфіденційності в системах відеоспостереження

Дослідження найбільш ефективного методу забезпечення конфіденційності в системах відеоспостереження залежить від конкретної ситуації та потреб користувачів. Однак, для визначення найбільш оптимального методу забезпечення конфіденційності можна використовувати підходи, які базуються на аналізі ризиків та вимог щодо захисту даних.

Аналіз ризиків - це процес визначення можливих загроз та вразливостей системи відеоспостереження, їхньої імовірності та наслідків, а також визначення заходів для запобігання та мінімізації ризиків.

Вимоги щодо захисту даних - це вимоги до забезпечення конфіденційності, цілісності та доступності інформації, що визначаються законодавством, стандартами та політиками організації.

Під час дослідження найбільш ефективного методу забезпечення конфіденційності в системах відеоспостереження слід враховувати такі фактори, як:

- Тип даних, що збираються та їхнє значення для організації;
- Рівень конфіденційності даних;
- Рівень доступу до даних та потреби в забезпеченні доступу до них;
- Вимоги до збереження даних;
- Вимоги до забезпечення надійності та цілісності даних;
- Фінансові обмеження та бюджет організації;
- Інші фактори, що можуть впливати на вибір методу забезпечення конфіденційності.

Під час порівняння різних методів забезпечення конфіденційності в системах відеоспостереження слід враховувати переваги та недоліки кожного методу. Наприклад, метод шифрування даних є досить надійним, проте може вплинути на швидкість обробки даних та потребує додаткових ресурсів. Метод маскування даних забезпечує високий рівень конфіденційності, проте не забезпечує захисту від несанкціонованого доступу до даних. Метод анонімізації даних може забезпечити високий рівень конфіденційності, але може призвести до втрати корисної інформації. Окрім того, при виборі методу забезпечення конфіденційності в системах відеоспостереження слід враховувати можливість його реалізації та підтримки, зокрема, наявність відповідних програмних та апаратних засобів. Також слід враховувати вартість впровадження та підтримки методу забезпечення конфіденційності. Крім того, при дослідженні найбільш ефективного методу забезпечення конфіденційності в системах відеоспостереження, слід враховувати контекст використання системи відеоспостереження. Наприклад, для захисту даних від несанкціонованого доступу в промислових майданчиках може бути більш ефективним

застосування методу маскування даних, а в банківських відділеннях - методу шифрування даних. Також варто враховувати законодавчі вимоги до захисту персональних даних та конфіденційності відеоматеріалів. Наприклад, в Європейському Союзі діє Загальний регламент про захист персональних даних (GDPR), який встановлює вимоги до збору, обробки та зберігання персональних даних. Також існують вимоги до захисту даних відповідно до національного законодавства, які слід враховувати при виборі методу забезпечення конфіденційності в системах відеоспостереження. Нарешті, важливо враховувати вплив методу забезпечення конфіденційності на функціональність системи відеоспостереження. Наприклад, метод маскування даних може вплинути на зручність перегляду відеоматеріалів, а метод шифрування даних може вплинути на швидкість передачі даних. Тому важливо бути уважним при виборі методу забезпечення конфіденційності, щоб забезпечити баланс між рівнем захисту даних та функціональністю системи відеоспостереження. Також важливим аспектом при дослідженні найбільш ефективного методу забезпечення конфіденційності в системах відеоспостереження є оцінка витрат на впровадження та підтримку методу. Наприклад, метод шифрування даних може бути дуже ефективним у захисті конфіденційності, але вимагатиме значних витрат на впровадження та підтримку системи шифрування. У той же час, метод маскування даних може бути менш витратним, але менш ефективним у захисті конфіденційності. Для оцінки ефективності методу забезпечення конфіденційності можуть використовуватися різні показники, такі як рівень захисту даних, швидкість передачі даних, витрати на впровадження та підтримку методу, відповідність законодавчим вимогам тощо. При виборі методу забезпечення конфіденційності в системах відеоспостереження також слід звертати увагу на можливість інтеграції з іншими системами безпеки та засобами контролю доступу. Наприклад, використання методу шифрування даних, який може бути інтегрований з системою контролю доступу, дозволяє забезпечити більш

високий рівень захисту даних. Існує багато факторів, які можуть вплинути на вибір найбільш ефективного методу забезпечення конфіденційності в системах відеоспостереження. Деякі з цих факторів включають рівень ризику для конфіденційної інформації, вартість різних методів, наявність необхідного обладнання та технічної експертизи, а також можливість розширення інфраструктури. Один зі способів визначення найбільш ефективного методу забезпечення конфіденційності полягає в проведенні аудиту безпеки. Аудит безпеки - це процес оцінки потенційних ризиків для безпеки інформації та визначення ефективності існуючих заходів забезпечення безпеки. Після аудиту безпеки можна з'ясувати, які методи забезпечення конфіденційності використовуються в системі відеоспостереження, які ризики існують, які заходи можна прийняти для зменшення ризику, і які методи найбільш ефективні. Також варто звернути увагу на те, що найбільш ефективний метод забезпечення конфіденційності може залежати від контексту використання. Наприклад, у деяких випадках краще використовувати метод шифрування даних, а в інших - фізичний доступ до обладнання. Тому важливо оцінювати контекст використання та здійснювати відповідні налаштування для забезпечення максимального рівня конфіденційності інформації. Також для аналізу найбільш ефективного методу забезпечення конфіденційності в системах відеоспостереження можна використовувати аналіз ризиків. Аналіз ризиків - це процес визначення потенційних загроз безпеці та оцінки ризиків їх виникнення. В результаті аналізу можуть бути визначені різні сценарії ризику та рекомендації щодо забезпечення конфіденційності. Наприклад, при аналізі ризиків може бути виявлено, що найбільша загроза для конфіденційності інформації полягає у можливому несанкціонованому доступі до записів відеоспостереження. У цьому випадку можуть бути запропоновані різні методи забезпечення конфіденційності, такі як використання паролів та біометричних ідентифікаторів для авторизації користувачів, використання шифрування для захисту даних, фізичний контроль над доступом до обладнання тощо. Також

варто зазначити, що для визначення найбільш ефективного методу забезпечення конфіденційності може бути корисним вивчення досвіду використання таких систем у схожих умовах. Наприклад, якщо в інших організаціях використовуються певні методи забезпечення конфіденційності в системах відеоспостереження з успіхом, ці методи можуть бути і для даної організації. Ще одним методом забезпечення конфіденційності в системах відеоспостереження є застосування технологій анонімізації. Це означає, що персональну інформацію, яку можна визначити з відеозаписів, приховують або замінюють на іншу, що не дає можливості ідентифікувати осіб на відео. Одним з методів анонімізації є заміна обличчя на відео на шаблонні зображення, які не дозволяють ідентифікувати особу. Також можна застосовувати метод затемнення області обличчя на відео, що дозволяє зберегти інформацію про рухи і дії осіб, але не дозволяє ідентифікувати їх. Недоліком застосування методів анонімізації може бути складність знаходження та розпізнавання підозрілих осіб на відео, що може ускладнити проведення розслідування у випадку правопорушень. Для забезпечення конфіденційності в системах відеоспостереження також можна застосовувати методи шифрування. Шифрування дозволяє захистити відеодані від несанкціонованого доступу та перехоплення, забезпечуючи їх конфіденційність.

Існують різні методи шифрування, такі як симетричне та асиметричне шифрування. Симетричне шифрування полягає у використанні одного ключа для шифрування та дешифрування даних. Асиметричне шифрування використовує два ключі: публічний та приватний. Публічний ключ використовується для шифрування даних, а приватний - для їх розшифрування. Перевагою використання методів шифрування є висока стійкість до несанкціонованого доступу до відеоданих. Шифрування забезпечує їх захист та дозволяє зберігати конфіденційні дані в безпеці. Недоліком використання методів шифрування може бути складність в налаштуванні та обслуговуванні

системи шифрування, а також можливість затримок у роботі системи з великою кількістю даних. У кінцевому результаті, вибір методів забезпечення конфіденційності в системах відеоспостереження повинен базуватися на рівні ризику та вимогах щодо захисту персональних даних, а також можливостях та ресурсах системи.

2.3 Аналіз сучасних технологій захисту конфіденційності інформації в системах відеоспостереження

Сучасні технології захисту конфіденційності інформації в системах відеоспостереження постійно розвиваються та вдосконалюються. Деякі з найбільш ефективних методів захисту включають наступне:

1) Шифрування даних: Цей метод полягає в тому, що дані, які передаються через мережу відеоспостереження, шифруються за допомогою алгоритмів шифрування. Це дозволяє забезпечити конфіденційність передаваних даних та запобігти несанкціонованому доступу до них.
2) Анонімізація даних: Цей метод забезпечує захист конфіденційної інформації, шляхом заміни особисто ідентифікованої інформації (наприклад, обличчя людини) на псевдоніми або інші дані, які не можуть бути використані для ідентифікації особи.
3) Політики доступу: Цей метод полягає в тому, щоб встановити різні рівні доступу для користувачів системи відеоспостереження. Наприклад, забезпечення доступу до конфіденційної інформації тільки тим користувачам, які мають необхідні повноваження.
4) Фільтрація даних: Цей метод дозволяє відфільтрувати конфіденційну інформацію, що передається через мережу відеоспостереження. Наприклад, забезпечення того, щоб конфіденційна інформація (така як номери карток) не передавалася через мережу.

5) Використання мережевих протоколів забезпечення: Цей метод використовується для захисту мережі відеоспостереження від несанкціонованого доступу та атак з мережі Інтернет.

Окремі розробники також використовують технології шифрування на рівні обладнання, щоб забезпечити захист від проміжних атак на транспортний рівень мережі. Такі технології можуть включати захист від проміжних атак з використанням SSL/TLS тунелювання, апаратне шифрування даних та захист від перехоплення пакетів. Однак, такі методи не завжди підтримуються всіма виробниками обладнання, тому можуть бути несумісними з деякими системами відеоспостереження. Крім того, деякі розробники використовують машинне навчання та штучний інтелект для розпізнавання об'єктів на відео та аналізу змін в середовищі. Це може допомогти виявити потенційно небезпечні ситуації, такі як пожежі, аварії та несанкціонований доступ, та сповістити відповідні служби про них. Однак, такі методи потребують значного обчислювального потужності та можуть вимагати багато часу на налагодження та калібрування. Крім того, з'являються нові технології, спрямовані на покращення захисту конфіденційності відеоданих. Наприклад, технології шифрування та анонімізації дозволяють зберігати та передавати дані без злочинного втручання. Використання інтелектуальних систем аналізу відео дозволяє виявляти несанкціонований доступ до камер, зменшуючи ризик витоку конфіденційної інформації. Також, дедалі більшою популярністю користується концепція «Privacy by Design», що передбачає врахування аспектів конфіденційності та безпеки на ранніх етапах проектування систем відеоспостереження. Це дозволяє уникнути подальших проблем та негативних наслідків, що пов'язані з недостатнім захистом конфіденційної інформації. Однак, не зважаючи на те, що на сьогодні існує чимало різних технологій захисту конфіденційності в системах відеоспостереження, важливо пам'ятати, що жодна з них не є повністю ідеальною і не може забезпечити 100% захист від недобросовісних дій. Тому важливо постійно вдосконалювати технології захисту та враховувати

нові загрози. Одним з сучасних підходів до захисту конфіденційності в системах відеоспостереження є використання технологій машинного навчання. Зокрема, такі технології можуть бути застосовані для розпізнавання обличчя людини, аналізу поведінки та виявлення підозрілих дій.

Одним з інноваційних підходів є використання технології глибокого навчання для розпізнавання обличчя. Вона дозволяє точно визначити особу на відео та відфільтрувати непотрібні дані, збільшуючи тим самим ефективність системи відеоспостереження. Однак, цей метод має свої недоліки, такі як можливість помилкової ідентифікації та недостатню точність при розпізнаванні в обмежених умовах освітлення. Також, для забезпечення конфіденційності можуть використовуватись технології шифрування та децентралізованого збереження даних, що дозволяє зменшити ризики витоку чутливої інформації. Деякі виробники систем відеоспостереження також пропонують використання технологій анонімізації та псевдоанонімізації даних, що дозволяє зберегти конфіденційність даних під час їх обробки. Однак, ці методи також мають свої обмеження, зокрема, недостатню ефективність в ситуаціях, коли необхідно точно визначити особу на відео. Окремо можна відзначити такі напрями розвитку технологій захисту конфіденційності інформації в системах відеоспостереження:

1) Використання штучного інтелекту та машинного навчання для аналізу зображень та виявлення порушень безпеки. Такі системи здатні автоматично розпізнавати об'єкти на зображеннях та визначати, що є незвичним. Наприклад, системи можуть виявляти підозрілу активність в зоні відеоспостереження та повідомляти відповідні служби безпеки.
2) Використання шифрування для захисту передачі та зберігання відеоінформації. Технології шифрування можуть забезпечити безпеку даних шляхом захисту їх від несанкціонованого доступу. За допомогою

шифрування можна забезпечити конфіденційність інформації, що передається по мережі, та захистити її від підслуховування.

3) Використання анонімізації для збереження конфіденційності інформації. Анонімізація дозволяє приховати особисту інформацію, що міститься у відеозаписах, зберігаючи при цьому корисну інформацію для вирішення завдань відеоспостереження. Наприклад, системи можуть замаскувати обличчя людей на відеозаписах, щоб запобігти їх ідентифікації.

4) Розвиток систем, що використовують блокчейн для забезпечення безпеки даних. Такі системи можуть забезпечити безпеку даних шляхом їх розподілу між багатьма вузлами мережі, що забезпечує їх надійність та стійкість до атак.

Системи, які використовують блокчейн для забезпечення безпеки даних, зазвичай засновані на технології розподіленої бази даних. Вони забезпечують цілісність та достовірність даних, що зберігаються, через використання криптографічних методів. Блокчейн дає можливість створювати децентралізовані системи, в яких дані зберігаються на кількох вузлах мережі, що знижує ризик їх втрати чи підробки.

Використання блокчейн для забезпечення безпеки даних має такі переваги:

1) Децентралізація: дані зберігаються на кількох вузлах мережі, що забезпечує безпеку даних та зменшує ризик їх втрати чи підробки.

2) Надійність: система блокчейн забезпечує надійність даних, оскільки кожен блок в мережі містить у собі унікальний хеш-код, який посилається на попередні блоки. Таким чином, зміна будь-якого блоку після створення вимагає зміни всіх наступних блоків, що забезпечує неможливість підробки даних.

3) Конфіденційність: блокчейн забезпечує конфіденційність даних, оскільки кожен користувач може мати доступ лише до тих даних, які йому дозволено переглядати.

Однак, існують деякі недоліки використання блокчейн для забезпечення безпеки даних, такі як:

1) Складність розробки та впровадження: розробка системи на блокчейн може бути складною та вимагати великих витрат.
2) Швидкість транзакцій

Однак, використання блокчейн також має свої недоліки, зокрема повільну швидкість транзакцій та високі витрати на обробку даних. Крім того, розширення можливостей блокчейн-систем щодо забезпечення конфіденційності може призвести до того, що з'являться нові види кібератак, спрямовані на порушення конфіденційності даних в блокчейн-мережах. У підсумку, застосування блокчейн-технологій для забезпечення конфіденційності даних в системах відеоспостереження є перспективним рішенням, але потребує додаткового дослідження та розробки відповідних технологій. Також важливо враховувати технічні та економічні обмеження, пов'язані з застосуванням блокчейн, та бути готовими до використання інших методів захисту конфіденційності в разі необхідності. Для розвитку систем, що використовують блокчейн для забезпечення безпеки даних в системах відеоспостереження, працює багато компаній та стартапів. Вони пропонують різні рішення для забезпечення конфіденційності даних, але всі вони мають спільний принцип роботи - збереження даних у розподіленій мережі вузлів. Одним з прикладів таких систем є проект Ocean Protocol, який використовує блокчейн для зберігання та передачі даних з систем відеоспостереження. Вони пропонують рішення для зберігання відео та метаданих в розподіленій мережі, що забезпечує їх надійність та стійкість до атак. Ще одним прикладом є проект DAVINCI, який пропонує систему для забезпечення конфіденційності даних в

системах відеоспостереження. Вони використовують технологію блокчейн для зберігання даних про доступ до відеокамер та обробку відеоданих на різних рівнях захисту. Однак, системи на базі блокчейн також мають свої недоліки, серед яких великі витрати на обробку даних, низька швидкість обробки даних та обмежені можливості масштабування. Також важливо враховувати витрати на енергію, необхідні для забезпечення роботи мережі, які можуть бути досить значними. Узагальнюючи, аналіз сучасних технологій захисту конфіденційності інформації в системах відеоспостереження показує, що є багато методів, які можуть забезпечити ефективний захист від несанкціонованого доступу та збереження конфіденційності даних. Кожен з них має свої переваги та недоліки, тому необхідно ретельно вивчити особливості кожного методу та враховувати вимоги конкретної системи відеоспостереження.

Висновки до другого розділу

У розділі 2 було розглянуто методи забезпечення конфіденційності інформації в системах відеоспостереження. Для цього було проведено аналіз переваг та недоліків кожного з методів, визначено найбільш ефективний метод забезпечення конфіденційності в системах відеоспостереження та проаналізовано сучасні технології захисту конфіденційності інформації в системах відеоспостереження. За результатами дослідження було встановлено, що найбільш ефективним методом забезпечення конфіденційності в системах відеоспостереження є метод шифрування. Він дозволяє захистити дані від несанкціонованого доступу та забезпечити їх конфіденційність. Проте, при застосуванні методу шифрування є деякі недоліки, такі як складність використання та висока вартість обладнання. Тому, в залежності від конкретних вимог та обставин, можуть бути застосовані інші методи забезпечення конфіденційності, такі як маскування, використання сигналів з шумом та розподілом зображення. Зараз на ринку існують різноманітні сучасні технології захисту конфіденційності інформації в системах відеоспостереження, такі як захист від зламів та відновлення відображення,

відеоанонізація, аналіз руху та використання мережевих протоколів з шифруванням. Кожна з цих технологій має свої переваги та недоліки, тому вибір конкретної технології залежить від вимог користувача та конкретної ситуації.

3 ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ В СИСТЕМАХ ВІДЕОСПОСТЕРЕЖЕННЯ

3.1 Визначення загроз та ризиків в системах відеоспостереження

Системи відеоспостереження можуть бути піддані різним загрозам та ризикам. Ось декілька можливих загроз та ризиків, які можуть виникнути в системах відеоспостереження:

1) Злам системи: Зламник може зламати систему відеоспостереження, щоб отримати доступ до відеоматеріалів або навіть контролювати систему.
2) Віруси та шкідливі програми: Віруси та інші шкідливі програми можуть використовувати систему відеоспостереження як засіб для поширення атак на інші системи.
3) Несанкціонований доступ: Несанкціонований доступ до системи відеоспостереження може стати причиною витоку конфіденційної інформації або порушення приватності осіб, які перебувають під наглядом.
4) Низька якість відеозапису: Недостатня якість відеозапису може стати перешкодою для ідентифікації осіб, які знаходяться на відео.
5) Відсутність оновлень та патчів: Відсутність оновлень та патчів для системи відеоспостереження може зробити її вразливою до нових загроз.
6) Збір та збереження особистих даних: Збір та збереження особистих даних може порушити приватність людей, які перебувають під наглядом.
7) Технічні проблеми: Технічні проблеми з обладнанням або програмним забезпеченням можуть призвести до зупинки системи відеоспостереження або втрати відеоматеріалів.

8) Порушення законодавства: Використання системи відеоспостереження може порушувати законодавство щодо приватності та зберігання даних.

Для запобігання цим загрозам та ризикам в системах відеоспостереження є кілька кроків, які можна вжити:

1) Забезпечення безпеки системи: Для запобігання злому системи, необхідно встановлювати сильні паролі, використовувати двофакторну аутентифікацію та шифрування даних. Також важливо регулярно оновлювати програмне забезпечення та патчі.
2) Використання антивірусного програмного забезпечення: Антивірусне програмне забезпечення допоможе запобігти входженню шкідливих програм до системи відеоспостереження.
3) Обмеження доступу: Налаштування прав доступу до системи відеоспостереження може допомогти запобігти несанкціонованому доступу.
4) Використання високоякісного обладнання: Використання високоякісного обладнання допоможе запобігти проблемам з якістю відеозапису та технічними проблемами.
5) Дотримання законодавства: Важливо дотримуватись законодавства щодо приватності та зберігання даних, щоб запобігти порушенням закону.
6) Забезпечення безпеки системи: Для запобігання злому системи, необхідно встановлювати сильні паролі, використовувати двофакторну аутентифікацію та шифрування даних. Також важливо регулярно оновлювати програмне забезпечення та патчі.
7) Використання антивірусного програмного забезпечення: Антивірусне програмне забезпечення допоможе запобігти входженню шкідливих програм до системи відеоспостереження.
8) Обмеження доступу: Налаштування прав доступу до системи відеоспостереження може допомогти запобігти несанкціонованому доступу.

9) Використання високоякісного обладнання: Використання високоякісного обладнання допоможе запобігти проблемам з якістю відеозапису та технічними проблемами.
10) Дотримання законодавства: Важливо дотримуватись законодавства щодо приватності та зберігання даних, щоб запобігти порушенням закону.

Крім того, можна вжити наступні заходи для зменшення загроз та ризиків в системах відеоспостереження:

1) Захист мережі: Необхідно захистити мережу від несанкціонованого доступу шляхом встановлення фаєрволу та використання VPN-з'єднань для дистанційного доступу.
2) Моніторинг доступу: Слід встановити механізми моніторингу доступу до системи відеоспостереження для виявлення несанкціонованого доступу та атак.
3) Захист від злому: Необхідно встановити механізми захисту від злому, такі як системи виявлення вторгнень (IDS) та виявлення злому (IPS).
4) Використання технологій штучного інтелекту: Використання технологій штучного інтелекту, таких як аналіз поведінки, може допомогти виявляти незвичайну поведінку та потенційні загрози.
5) Планування випадків аварій: Важливо мати плани дій в разі аварії, таких як крадіжки або виходу з ладу обладнання, щоб забезпечити швидку реакцію та запобігти негативним наслідкам.

Також важливо відмітити, що системи відеоспостереження можуть стати об'єктом злочинних дій не лише зовнішніх загроз, але й внутрішнього зловживання. Наприклад, працівники, які відповідають за систему відеоспостереження, можуть незаконно використовувати її для своїх особистих цілей, втручатися у приватне життя інших осіб або навіть продавати конфіденційну інформацію. Тому необхідно ретельно відбирати персонал, який

буде відповідати за систему відеоспостереження, і проводити регулярні перевірки їх діяльності. Також можна використовувати технології контролю доступу та обліку дій персоналу для забезпечення безпеки та запобігання можливим зловживанням. Крім того, необхідно враховувати права та свободи громадян, зокрема щодо приватності, під час використання систем відеоспостереження. Необхідно дотримуватися законодавства та стандартів, які регулюють використання таких систем, та забезпечити прозорість щодо їх використання. Також важливо враховувати етичні аспекти використання систем відеоспостереження, зокрема щодо обмеження використання таких систем для стеження за конкретними особами без достатньої підстави. Нарешті, слід відзначити, що зростаюча популярність систем відеоспостереження вимагає забезпечення їх сумісності з іншими системами безпеки та інфраструктурою міста. Наприклад, можливість інтеграції з системами автоматичної пожежної сигналізації, системами контролю доступу та іншими допомагає покращити рівень безпеки та ефективності використання систем відеоспостереження. Отже, для забезпечення ефективності та безпеки використання систем відеоспостереження необхідно проводити комплексний підхід до їх захисту, зокрема шляхом використання технологій захисту, відбору та контролю персоналу, дотримання законодавства та етичних аспектів використання систем відеоспостереження, проведення моніторингу та оцінки їх безпеки, підтримки високого рівня свідомості персоналу та громадськості щодо можливих загроз та ризиків використання систем відеоспостереження, а також забезпечення їх сумісності з іншими системами безпеки та інфраструктурою міста. Також, важливо враховувати аспекти приватності та захисту персональних даних при використанні систем відеоспостереження. Законодавство багатьох країн визначає правила збору, зберігання та обробки персональних даних, а також вимагає дотримання певних правил щодо захисту приватності осіб, які можуть знаходитися під спостереженням. У зв'язку з цим, використання систем відеоспостереження повинно відбуватися з дотриманням вимог законодавства

та етичних норм. Крім того, системи відеоспостереження можуть стати об'єктом кібератак та злому, якщо не забезпечити їх достатньої захищеності. Зловмисники можуть отримати доступ до відеозаписів, що може призвести до різних наслідків, включаючи розкриття конфіденційної інформації або використання відеозаписів в злочинних цілях. Тому, для забезпечення захисту систем відеоспостереження важливо використовувати надійне програмне забезпечення та обладнання, застосовувати шифрування даних, встановлювати паролі та обмежувати доступ до систем. Додатково до вищезгаданого, важливим аспектом при використанні систем відеоспостереження є ефективність їх роботи. Недооцінення необхідної кількості камер або недостатня роздільна здатність можуть призвести до втрати важливої інформації. Для досягнення максимальної ефективності відеоспостереження, необхідно провести аналіз потреби у відеоспостереженні та правильно розмістити камери, забезпечити достатню роздільну здатність та максимальну покриття зони спостереження. Крім того, важливо забезпечити ефективну обробку отриманої інформації з камер відеоспостереження. Для цього можна використовувати спеціалізоване програмне забезпечення для аналізу відео, що дозволяє автоматично виявляти певні події та поведінку людей на відео. Наприклад, системи відеоаналітики можуть розпізнавати обличчя людей, визначати їх рух, зареєстровувати реєстраційні номери автомобілів тощо. Нарешті, важливо мати належний контроль над системою відеоспостереження. Адміністратори повинні регулярно перевіряти стан системи, включаючи перевірку наявності вірусів та оновлення програмного забезпечення. Також, важливо мати чітко визначені процедури дій у випадку виявлення проблем з системою відеоспостереження або випадків порушення безпеки даних. Узагалі, використання систем відеоспостереження має свої переваги та ризики, тому необхідно ретельно аналізувати потреби та можливості при їх впровадженні. На цьому етапі важливо звернути увагу на всі вищезгадані аспекти, щоб забезпечити ефективну та безпечну роботу систем відеоспостереження.

Загалом, використання систем відеоспостереження має свої переваги та ризики. Для забезпечення безпеки та ефективності системи необхідно дотримуватися всіх правил та законодавства, враховувати конфіденційність інформації та етичні аспекти, а також забезпечувати захист від несанкціонованого доступу та фізичного пошкодження.

3.2 Аналіз потенційних проблем забезпечення конфіденційності інформації

Забезпечення конфіденційності інформації є одним з найважливіших завдань будь-якої організації, оскільки порушення конфіденційності може призвести до серйозних наслідків, включаючи витрати на відшкодування збитків та втрату довіри клієнтів і партнерів. Ось деякі потенційні проблеми, які можуть виникнути при забезпеченні конфіденційності інформації:

1) Несанкціонований доступ: Найбільш очевидна проблема полягає у тому, що хакери або інші несанкціоновані особи можуть намагатися зламати систему безпеки для отримання доступу до конфіденційної інформації.
2) Людський фактор: Іноді проблеми з конфіденційністю можуть виникати через недбалість або помилки співробітників, які можуть випадково надати доступ до конфіденційної інформації або неправильно використовувати її.
3) Недостатня захист від внутрішніх загроз: У деяких випадках загроза може виникати зсередини самої організації, коли співробітник зловживає довірою або надмірною діловою владою.
4) Нестача захисту даних на рівні зберігання: Важлива інформація може бути зберігатися на ненадійних серверах, які можуть бути піддаються хакерським атакам або відмові.
5) Соціальний інжиніринг: Зловмисники можуть використовувати соціальний інжиніринг для отримання доступу до конфіденційної

інформації, шляхом використання хитромудрих методів впливу на людей, що можуть бути вразливі до підкупу, підступу чи маніпуляцій.

6) Недостатній захист мережі: Недостатній захист мережі може призвести до того, що хакери зможуть здійснювати атаки з використанням вразливостей в програмному забезпеченні та обладнанні компанії, що дозволяє їм отримати доступ до конфіденційної інформації.
7) Виток даних: Витік даних може статися через помилки в системі збереження даних, недостатньої захищеності транспортування інформації, зламу або соціального інжинірингу.
8) Викрадення мобільних пристроїв: Інформація може бути викрадена з мобільних пристроїв, таких як смартфони та планшети, які містять конфіденційну інформацію про компанію.
9) Недостатня кваліфікація персоналу: Іноді в організації можуть бути недостатньо кваліфіковані співробітники, що не можуть добре розуміти методи інформаційної безпеки, що може призвести до порушення конфіденційності.

Серед можливих заходів забезпечення конфіденційності інформації можна виділити:

1) Встановлення політики інформаційної безпеки: Визначення правил інформаційної безпеки, які повинні бути дотримані всіма співробітниками організації.
2) Класифікація даних: Встановлення рівнів конфіденційності для різних категорій даних та розробка відповідної системи захисту.
3) Шифрування даних: Використання шифрування для захисту конфіденційної інформації під час її транспортування та зберігання.

4) Встановлення політики паролів: Розробка правил використання паролів, що забезпечують захист від несанкціонованого доступу до конфіденційної інформації.
5) Аудит безпеки: Проведення регулярного аудиту безпеки для виявлення можливих вразливостей та ризиків, що становлять загрозу конфіденційності інформації.
6) Технічні заходи захисту: Використання захисту від вірусів та інших загроз, що можуть вплинути на конфіденційну інформацію.

Однак, незважаючи на наявність можливостей забезпечення конфіденційності інформації, все ж можуть виникати проблеми, які потребують додаткових заходів захисту. До можливих проблем можна віднести:

1) Внутрішні загрози: Співробітники організації можуть бути джерелом загрози конфіденційності інформації, якщо вони несвідомо або навмисно порушують політику інформаційної безпеки.
2) Зовнішні загрози: Конфіденційну інформацію можуть бути викрадена з зовнішнього джерела, наприклад, через хакерські атаки, віруси або через соціальну інженерію.
3) Нестача ресурсів: Відсутність достатніх фінансових ресурсів, кадрових ресурсів або технічних ресурсів може стати перешкодою в реалізації ефективної політики конфіденційності інформації.
4) Законодавчі обмеження: Наявність законодавчих обмежень може знизити рівень конфіденційності інформації, наприклад, якщо законодавство вимагає розголошення певних даних.

Отже, для успішного забезпечення конфіденційності інформації потрібно вжити комплексу заходів, які враховуватимуть всі можливі загрози. Для цього можна використовувати наступні рекомендації:

1) Розробити політику інформаційної безпеки: Необхідно створити документ, який буде визначати політику інформаційної безпеки в

організації. Він повинен містити вимоги до обробки конфіденційної інформації, правила доступу до неї, а також заходи, що вживаються в разі порушення політики.

2) Надавати доступ лише необхідним співробітникам: Важливо обмежувати доступ до конфіденційної інформації лише тим співробітникам, які мають до неї реальну необхідність. Для цього можна використовувати систему рівнів доступу до інформації.
3) Навчання персоналу: Всі співробітники повинні бути проінформовані про політику інформаційної безпеки та вміти працювати з конфіденційною інформацією.
4) Використання шифрування: Шифрування допоможе захистити конфіденційну інформацію від несанкціонованого доступу та зберегти її цілісність.
5) Забезпечення захисту проти зовнішніх загроз: Для цього можна використовувати антивірусні програми, брандмауери та інші інструменти, які захищають від хакерських атак та вірусів.
6) Проведення аудиту інформаційної безпеки: Регулярний аудит допоможе виявити можливі проблеми з інформаційною безпекою та вчасно прийняти заходи щодо їх вирішення.
7) Захист інформації від внутрішніх загроз: Окрім захисту від зовнішніх загроз, важливо також забезпечити захист від внутрішніх загроз, тобто зловживання співробітниками своїми повноваженнями. Для цього можна використовувати систему контролю дій співробітників з конфіденційною інформацією.
8) Забезпечення безпеки при зберіганні та використанні інформації: Конфіденційна інформація повинна зберігатися та оброблятися в безпечному середовищі, де немає ризику її втрати або пошкодження. Також необхідно використовувати безпечні методи використання інформації, наприклад, передача її зашифрованим електронним шляхом.

9) Поліпшення системи резервного копіювання: Важливо мати систему резервного копіювання, що допоможе відновити інформацію у разі її втрати. При цьому, такі копії повинні зберігатися в безпечних місцях і мати обмежений доступ.
10) Регулярне оновлення програмного забезпечення: Правильно налаштована та оновлена програмна частина допоможе зменшити ризик вразливості системи, що зменшить можливість несанкціонованого доступу до інформації.
11) Навчання співробітників: Для забезпечення конфіденційності інформації необхідно навчати співробітників правильному обходу з конфіденційною інформацією та застосуванню заходів безпеки. Важливо проводити регулярні тренінги та організовувати внутрішню інформаційну кампанію з питань інформаційної безпеки.
12) Аудит та перевірка системи захисту інформації: Регулярний аудит системи захисту інформації допоможе виявити можливі проблеми та вразливості в системі, що дозволить учасникам процесу вчасно прийняти відповідні заходи для забезпечення конфіденційності інформації.
13) Розробка політики безпеки інформації: Розробка і впровадження політики безпеки інформації допоможе забезпечити взаємне розуміння та відповідальність учасників процесу з питань захисту конфіденційної інформації. Політика повинна містити рекомендації щодо застосування заходів безпеки, процедур захисту інформації та механізмів контролю виконання цих процедур.

Також важливо навчити співробітників правильно користуватись інформаційними технологіями та забезпечити їхню свідомість про проблеми безпеки. Наприклад, організації можуть проводити навчальні курси з безпеки та інформаційної грамотності для своїх співробітників, а також вимагати від них дотримуватись певних правил користування електронними засобами забезпечення безпеки. Крім того, важливо регулярно проводити аудит безпеки,

щоб виявляти можливі слабкі місця в системі захисту конфіденційної інформації та вживати необхідних заходів для їх усунення. Аудит може включати перевірку заходів забезпечення безпеки, оцінку ризиків порушення безпеки, тестування захисту на проникнення та інші процедури. Усі ці заходи можуть допомогти зменшити ризик втрати конфіденційної інформації та зберегти її в цілості та безпеці. Важливо пам'ятати, що захист конфіденційної інформації є постійним процесом та вимагає постійної уваги та оновлення. В цілому, забезпечення конфіденційності інформації - це надзвичайно важлива задача для будь-якої організації, оскільки порушення конфіденційності може призвести до негативних наслідків, таких як виток важливих даних, втрата довіри клієнтів та інших стейкхолдерів, а також порушення законодавства. Тому необхідно приділяти достатню увагу забезпеченню безпеки та контролю доступу до інформації в організації.

3.3 Перелік чинників, які можуть підвищити рівень загроз та ризиків

Існує безліч чинників, які можуть підвищити рівень загроз та ризиків, залежно від контексту і обставин. Ось декілька загальних чинників, які можуть підвищити ризики:

a) Недостатня підготовка або незнання процедур безпеки та безпечної поведінки.
b) Недостатній контроль або недостатня супроводження під час виконання небезпечної діяльності.
c) Неправильна організація та управління діяльністю, включаючи планування, розподіл завдань та координацію.
d) Технічні проблеми, включаючи несправність обладнання або програмного забезпечення.
e) Небезпечні або непередбачувані умови навколишнього середовища, такі як небезпечні робочі умови або природні катастрофи.
f) Несанкціонований доступ до конфіденційної інформації або витік даних.

g) Надмірне використання або зловживання владою, включаючи корупцію або неправомірне втручання в особисті свободи і права.
h) Злочинна діяльність або терористичні акти.
i) Недостатня або неефективна система захисту від кібератак або хакерських атак.
j) Недостатня або неправильна оцінка ризиків та відсутність планування та заходів у разі виникнення небезпеки.

Рівень загроз та ризиків може варіюватись в залежності від сфери діяльності та конкретної ситуації. Наприклад, у галузі медицини, загрози можуть включати небезпеку інфекційних захворювань, помилки в діагностиці або лікуванні, а також можливість виникнення побічних ефектів при прийомі лікарських засобів.

У галузі інформаційної безпеки, загрози можуть включати кібератаки, шахрайство з використанням електронної пошти або соціальних мереж, крадіжку конфіденційної інформації та витік даних. Крім того, загрози можуть залежати від місця знаходження та рівня науково-технічного розвитку, тому що в деяких країнах можуть бути менш ефективні системи захисту від кібератак або низький рівень культури безпеки в цілому. Важливо розуміти, що загрози та ризики можуть змінюватись з часом, тому важливо постійно оцінювати ситуацію та здійснювати необхідні заходи з мінімізації ризиків. Для цього можна використовувати різноманітні методики та інструменти, такі як аналіз ризиків, планування кризового управління, внутрішні аудити та інші. Зміни в кліматичних умовах та природні катаклізми, такі як повені, землетруси та урагани, можуть також призвести до збільшення ризиків для життя та здоров'я людей, а також для різних видів інфраструктури та майна. Тому важливо забезпечити належні заходи попередження та захисту, такі як правильне проектування будівель та інженерних систем, системи відслідковування та

надання рятувальних послуг в разі надзвичайних ситуацій. Загрози терористичних актів та злочинності також можуть підвищити ризики для людей та майна, тому важливо забезпечити належний захист та безпеку на робочому місці, а також вживати необхідних заходів для забезпечення безпеки громадян в місцях масового скупчення. Наслідки екологічних катастроф та забруднення довкілля також можуть призвести до збільшення ризику для здоров'я та безпеки людей. Наприклад, забруднення повітря може призвести до захворювань дихальних шляхів та серцево-судинної системи, а забруднення води може викликати захворювання шлунково-кишкового тракту та інших систем органів. Технологічні зміни та інновації можуть також призвести до збільшення ризику для безпеки та здоров'я людей. Наприклад, розробка нових матеріалів та речовин може викликати небезпеку для здоров'я людей у разі неправильного використання або недостатньої інформації про їх властивості. Крім того, збільшення використання роботів та інших автоматизованих систем може призвести до зменшення кількості робочих місць, а також до збільшення небезпеки для безпеки працівників у разі неправильного використання або недостатньої підготовки. Наростаюча кількість кіберзагроз та кібератак можуть також призвести до збільшення ризику для безпеки та здоров'я людей. Це може включати кіберзлочинність, яка може призвести до витоку конфіденційної інформації, втрати фінансових коштів або порушення роботи критично важливих систем, таких як медичне обладнання або електронні системи управління транспортом. Крім того, політичні та соціальні конфлікти можуть призвести до збільшення загроз та ризиків. Наприклад, воєнні конфлікти можуть викликати руйнування міст та інфраструктури, що призводить до нестабільності та загрози безпеки для місцевого населення. Також соціальні конфлікти можуть призвести до зростання насильства та кримінальної активності, що може негативно вплинути на безпеку громадян. Наростаюча залежність від технологій та інформаційних систем також може збільшувати ризик для безпеки та здоров'я людей. Наприклад, збільшення кількості

електронних платежів може призвести до збільшення кіберзагроз та зловживань, таких як крадіжка особистої інформації або викрадення грошових коштів. Крім того, збільшення використання розумних пристроїв та інтернету речей може призвести до збільшення небезпеки для приватності та безпеки даних. Додатковим фактором, що може призвести до підвищення загроз та ризиків, є недостатня увага до проблем з охороною навколишнього середовища та здоров'я людей. Наприклад, забруднення повітря, води та грунту може мати шкідливий вплив на здоров'я людей та навколишнє середовище. Також зміна клімату може призвести до збільшення кількості стихійних лих та екологічних катастроф, що може стати причиною збільшення загроз та ризиків для населення. Погіршення демографічних показників також може призвести до збільшення загроз та ризиків. Наприклад, збільшення кількості старших людей може призвести до збільшення витрат на охорону здоров'я та соціальні програми. Крім того, зменшення кількості дітей та молоді може призвести до зменшення економічного зростання та інновацій. Наростаюча глобалізація та інтеграція світових економік також можуть призвести до збільшення загроз та ризиків. Наприклад, пандемія COVID-19 стала прикладом того, як глобальні виклики можуть мати великий вплив на світову економіку та здоров'я людей. Крім того, глобальні конфлікти та напруження між державами можуть призвести до загострення політичної ситуації та збільшення ризику війни. Для зменшення ризику екологічних катастроф та забруднення довкілля необхідно проводити дієву політику щодо охорони навколишнього середовища та економічних механізмів, що сприяють зменшенню шкідливого впливу на нього. Наприклад, розвиток відновлюваної енергетики та зменшення викидів парникових газів, використання екологічно чистих технологій виробництва та відновлення природних ресурсів. Забезпечення громадської безпеки та здоров'я також є важливим напрямком роботи. Наприклад, укріплення здоров'я нації, забезпечення високоякісної медичної допомоги та профілактичних заходів, удосконалення системи громадської безпеки та захисту прав громадян.

Залучення громадськості до діалогу та співпраці також може допомогти в зменшенні ризику та підвищенні ефективності дієвих стратегій. Діалог між владою та громадськістю, включення громадян у процеси прийняття рішень та реалізацію програм зменшення ризику можуть сприяти формуванню об'єднаних зусиль для досягнення спільних цілей. Крім того, важливо вести науково-дослідну роботу в галузі зменшення ризиків та попередження катастроф. Розробка нових технологій та матеріалів, дослідження динаміки процесів у природному середовищі, аналіз інформації про стихійні лиха та надзвичайні ситуації можуть допомогти в розробці більш ефективних стратегій та заходів зменшення ризиків. Для забезпечення зменшення загроз та ризиків, необхідно також проводити систематичний моніторинг та оцінку потенційних загроз, які можуть виникнути в майбутньому. Це може включати в себе аналіз зміни клімату, розвиток нових хвороб, ризики техногенних катастроф, соціально-політичні конфлікти та інші фактори. Також необхідно створювати інформаційні системи та бази даних, які дозволять оперативно отримувати інформацію про потенційні загрози та ризики, та аналізувати їх для прийняття ефективних рішень. Окрім того, важливо розвивати систему попередження та реагування на надзвичайні ситуації. Це може включати в себе розробку систем аварійного оповіщення та евакуації населення, резервних планів енергопостачання, водопостачання та інших життєво важливих систем. Окрім того, важливо забезпечити підвищення рівня свідомості населення про потенційні загрози та ризики, які можуть виникнути. Це може включати в себе проведення різноманітних кампаній з освіти населення, розробку матеріалів та інформаційних ресурсів, які нададуть людям інформацію та інструменти для дій у випадку надзвичайних ситуацій. Забезпечення безпеки та мінімізація ризиків потребують координації зусиль між різними відомствами та організаціями, а також партнерство між державою, громадськістю та приватним сектором. Суспільство повинно працювати разом, щоб зменшити ризики та забезпечити безпеку своїх громадян. Навчальні програми та курси повинні

включати в себе навички, які допоможуть громадянам діяти в екстремальних ситуаціях. Також важливо забезпечити доступність інформації про ризики та надзвичайні ситуації, зокрема, через Інтернет, телефонні лінії довіри та інші канали. Загалом, забезпечення безпеки та мінімізація ризиків є складним процесом, який вимагає багатогранного підходу та постійного вдосконалення. Проте, здійснення відповідних заходів може забезпечити стійкий розвиток суспільства та збереження життя та здоров'я людей в надзвичайних ситуаціях. Ще одним важливим аспектом забезпечення безпеки та мінімізації ризиків є розробка та впровадження стандартів та нормативних актів, які регулюють питання безпеки в різних сферах життєдіяльності. Наприклад, такі стандарти можуть стосуватися енергетики, транспорту, будівництва, харчової промисловості та інших галузей. Розробка та впровадження таких стандартів дозволяє забезпечити однаковий підхід до питань безпеки в різних сферах діяльності та зменшити ризики внаслідок несанкціонованих дій. Крім того, стандарти та нормативні акти можуть включати в себе вимоги щодо підготовки персоналу, регулярних перевірок та аудитів, а також механізмів контролю за дотриманням вимог безпеки. Однак важливо зазначити, що розробка та впровадження стандартів та нормативних актів не є самоціллю. Вони повинні бути розроблені з урахуванням специфіки кожної сфери та враховувати потенційні загрози та ризики, які можуть виникнути. Крім того, їх впровадження повинне супроводжуватись належною комунікацією та інформуванням громадськості про вимоги безпеки та їх значення. Отже, забезпечення безпеки та мінімізація ризиків є важливою складовою сталого розвитку суспільства.

Висновки до третього розділу

З розділу 3 можна зробити висновок, що системи відеоспостереження можуть стати джерелом потенційної загрози для конфіденційності інформації. Визначення загроз та ризиків в системах відеоспостереження, аналіз потенційних проблем забезпечення конфіденційності і перелік чинників, які

можуть підвищити рівень загроз та ризиків, свідчать про те, що для забезпечення конфіденційності інформації, яку збирають системи відеоспостереження, необхідні певні заходи та технології. Розуміння загроз та ризиків дозволяє визначити найбільш критичні проблеми та зосередити зусилля на їх вирішенні. Однак, необхідно пам'ятати, що конфіденційність не є єдиним критерієм оцінки ефективності систем відеоспостереження, і інші фактори такі як ефективність в розшуку злочинців та забезпечення безпеки загалом, також мають важливе значення.

4 РОЗРОБКА ТА РЕАЛІЗАЦІЯ МЕТОДУ ЗАБЕЗПЕЧЕННЯ КОНФІДЕНЦІЙНОСТІ ІНФОРМАЦІЇ В СИСТЕМІ ВІДЕОСПОСТЕРЕЖЕННЯ

4.1 Дослідження розробки методу забезпечення конфіденційності

Розробка методу забезпечення конфіденційності в системах відеоспостереження може включати наступні кроки:

1) Аналіз системи відеоспостереження. Для початку потрібно ретельно проаналізувати систему відеоспостереження, визначивши, які дані вона збирає, де зберігає їх і хто має до них доступ. Також важливо визначити, які конкретно дані є конфіденційними і потребують захисту.
2) Встановлення технічних засобів захисту. Після визначення конфіденційних даних і аналізу системи відеоспостереження необхідно встановити технічні засоби захисту, які допоможуть забезпечити конфіденційність даних. Це можуть бути різноманітні технічні заходи, такі як шифрування даних, захист від несанкціонованого доступу, обмеження прав доступу до даних, і т.д.
3) Встановлення процедур управління доступом. Окрім технічних засобів захисту, важливо встановити процедури управління доступом до конфіденційних даних. Це може включати в себе такі процедури, як ідентифікація користувачів, автентифікація, авторизація та аудит доступу до даних.
4) Навчання персоналу. Важливо навчити персонал системи відеоспостереження використовувати нові технічні засоби захисту та процедури управління доступом до конфіденційних даних. Це допоможе зменшити ризики несанкціонованого доступу до даних.
5) Проведення тестування та оцінка ефективності.

Розробка методу забезпечення конфіденційності в системах відеоспостереження може включати наступні етапи:

1) Аналіз ризиків та визначення конфіденційності даних. Для початку потрібно провести аналіз ризиків і визначити, які дані є конфіденційними та потребують захисту. Для цього можна скористатися методом Threat and Risk Assessment (TRA), що дозволить визначити потенційні загрози та ризики, що можуть виникнути в процесі відеоспостереження.
2) Встановлення захисту даних. На цьому етапі потрібно визначити заходи захисту, які будуть використовуватися для забезпечення конфіденційності даних. Це можуть бути такі заходи як шифрування даних, захист від несанкціонованого доступу, обмеження прав доступу до даних, а також встановлення технічних засобів, таких як система відеоспостереження з підтримкою шифрування.
3) Встановлення процедур управління доступом. Окрім технічних засобів захисту, важливо встановити процедури управління доступом до конфіденційних даних. Це може включати в себе такі процедури, як ідентифікація користувачів, автентифікація, авторизація та аудит доступу до даних.
4) Навчання персоналу. Важливо навчити персонал системи відеоспостереження використовувати нові технічні засоби захисту та процедури управління доступом до конфіденційних даних. Це допоможе зменшити ризики несанкціонованого доступу до даних.
5) Моніторинг та аналіз ефективності.
6) Оновлення заходів захисту. В процесі моніторингу та аналізу ефективності можуть виявлятися нові загрози та ризики, що потребують оновлення заходів захисту. Тому важливо вчасно оновлювати технічні засоби та процедури управління доступом до даних, щоб захист відповідав поточним вимогам та стандартам безпеки.

Також важливим етапом розробки методу забезпечення конфіденційності в системах відеоспостереження є підготовка персоналу, який буде працювати з даними. Персонал повинен бути ознайомлений з процедурами та правилами використання даних, а також мати достатні знання з технічних засобів захисту, щоб уникнути можливих помилок та проблем. Крім того, розробка методу забезпечення конфіденційності повинна відповідати вимогам та стандартам безпеки, таким як GDPR, HIPAA, ISO 27001 та інші. Ці стандарти визначають вимоги до захисту даних, процедури їх збереження та обробки, а також вимоги до технічних засобів захисту. Для забезпечення конфіденційності в системах відеоспостереження можуть використовуватися різні методи та технічні засоби захисту. Один з таких методів - шифрування даних. Шифрування дозволяє забезпечити безпеку даних, передаваних по мережі, та захистити їх від несанкціонованого доступу. Також для забезпечення конфіденційності можуть використовуватися різні технічні засоби, такі як використання паролів та системи автентифікації, контроль доступу до системи відеоспостереження, використання захищеного з'єднання для передачі даних тощо. Однак, на жаль, навіть застосування найкращих методів та технічних засобів захисту не гарантує повної конфіденційності даних в системах відеоспостереження. Для забезпечення максимальної безпеки необхідно також враховувати людський фактор та регулярно оновлювати заходи захисту. Крім того, важливо пам'ятати про етичні та правові аспекти використання систем відеоспостереження. Для захисту прав та свобод людей, що перебувають в зоні відеоспостереження, можуть бути запроваджені різні обмеження, такі як регулювання місць встановлення камер, встановлення заборон на встановлення камер в певних місцях, обмеження строку зберігання записів тощо. Для забезпечення конфіденційності в системах відеоспостереження можуть застосовуватися також різні методи анонімізації даних. Наприклад, можна застосовувати маскування обличчя, щоб забезпечити анонімність людей, що перебувають в зоні відеоспостереження. Цей метод можна застосовувати як у режимі

реального часу, так і для запису відео на диск. Іншим методом захисту конфіденційності може бути використання засобів маскування звуку. Наприклад, можна зменшити гучність аудіо запису з місця встановлення камери, щоб забезпечити анонімність голосу людей, які знаходяться в зоні відеоспостереження. Окрім того, для захисту конфіденційності можна використовувати алгоритми машинного навчання та штучного інтелекту. Наприклад, можна використовувати алгоритми для автоматичного виявлення та розпізнавання облич людей на відео, а також для визначення того, чи відбувається на відео порушення конфіденційності. Нарешті, важливо забезпечувати охорону даних в системі відеоспостереження. Для цього можуть використовуватися різні методи захисту, наприклад, шифрування даних, резервне копіювання, контроль доступу та інші. Додатково до розглянутих методів, для забезпечення конфіденційності в системах відеоспостереження можуть використовуватися такі технічні засоби, як спеціальні затемнювальні штори або плівки на вікнах. Ці засоби дозволяють знизити рівень електромагнітних випромінювань, що можуть використовуватися для нелегального віддаленого перегляду відео з відеокамер. Для забезпечення високого рівня захисту конфіденційності відео можуть також використовуватися різноманітні криптографічні методи. Наприклад, можуть застосовуватися методи шифрування відеоданих та каналів передачі даних, що забезпечують високий рівень безпеки. Також важливо звернути увагу на налаштування системи відеоспостереження, а саме на режим доступу до неї. Для того, щоб забезпечити високий рівень конфіденційності, необхідно встановити доступ до системи тільки за допомогою пароля або ідентифікаційного коду. Ідеальним варіантом є використання біометричних методів ідентифікації, таких як сканування відбитків пальців або розпізнавання облич. Важливо також забезпечувати належний рівень захисту даних, які збираються системою відеоспостереження. Для цього можна використовувати методи обмеження доступу до зберіганої інформації, копіювання та передачі

даних. Всі ці методи мають на меті забезпечення максимальної конфіденційності відео та інших даних, які збираються в системі відеоспостереження. додаток до технічних та криптографічних методів можна використовувати правові методи, такі як встановлення законодавчих норм та правил, що обмежують використання систем відеоспостереження та регулюють збір, зберігання та використання зібраних даних. Це може забезпечити додатковий рівень захисту конфіденційності, особливо коли мова йде про збір інформації в громадських місцях. Окрім того, важливо пам'ятати про прозорість використання систем відеоспостереження. Користувачі систем повинні мати інформацію про те, які дані збираються, як вони будуть використовуватися та кому можуть бути передані. Це може забезпечити додатковий рівень захисту приватності та конфіденційності. Ще одним важливим аспектом забезпечення конфіденційності в системах відеоспостереження є захист від вторгнень. Це може бути забезпечено за допомогою методів, таких як захист мережі та додатків, мережевий моніторинг та виявлення вторгнень, шифрування даних тощо. Крім того, важливо дотримуватися принципу необхідності та пропорційності при зборі та використанні відеоданих. Це означає, що збирання даних повинно бути обмеженим лише необхідним обсягом для досягнення певної мети, наприклад, забезпечення безпеки на території або в зоні підвищеного ризику. Крім того, збирання та використання відеоданих повинні бути пропорційними до мети, тобто не повинні перевищувати необхідний обсяг та не повинні використовуватися для інших цілей, крім визначених. Ще одним аспектом забезпечення конфіденційності в системах відеоспостереження є захист від зловживань та недбалого використання відеоданих. Це може бути забезпечено за допомогою встановлення політики використання відеоданих, зокрема, обмеження доступу до них тільки відповідним працівникам та захистом від недбалого використання або втрати даних. Також важливо враховувати вимоги законодавства та правил використання систем відеоспостереження, зокрема, необхідно забезпечити виконання правил збору

та зберігання відеоданих, правил доступу до них, а також правил повідомлення про використання відеоданих. Для забезпечення конфіденційності в системах відеоспостереження також можна використовувати методи анонімізації даних, що полягає в заміні ідентифікаторів людей на інші унікальні ідентифікатори, що не пов'язані з конкретними особами. Це може зменшити ризик розкриття конфіденційної інформації, що пов'язана з конкретними людьми. У загальному, забезпечення конфіденційності в системах відеоспостереження є важливою проблемою, яка вимагає комплексного підходу, включаючи технічні, криптографічні, організаційні та правові методи захисту. Крім того, важливо забезпечувати культуру використання систем відеоспостереження та дотримання вимог законодавства щодо захисту приватності та конфіденційності.

4.2 Дослідження процесу реалізації розробленого методу

Дослідження процесу реалізації розробленого методу забезпечення конфіденційності в системах відеоспостереження може включати наступні кроки:

1) Аналіз потреб користувачів: Для визначення потреб користувачів необхідно провести аналіз їх вимог та очікувань від системи відеоспостереження, зокрема щодо забезпечення конфіденційності. Після аналізу вимог необхідно визначити, які технічні та організаційні заходи можуть бути застосовані для забезпечення конфіденційності.
2) Розробка технічного рішення: На основі аналізу вимог можна розробити технічне рішення для забезпечення конфіденційності в системі відеоспостереження. Це може включати застосування шифрування відеоданих, встановлення обмежень доступу до відеоданих, встановлення систем контролю доступу та інші технічні заходи.
3) Встановлення програмного забезпечення: Після розробки технічного рішення необхідно встановити програмне забезпечення для забезпечення

його функціонування. Це може включати встановлення спеціалізованих програм для шифрування відеоданих та програм для керування доступом до відеоданих.

4) Налаштування системи: Після встановлення програмного забезпечення необхідно налаштувати систему для забезпечення конфіденційності. Це може включати налаштування параметрів шифрування, встановлення прав доступу до відеоданих, налаштування систем контролю доступу та інші налаштування.
5) Тестування та впровадження: Після налаштування системи необхідно провести тестування розробленого методу на відповідність вимогам користувачів та вимогам безпеки. У процесі тестування можуть бути виявлені помилки та недоліки, які необхідно виправити перед впровадженням методу.
6) Навчання персоналу: Після успішного тестування та впровадження методу необхідно провести навчання персоналу з використання нової системи забезпечення конфіденційності. Це може включати навчання з встановлення прав доступу до відеоданих, роботи з програмним забезпеченням для забезпечення конфіденційності та інші теми, що стосуються безпеки відеоспостереження.
7) Запровадження системи: Після успішного навчання персоналу можна запровадити систему в роботу та забезпечити постійний контроль її роботи. Важливо забезпечити регулярні оновлення системи та перевірки на відповідність вимогам безпеки.

Крім того, важливим аспектом реалізації методу є забезпечення сумісності з існуючими системами відеоспостереження. Якщо система забезпечення конфіденційності не може працювати з існуючими системами, то це може призвести до недоступності важливих відеоданих. Крім того, важливо забезпечити можливість відновлення даних в разі їх втрати або пошкодження. Для цього можуть використовуватись різні методи, такі як резервне копіювання

даних на зовнішні носії або використання хмарних сервісів збереження даних. Нарешті, важливо забезпечити постійний моніторинг роботи системи забезпечення конфіденційності. Це може включати аналіз логів доступу до відеоданих, моніторинг роботи системи забезпечення конфіденційності та виявлення потенційних загроз безпеці. Це допоможе забезпечити вчасну виявлення та усунення можливих проблем з безпекою та конфіденційністю. Усі ці аспекти допоможуть забезпечити успішну реалізацію методу забезпечення конфіденційності в системах відеоспостереження та забезпечити надійний захист персональних даних та конфіденційності. Для ефективної реалізації методу забезпечення конфіденційності в системах відеоспостереження необхідно врахувати деякі особливості роботи з відеоданими. Зокрема, важливо визначити, які саме дані потрібно захищати, як їх обробляти та зберігати. Під час розробки методу потрібно враховувати правові аспекти захисту персональних даних. Для цього важливо дотримуватись вимог законодавства щодо захисту персональних даних, таких як загальний регламент про захист персональних даних (GDPR) в Європейському Союзі або Закон про захист персональних даних в США. Крім того, важливо розглянути варіанти зменшення обсягу обробки даних, що зменшує витрати на обробку та зберігання відеоданих. Один з таких варіантів - використання алгоритмів обрізання відеофрагментів для зменшення кількості зберіганих даних. У реалізації методу також можна використовувати технології шифрування даних для забезпечення їх безпеки під час трансмісії та зберігання. Також важливо забезпечити максимально можливу фізичну безпеку серверів збереження відеоданих, наприклад, за допомогою розташування їх у захищених приміщеннях або використання електронного контролю доступу. Крім того, метод може включати розробку механізмів контролю доступу до відеоданих. Це дозволяє забезпечити, що доступ до відеоданих мають тільки дозволені користувачі, а заборонені користувачі не мають доступу до цих даних. Щоб додатково захистити дані від несанкціонованого доступу, можна

використовувати різні техніки шифрування. Наприклад, шифрування каналу зв'язку між камерою та сервером або шифрування самої зображення перед його передачею. Це ускладнює можливість доступу до даних з боку зловмисника, який намагається перехопити передачу даних. Окрім того, важливо встановити правильні права доступу до даних в системі відеоспостереження. Тільки авторизовані користувачі повинні мати доступ до конфіденційної інформації. Також можна застосовувати механізми аудиту дій користувачів, які дозволять відслідковувати, хто, коли та що змінював в системі відеоспостереження. Нарешті, важливо забезпечити фізичну безпеку обладнання системи відеоспостереження. Камери повинні бути розміщені в таких місцях, щоб ніхто не міг їх підривати або зламувати, а обладнання повинно бути захищене від фізичних пошкоджень та втрати електропостачання. Для забезпечення фізичної безпеки обладнання системи відеоспостереження можна використовувати різні методи. Наприклад, камери можуть бути розміщені на висоті, щоб унеможливити їх зламання або руйнування, а також використовувати спеціальні оболонки для захисту камер від погодних умов. Для забезпечення електропостачання обладнання важливо мати резервне джерело живлення, наприклад, генератор електроструму або UPS (унінтераптібл повер суплай). Це допоможе уникнути втрати даних в разі перерви в електропостачанні. Також важливо забезпечити безпеку самої системи відеоспостереження від можливих кібератак. Для цього можна використовувати програмне забезпечення, що захищає від зламу та віддаленого доступу до системи відеоспостереження. Одним із ефективних методів захисту від кібератак є регулярне оновлення програмного забезпечення та патчів безпеки. Також можна використовувати систему виявлення вторгнень, яка допомагає виявити та запобігти атакам. Окремо слід зазначити, що під час розробки методу забезпечення конфіденційності в системах відеоспостереження потрібно враховувати законодавчі та регуляторні вимоги, що регулюють обробку персональних даних та відеозаписів. Наприклад, у багатьох країнах існують законодавчі вимоги

щодо зберігання відеозаписів, строків їх зберігання та правил доступу до них. Тому при розробці методу потрібно враховувати ці вимоги та дотримуватись їх під час реалізації. Також важливо враховувати технічні обмеження та вимоги до обладнання системи відеоспостереження. Наприклад, якщо система має обмежену потужність обробки, то необхідно розробляти метод з урахуванням цих обмежень. Також важливо забезпечити сумісність методу з наявним обладнанням та програмним забезпеченням, яке використовується в системі відеоспостереження. Для забезпечення надійності та безпеки методу забезпечення конфіденційності в системах відеоспостереження можна застосовувати різноманітні заходи захисту. Зокрема, можна використовувати алгоритми шифрування для захисту відеопотоку та збереження відеозаписів у зашифрованому вигляді. Також можна використовувати методи анонімізації, які дозволяють приховати особисті дані людей, які зображені на відеозаписах. Наприклад, можна використовувати методи заміни облич, розмиття образів, зміни кольору волосся та одягу. Крім того, важливо забезпечити захист від несанкціонованого доступу до системи відеоспостереження. Це можна зробити шляхом використання паролів, двофакторної аутентифікації та різних методів ідентифікації та авторизації користувачів. Також можна використовувати системи виявлення вторгнень та моніторингу подій, які дозволяють виявляти та реагувати на можливі загрози. Окрім того, важливо забезпечити належний рівень кваліфікації та навчання персоналу, який відповідає за роботу з системою відеоспостереження. Це дозволить забезпечити правильну настройку та роботу системи, а також вчасне реагування на можливі проблеми та загрози. Для запобігання несанкціонованому доступу до відеоданих також можна використовувати різні методи шифрування, такі як симетричне та асиметричне шифрування. Симетричне шифрування використовує один ключ для шифрування та дешифрування даних, тоді як у асиметричному шифруванні використовується пара ключів: приватний та публічний. Приватний ключ відомий лише власнику, тоді як публічний ключ доступний для широкого

загалу. Для шифрування використовується публічний ключ, а для дешифрування - приватний. Також важливим аспектом забезпечення конфіденційності є фізична безпека системи відеоспостереження, яка полягає в обмеженні фізичного доступу до пристроїв зберігання та передачі даних, а також в захисті від несанкціонованого доступу до інформації через мережеві порти, паролі та інші захисти від кібератак. Крім того, для забезпечення конфіденційності важливо розробити політику доступу до відеоданих, яка визначатиме, які користувачі мають доступ до даних та яким чином вони можуть з ними працювати. Також може використовуватись механізм аудиту доступу, що дозволить контролювати доступ до даних та визначати, хто та коли мав до них доступ. Отже, забезпечення конфіденційності в системах відеоспостереження - це складний процес, що вимагає використання різноманітних заходів та технологій для захисту від несанкціонованого доступу та збереження даних у безпеці.

4.3 Дослідження особливостей використання розробленого методу

Однією з особливостей використання розробленого методу є його гнучкість та можливість адаптації до різних вимог щодо конфіденційності. Залежно від специфіки відеосистеми та вимог до захисту конфіденційної інформації, метод може бути налаштований з використанням різних алгоритмів шифрування, аутентифікації та ідентифікації користувачів. Іншою важливою особливістю є можливість застосування методу на різних етапах відеоспостереження, починаючи від запису відео та закінчуючи його зберіганням. Це дозволяє забезпечити конфіденційність відеоданих на різних етапах обробки та зберігання, а також у різних місцях їх зберігання. Також варто зазначити, що розроблений метод дозволяє забезпечити конфіденційність не лише відеоданих, а й метаданих, таких як дата та час запису, місце зйомки, камера, що зафіксувала відео, тощо. Це дозволяє зберегти не тільки конфіденційність вмісту відео, а й інших важливих даних, що стосуються відеоспостереження. Крім того, розроблений метод може бути успішно використаний у різних

галузях, де відеоспостереження відіграє важливу роль, зокрема в охороні об'єктів, транспортних системах, медичній діагностиці та інших. Додатково про особливості використання розробленого методу можна сказати, що він може бути застосований в різних сферах, де необхідно забезпечувати конфіденційність відеоінформації, наприклад, у сфері банківської діяльності, промисловості, медицини, громадської безпеки тощо. Крім того, залежно від потреб користувача, можна вибирати різні параметри методу, такі як розмір ключа шифрування, рівень стискання, якість відео тощо. Також слід зазначити, що розроблений метод може використовуватися як на стадії запису відео, так і на стадії його передачі та зберігання. Це дає можливість захистити відеоінформацію на різних етапах її життєвого циклу. До переваг розробленого методу також можна віднести те, що він забезпечує конфіденційність відеоданих без значного зниження якості відео. Більш того, метод дозволяє зберігати рівень деталізації відео на рівні, достатньому для вирішення завдань, які передбачає використання систем відеоспостереження. Окрім цього, розроблений метод є достатньо ефективним та може бути застосований на практиці в різних умовах, що робить його досить універсальним. Однак, слід пам'ятати, що немає абсолютно безпечних методів шифрування, тому він має бути використаний в поєднанні з іншими методами захисту відеоданих для максимального забезпечення конфіденційності. Використання розробленого методу забезпечення конфіденційності в системах відеоспостереження має кілька особливостей. По-перше, для успішного застосування методу необхідно провести достатній аналіз ризиків та визначити, які саме дані мають бути захищені, і які можуть бути доступні для перегляду різними користувачами системи відеоспостереження. По-друге, метод може вимагати додаткового обладнання, яке забезпечує шифрування та дешифрування відеоданих, що може збільшувати вартість встановлення та підтримки системи відеоспостереження. По-третє, важливо мати достатній рівень обізнаності та навичок серед персоналу, який відповідає за налаштування та підтримку системи

відеоспостереження, щоб забезпечити правильну роботу методу. Нарешті, важливо визначити діапазон застосування методу, тобто, наскільки далеко можна застосовувати його у системі відеоспостереження, щоб не впливати на якість та швидкість обробки відеоданих, а також не зменшувати ефективність системи відеоспостереження в цілому. На практиці використання розроблений метод дозволяє забезпечувати конфіденційність в системах відеоспостереження за допомогою шифрування трафіку і перетворення даних перед трансляцією. Це дозволяє зменшити ризик несанкціонованого доступу до відеоданих та збільшити рівень захисту особистої інформації. Додатково, розроблений метод може бути ефективним при використанні в системах відеоспостереження з обмеженими обчислювальними можливостями, оскільки він не потребує значних витрат на обчислення. Враховуючи зростаючу популярність відеоспостереження в різних сферах, таких як безпека, транспорт, медицина та бізнес, цей метод може бути корисним для захисту конфіденційності відеоданих у різних галузях. Нарешті, варто зазначити, що розроблений метод не є універсальним і може вимагати певної адаптації для використання в конкретних відеоспостережних системах. Важливо враховувати особливості кожної системи, а також вимоги до захисту конфіденційності даних, щоб досягти оптимального рівня захисту і ефективності.

Висновки до четвертого розділу

З розділу 4 можна зробити висновок, що був розроблений метод забезпечення конфіденційності інформації в системах відеоспостереження, який був реалізований і випробуваний. Опис розробки методу та процесу його реалізації свідчать про те, що це був достатньо складний процес, який включав в себе розробку алгоритмів, програмного забезпечення та апаратної складової. Особливості використання розробленого методу дозволяють забезпечити конфіденційність інформації, що збирається системою відеоспостереження, шляхом шифрування та обмеження доступу до неї лише авторизованих користувачів. Отже, можна стверджувати, що розроблений метод є ефективним

і здатним забезпечити конфіденційність інформації в системах відеоспостереження. Однак, важливо пам'ятати, що кожна система відеоспостереження є унікальною і може мати свої вимоги до захисту конфіденційності інформації. Тому, при впровадженні розробленого методу, необхідно забезпечити адаптацію до конкретної системи та урахування її особливостей.

ВИСНОВКИ

У ході дослідження методів забезпечення конфіденційності інформації, яка отримується та зберігається в системі відеоспостереження, було виявлено, що це завдання вимагає комплексного підходу. Основною метою заходів забезпечення конфіденційності є запобігання несанкціонованому доступу до інформації, а також її неправомірному використанню. У рамках дослідження були розглянуті різні методи забезпечення конфіденційності, такі як шифрування даних, захист мережевого трафіку, використання паролів і біометричних методів аутентифікації, а також засоби знищення інформації після її використання. Було встановлено, що вибір конкретних методів залежить від типу і розміру системи відеоспостереження, а також від потенційних загроз безпеці інформації. Важливою складовою забезпечення конфіденційності є регулярне оновлення програмного забезпечення і апаратного забезпечення системи, а також проведення аудиту заходів забезпечення безпеки. Для забезпечення конфіденційності інформації в системі відеоспостереження, необхідно дотримуватися деяких основних принципів. Перш за все, необхідно встановити дозволи на доступ до інформації тільки для тих користувачів, які мають право на це. Також необхідно захищати інформацію від несанкціонованого доступу за допомогою різноманітних методів шифрування. Ще одним важливим кроком є забезпечення безпеки мережі, на якій працює система відеоспостереження. Для цього можна використовувати заходи, такі як захист мережевого трафіку, використання віртуальних приватних мереж (VPN), встановлення брандмауерів та інших захистів. Для забезпечення відповідного рівня конфіденційності важливо також використовувати сучасні засоби аутентифікації, такі як біометричні методи, що дозволяють ідентифікувати користувачів на основі їхніх фізичних

характеристик. Окрім цього, необхідно забезпечувати відповідний рівень захисту даних після їх використання, наприклад, використовуючи засоби знищення інформації після закінчення строку її зберігання. Важливо також проводити регулярні перевірки системи відеоспостереження та аналізувати її потенційні вразливості, щоб своєчасно виявляти та виправляти можливі проблеми. Отже, можна зробити висновок, що забезпечення конфіденційності інформації, яка отримується та зберігається в системі відеоспостереження, є важливою задачею, яка вимагає використання різноманітних методів і заходів. Необхідно дотримуватися принципу комплексного підходу та використовувати найбільш ефективні засоби забезпечення безпеки для конкретної системи відеоспостереження.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

- Арапова А. Система управління ризиками як необхідна складова забезпечення кібербезпеки. URL:http://repository.mdu.in.ua/jspui/bitstream/123456789/658/1/kiberbezpeka_2018.pdf (дата звернення: 19.04.2023).
- Архипов О. Інформаційні ризики: методи та способи дослідження, моделі ризиків і методи їх ідентифікації / О. Архипов, А. Скиба // Захист інформації. – 2013. – Т. 15, № 4. – С. 366–375.
- Богуш В. М., Кривуца В. Г., Кудін А. М., Інформаційна безпека: Термінологічний навчальний довідник/ За ред. Кривуци В. Г. К., 2004. 508 с
- Верескун М. Методичне забезпечення системи інформаційної безпеки промислових підприємств / М. Верескун // Економіка і організація управління. – 2014. – Вип. 1–2. – С. 54–60.
- Волосович С., Клапків Л. Детермінанти виникнення та реалізації кіберризиків. URL: http://zt.knteu.kiev.ua/files/2018/03(98)/10.pdf. (дата звернення: 19.04.2023).
- Завгородня М. Можливості та ризики використання цифрових технологій упромисловості.URL:https://ir.kneu.edu.ua/bitstream/handle/2018/31551/ZE_2019_ 55.pdf?sequence=1&is Allowed=y. (дата звернення: 29.04.2023).
- Збожинський С. Інформаційна безпека під час застосування цифрових технологій. URL: http://yur–gazeta.com/publications/practice/zahist–intelektualnoyi–vlasnosti–avtorske–pravo/informaciyna–bezpeka–pid–chas–zastosuvannya–cifrovih–tehnologiy.html. (дата звернення: 29.04.2023).
- Інформаційна безпека підприємства у динамічному ринковому середовищ М.П. Войнаренко, Г.І. Рзаєв, Т.Г. Рзаєва / Хмельницький національний університет 2014р.

- . Інформаційна загроза. URL: https://uk.wikipedia.org/wiki/Інформаційна_загроза (дата звернення: 19.04.2023).
- Кириленко А., Бабинюк О. Кібербезпека на захисті бізнесу. URL: https://ir.kneu.edu.ua/bitstream/handle/2018/31417/ZE_2019_118.pdf?sequence=1. (дата звернення: 22.04.2023).
- Основні складові інформаційної безпеки / URL: https://studfile.net/preview/14517462/page:2/ (дата звернення: 22.04.2023).
- Сакович Л.М / Порівняльний аналіз моделей надійності програмного забезпечення засобів спеціального зв'язку// Сакович Л.М., Павлов В.П., Лівенцев С.П., Небесна Я.Е. ///Information Technology and Security" № 2(2)- 2012
- Северина С. Інформаційна безпека та методи захисту інформації / С. Северина // Вісник Запорізького національного університету. Економічні науки. – 2016. – № 1. – С. 155–161. (дата звернення: 29.04.2023).
- Сотниченко В. Інформаційна безпека як базова складова економічної безпеки телекомунікаційного підприємства. URL: http://www.dut.edu.ua/uploads/p_1010_25433567.pdf. (дата звернення: 22.04.2023).
- Шемчук Віктор Вікторович/ Навчально-наукового гуманітарного інституту Таврійського національного університету імені В. І. Вернадського / загрози інформаційній безпеці: проблеми визначення та подолання/ URL: http://maup.com.ua/assets/files/expert/7/23.pdf (дата звернення: 22.04.2023).
- http://datami.ua/informatsijna-bezpeka-vidi-zagroz-i-metodi-yih-usunennya/ (дата звернення: 25.04.2023).
- https://www.researchgate.net/publication (дата звернення: 25.04.2023).
- https://pidru4niki.com/16330826/politologiya/metodi_zabezpechennya_informatsiynoyi_bezpeki (дата звернення: 25.04.2023).

- Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1–002–99.–К.. ДСТСЗІ СБ України, 1999. – 16 с
- ОСНОВИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ Заплотинський Б.А.
- https://www.ibm.com/support/pages/sites/default/files/inline-files/$FILE/TSS%20TOMs%20V1.0%202017-12-18_uk_UA_0.pdf (дата звернення: 25.04.2023).
- Головань С.М. Нормативне забезпечення інформаційної безпеки / С.М. Головань, О.С. Петров, В.О. Хорошко, Д.В. Чирков, Л.М. Щербак / За ред. проф. В.О. Хорошка. – К.: ДУІКТ, 2008. – 533 с.
- Хорошко В.О. Основи інформаційної безпеки / В.О. Хорошко, В.С. Чередниченко, М.Є. Шелест /За ред. проф. В.О. Хорошка. – К.: ДУІКТ, 2008. – 186 с.
- Термінологічний довідник з питань технічного захисту інформації / С.Р. Коженевський, Г.В. Кузнецов, В.О. Хорошко, Д.В. Чирков / За ред. проф. В.О. Хорошка. – К.: ДУІКТ, 2007. – 365 с.
- Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 №81/94-ВР//ВВР, 1994. — № 31. — С. 287.
- Богуш В. М. Інформаційна безпека держави / В. М. Богуш, О. К. Юдін. — К. : МК-Прес, 2005. — 432 с.
- Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. Навчальний посібник / С.О. Іванченко, О.В. Гавриленко, О.А. Липський, А.С. Шевцов – К.: ІСЗЗІ НТУУ «КПІ», 2016. − 104 с.
- Інформаційна безпека: навчальний посібник / [Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв та ін.]; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. – Львів: Видавництво Львівської політехніки, 2019. – 580 с.

- Технології захисту інформації / Ю. А. Тарнавський – Київ : КПІ ім. Ігоря Сікорського, 2018. – 162 с
- Захист інформації в автоматизованих системах управління : навчальний посібник / Уклад. І. А. Пількевич, Н. М. Лобанчикова, К. В. Молодецька. – Житомир : Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.
- Остапов С. Е. технологія захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.
- Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби : посібник / [В. Л. Бурячок, С. В. Толюпа, В. В. Семко та ін.]. – К. : ДУТ-КНУ, 2016. – 178 с.
- Bashir M., Christin N. Three case studies in quantitative information risk analysis. In Proceedings of the CERT/SEI Making the Business Case for Software Assurance Workshop. P. 77—86, Pittsburgh, PA, September 2008.
- Захист інформації в автоматизованих системах управління : навчальний посібник / Уклад. І. А. Пількевич, Н. М. Лобанчикова, К. В. Молодецька. – Житомир : Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.
- Остапов С. Е. технологія захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.
- Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби : посібник / [В. Л. Бурячок, С. В. Толюпа, В. В. Семко та ін.]. – К. : ДУТ-КНУ, 2016. – 178 с.
- Захист конфіденційної інформації - персональних даних [Електронний ресурс]. – Режим доступу https://cutt.ly/iuggGRH (дата звернення: 29.04.2023).
- Голубенко О.Л., Хорошко В.О., Петров О.С., Головань С.М., Яремчук Ю.Є., Політика інформаційної безпеки: підручник. – Луганськ: вид-во СНУ ім.. В.Даля, 2009, - 300с.
- Ємельянов С.Л. Основи інформаційної безпеки. – Одеса: Фенікс, 2014.– 357 с.

- Бурячок В.Л. Інфомаційна та кібербезпека / В.Л. Бурячок, В.Б. Толубко, В.О. Хорошко, С.В. Толюпа. – К.: ДУТ, 2015. – 288 с.
- https://ecpl.com.ua/wp-content/uploads/2019/02/107-REKOMENDATSIY.pdf (дата звернення: 27.04.2023).
- http://politics.ellib.org.ua/pages-8288.html (дата звернення: 27.04.2023).
- https://valtek.com.ua/ua/system-integration/security-control-system/integrated-security-systems/information-security-system-review (дата звернення: 27.04.2023).
- Грайворонський М. В. Безпека інформаційно-комунікаційних систем / М. В. Грайворонський, О. М. Новіков – К.: Видавнича група BHV, 2009. – 608 с.
- Коркішко Т. Алгоритми та процесори симетричного блокового шифрування / Т. Коркішко, А. Мельник, В. Мельник. – Львів. БаК, 2003. – 168 с.
- Богуш В.М., Довидьков О.А. Основи захищених інформаційних технологій. – К.: ДУІКТ, 2005 - 450 с.
- Богуш В.М., Кривуца В.Г., Кудін А.М. Інформаційна безпека: термінологічний навчальний довідник. – К.: ООО “Д.В.К.” 2004. – 508 с.
- Горячева К. Фінансова безпека підприємства, сутність та місце в системі економічної безпеки // Економіст. — 2003. — № 8. — С. 23–28.
- Задірака В. К. Методи захисту фінансової інформації. — Тернопіль: Збруч, 2000. — 460 с.
- Комаха А. Організація служби економічної безпеки на підприємстві // Бізнес і безпека. — 2002. — № 3. — С. 12–13.
- https://library.kre.dp.ua/Books (дата звернення: 29.04.2023).
- https://www.researchgate.net/publication/323728995_Doslidzenna_efektivnosti_metodiv_biometricnoi_avtentifikacii (дата звернення: 29.04.2023).
- http://www.rusnauka.com/1_NIO_2011/Medecine/77655.doc.htm (дата звернення: 29.04.2023).

- http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe (дата звернення: 29.04.2023).
- Ахрамович. В.М. Ідентифікація й аутентифікація, керування доступом. Сучасний захист інформації. К. ДУТ:-2016 .-№4.- с. 47-51
- П. Браіловський М.М., Головень СМ. та інші. - Технічний захист інформації на об'єктах інформаційної діяльності/ За ред. Проф. В.О. Хорошка. -К.:ДУІКТ, 2007.
- https://dut.edu.ua/repozitorii/sikz (дата звернення: 28.04.2023).
- Біометричні технології в XXI столітті та їх використання правоохоронними органами: посібник / В. П. Захаров, В. І. Рудешко; Львів. держ. ун-т внутр. справ. — 2-ге вид., допов. — Львів: ЛьвДУВС, 2015. — 491 с.
- https://elartu.tntu.edu.ua/bitstream/lib/29788/2/mag_Vaplyak_A_P_RBm-61.pdf (дата звернення: 28.04.2023).
- https://www.usebouncer.com/uk (дата звернення: 28.04.2023).
- https://worldvision.com.ua/articles/formi-biometricheskoy-autentifikatsii (дата звернення: 28.04.2023).
- https://interesinformation.blogspot.com/2020/12/blog-post.html (дата звернення: 29.04.2023).
- https://sites.google.com/site/identifikaciataautentifikacia/ponatta-pro-autentifikaciu/metodi-autentifikaciie (дата звернення: 29.04.2023).
- https://e-tk.lntu.edu.ua/mod/resource/view.php?id=3261 (дата звернення: 29.04.2023).
- http://kristall-systems.net.ua/ua/novosti/pochemu_biometricheskay_autentifikatsiy_luchshe_chem_vyi_dumaete/ (дата звернення: 29.04.2023).