УДК 004.8:65.05:681.5 DOI: 10.31673/2518-7678.2019.0306373

Катков Ю.І., к.т.н.; **Сєрих С.О.,** к.т.н.;
Шашлов А.В., студент; **Вергун Д.С.,** студент

КІБЕРНЕТИЧНІ СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ОБ'ЄКТІВ ПІДПРИЄМСТВА КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Katkov Yu. I., Sierykh S. O., Shashlov An. V., Vergun D.S. Cyber-based video surveillance systems to ensure the safety of critical infrastructure facilities

The article discusses the cybernetic approach to the study of video surveillance systems, which are an integral part of the crisis management system and are called cybernetic video surveillance systems to ensure the safety of critical infrastructure facilities. Security (providing protection against risks, challenges and threats) of critical infrastructure enterprises is today the basis for successful economic development. Therefore, in a critical infrastructure, to ensure the safety of enterprise facilities, it is necessary to have a crisis management system that can manage situations using cybernetic systems and digitalization technologies (datafication). Crisis management systems consist of many different types of systems for making decisions on countering all sorts of risks, challenges or threats. Crisis management systems include a number of subsystems: diagnostics and forecasting of the state of the organization; marketing and management; anti-crisis investment policy; personnel management and management activities; information support; security, including video surveillance systems. Modern crisis management systems tend to be equipped with cybernetic (intelligent) systems that are able to perceive, store, transmit and transform information. The application of the cybernetic approach to the study of video surveillance systems is due to the fact that in any security subsystem there is always a video surveillance subsystem. It is designed to solve a set of urgent tasks of ensuring security on the territory of enterprises' facilities and increasing the efficiency of the enterprise from critical infrastructure, for example, nuclear power plants, ammonia plants and others. These tasks include: automated access control to the territory and premises of enterprises; ensuring broadcast recording of force majeure situations and others.

Keywords. Intelligent system, cyber video surveillance, security, vulnerable elements critical infrastructure

Катков Ю. І. , Сєрих С. О., Шашлов А. В., Вергун Д.С. Кібернетичні системи відеоспостереження для забезпечення безпеки об'єктів підприємства критичної інфраструктури

У статті розглядаються кібернетичний підхід до вивчення систем відеоспостереження, які є складовою частиною системи антикризового управління та називаються кібернетичними системами відеоспостереження для забезпечення безпеки об'єктів підприємства критичної інфраструктури. Забезпечення безпеки (забезпечення захисту від ризиків, викликів і загроз) об'єктів підприємств критичної інфраструктури є сьогодні основою успішного розвитку економіки. Сучасні системи антикризового управління мають тенденцію оснащення кібернетичними (інтелектуальними) системами, які здатні сприймати, зберігати, передавати і перетворювати певну інформацію. Застосування кібернетичного підходу до вивчення систем відеоспостереження пов‘язане з тім, що у будь-якій підсистемі безпеки обов'язково є підсистема відеоспостереження. Вона призначена для вирішення комплексу актуальних завдань забезпечення безпеки на території об‘єктів підприємств і підвищення ефективності роботи підприємства зі складу критичної інфраструктури, наприклад, атомних електростанцій, заводів з виробництва аміаку тощо. До таких завдань відносяться: автоматизований контроль доступу на територію і в приміщення підприємств; забезпечення відео трансляції, запис форс-мажорних ситуацій та інші.

Ключові слова. Інтелектуальна система, кібернетична відеоспостереження, безпека, вразливі елементи критична інфраструктура

Катков Ю. И., Серых С. А., Шашлов А. В., Вергун Д.С. Кибернетические системы видеонаблюдения для обеспечения безопасности объектов предприятия критической инфраструктуры

В статье рассматриваются кибернетический подход к изучению систем видеонаблюдения, которые являются составной частью системы антикризисного управления и называются кибернетическими системами видеонаблюдения для обеспечения безопасности объектов предприятия критической инфраструктуры. Обеспечение безопасности (обеспечение защиты от рисков, вызовов и угроз) объектов предприятий критической инфраструктуры является сегодня основой успешного развития экономики. Современные системы антикризисного управления

имеют тенденцию оснащение кибернетическими (интеллектуальными) системами, которые способны воспринимать, хранить, передавать и преобразовывать информацию. Применение кибернетического подхода к изучению систем видеонаблюдения связано с тем, что в любой подсистеме безопасности обязательно есть подсистема видеонаблюдения. Она предназначена для решения комплекса актуальных задач обеспечения безопасности на территории объектов предприятий и повышения эффективности работы предприятия из состава критической инфраструктуры, например, атомных электростанций, заводов по производству аммиака и др. К таким задачам относятся: автоматизированный контроль доступа на территорию и в помещения предприятий; обеспечение трансляция запись форс-мажорных ситуаций и другие.

Ключевые слова. Интеллектуальная система, кибернетическая видеонаблюдения, безопасность, уязвимые элементы критическая инфраструктура.

Вступ

У статті розглядаються кібернетичний підхід до вивчення систем відеоспостереження, які є складовою частиною системи антикризового управління та називаються кібернетичними системами відеоспостереження для забезпечення безпеки об'єктів підприємства критичної інфраструктури.

Забезпечення безпеки (забезпечення захисту від ризиків, викликів і загроз) об'єктів підприємств критичної інфраструктури є сьогодні основою успішного розвитку економіки. Наочний приклад: успішна атака десятка дронів на кілька нафтопереробних заводів Саудівської Аравії викликала зміни котирувань вартості нафти. Це наочно показує вразливість об'єктів критичної інфраструктури. Тому в критичній інфраструктурі для забезпечення безпеки об'єктів підприємства необхідно мати в наявності систему антикризового управління, здатну управляти ситуаціями за допомогою кібернетичних систем (cybernetic systems) і технологій цифровізації (datafication).

Системи антикризового управління складаються з безлічі різноманітних типів систем для прийняття рішення щодо протидії різного роду ризиків, викликів або загрозам. Відомо, що відповідно до теорії антикризового управління така система включає ряд підсистем: діагностики та прогнозування стану організації; маркетингу і менеджменту; антикризової інвестиційної політики; управління персоналом та організаційно-управлінських заходів; інформаційного забезпечення; безпеки та ін. [1-18]

Сучасні системи антикризового управління мають тенденцію оснащення кібернетичними (інтелектуальними) системами, які здатні сприймати, зберігати, передавати і перетворювати певну інформацію. Така кібернетична підсистема складається з адаптивних систем спостереження за агрегацією даних, систем аналізу цих даних, а також засобів протидії кризам.

Відомо, що кібернетична система - це безліч взаємопов'язаних об'єктів (елементів системи) здатних сприймати, запам'ятовувати і переробляти інформацію, а також обмінюватися інформацією. Відомо, що кібернетика розглядає системи незалежно від природи елементів, що входять в них. Кібернетичним системам властиві самоорганізація і самонавчання (адаптація, накопичення досвіду). Приклади кібернетичних систем - автоматичні регулятори в техніці, комп'ютери, біологічні популяції та інші. Кожна така система являє собою безліч взаємопов'язаних об'єктів, здатних сприймати, запам'ятовувати і переробляти інформацію, а також обмінюватися нею.

Застосування кібернетичного підходу до вивчення систем відеоспостереження пов‘язане з тім, що у будь-якій підсистемі безпеки обов'язково є підсистема відеоспостереження. Вона призначена для вирішення комплексу актуальних завдань забезпечення безпеки на території об‘єктів підприємств і підвищення ефективності роботи підприємства зі складу критичної інфраструктури, наприклад, атомних електростанцій, заводів з виробництва аміаку тощо. До таких завдань відносяться: автоматизований контроль доступу на територію і в приміщення підприємств; забезпечення відео трансляції, запис форс-мажорних ситуацій та інші.

Видимо, що системи відеоспостереження забезпечують збір даних для контролю безпеки об'єктів підприємства. Сучасні системи відеоспостереження в режимі онлайн спостерігають процеси або події, перетворюють цифрової відеоряд в бази «великих даних». Ці бази даних

використовуються для відстеження тенденцій зміни процесів або станів. Впровадження різних технологій штучного інтелекту дозволяє виконувати прогнозний аналіз в реальному масштабі часу цих онлайн кількісних даних і генерувати варіанти для прийняття рішень щодо запобігання криз. Оцифрування спостережуваних процесів або подій виконується за допомогою технологій IP- відеоспостереження, які мають широке коло галузевих рішень. На сьогодні відомі рішення побудови систем IP-відеоспостереження для різних об'єктів критичної інфраструктури, наприклад:

1. Для бізнес-інфраструктури - системи IP-відеоспостереження враховують специфіку торгових центрів, магазинів, бізнес-центрів, офісів, банків, готелів, ресторанів і кафе.

2. Для «Безпечного і розумного міста» - системи IP-відеоспостереження створюються для спостереження в освітніх і медичних установах; в місцях масових заходів (в музеях і галереях, в спортивних спорудах, в місцях відпочинку і розваг), в транспорті (на лініях руху, в вокзалах (станціях) автомобільних, залізниць, аеропортах, метро, в паркінгах, на парковках і АЗС) .

3. Для державних і виправних установ, об'єктах приватної власності (житлові комплекси, будинки) - системи IP-відеоспостереження створюються для спостереження за процесами і подіями доступу, пожежної безпеки, збереження та інше.

4. Для об'єктів виробництва з підвищеною небезпекою - системи IP-відеоспостереження створюються для спостереження за процесами і подіями доступу на об'єктах, наприклад, на електростанціях, водосховищах, виробництвах небезпечних речовин, а також для контролю процесів і подій ввезення / вивезення та збереження на об'єктах логістики (морські та річкові порти, логістичні центри, склади).

5. Для контролю технологічних процесів на об'єктах промисловості - системи IP-відеоспостереження створюються для спостереження за процесами і подіями виконання технологій виробництва продукції на підприємствах, при будівництві, видобутку корисних копалин, в сільському господарстві.

Кожне таке рішення відображає особливості об'єкта і має унікальність. Але застосування кібернетичного підходу до вивчення систем відеоспостереження як складних об'єктів живої і неживої природи полягає в розгляд їх як перетворювачів інформації. Тому актуальним є вивчення загальних принципів побудови, апаратного та програмного забезпечення кібернетичних систем відеоспостереження для забезпечення безпеки об'єктів підприємства критичної інфраструктури.

Виклад основного матеріалу дослідження

Кібернетичні системи відеоспостереження - це впорядкована сукупність об'єктів (елементів системи), що взаємодіють і взаємопов'язаних між собою, які здатні сприймати, запам'ятовувати і переробляти відеоінформацію, а також обмінюватися нею.

Кібернетична система відеоспостереження є відкритою. Має як вхідні, так і вихідні канали, по яких вона обмінюється сигналами із зовнішнім середовищем. Відомо, що відкрита кібернетична система може розглядатися як перетворювач вхідних сигналів у вихідні, тобто як перетворювач інформації. Тому вважаємо, що кібернетична система відеоспостереження складається з рецепторів у вигляді датчиків або детекторів, мережі телекомунікації (каналів прямого і зворотного зв'язку) та аналізаторів сигналів.

Пропонується вважати, що функціонування кібернетичної системи відеоспостереження описується трьома видами функцій: функціями, які враховують зміну станів елементів системи; функціями, що викликають зміни в структурі системи (в тому числі і внаслідок зовнішнього впливу); функціями, що забезпечують передавання сигналів за її межі.

Рецепторами є відеокамери, які перетворять спостереження поточного стану об'єкта в відеоряд (в відео- та аудіо інформацію). Відеокамери можуть виконувати функції датчика (перетворювача контрольованої величини в зручний для використання сигнал) або детектора (пристрій, якій вказує на наявність перевищення порогового значення відповідної величини). Відеокамер може бути від 1 до 1000. Кожна з них створює відеоряд вихідних даних.

Відеоряд перетворюється в початкових масив даних, які передають по каналах телекомунікації до аналізатора сигналів. Вихідний масив даних фіксує безперервні або дискретні стану об'єктів (елементів) системи, що спостерігається. Відеоряд описується безліччю параметрів, які поділяються на безперервні, які приймають будь-які значення в певному інтервалі, або дискретні, які приймають кінцеві значення.

У кібернетичних системах відеоспостереження мережу телекомунікації створюється на основі проводових або безпроводових телекомунікаційних технологіях. Ці мережі можуть передавати дані на будь-які відстані.

У кібернетичних системах відеоспостереження аналізаторами сигналів є апаратно-програмні комплекси зі спеціальним програмним забезпеченням штучного інтелекту. За допомогою технологій штучного інтелекту кібернетична система відеоспостереження здатна: сприймати певну «інформацію»; зберігати цю інформацію в «пам'яті»; передавати її по «каналах зв'язку»; аналізувати (переробляти) інформацію в «сигнали», що направляють діяльність об'єкта будь-якої системи в відповідну сторону.

Ступінь глибини аналізу різниться: за своєю складністю; за ступенем визначеності; за рівнем організації. Залежно від прийнятих критеріїв обмеження небезпеки генеруються варіанти рішень для автоматичного або автоматизованого прийняття рішення в поточних або критичних ситуаціях. Аналіз відеоданих може проводитися безперервно або дискретно в часі, що визначається необхідним ступенем точності дослідження процесу, технічними і математичними зручностями. Аналіз відеоданих виконується на основі детермінованих або імовірнісних математичних моделей.

Складність побудови кібернетичних систем відеоспостереження визначається двома факторами. По-перше, розмірністю системи (загальне число параметрів, що характеризують стан всіх її елементів), по-друге, складністю структури системи (загальним числом зв'язків між її елементами та їх різноманітністю). Складні кібернетичні системи відеоспостереження - це системи, опис яких не зводиться до опису окремих елементів і загальної кількості однотипних елементів. Складні системи відрізняються від простих тим, що вони здатні керувати своєю поведінкою.

Таким чином, головною відмінністю кібернетичних систем відеоспостереження від звичайних є здатність аналізувати дані про поточний стан об'єктів відносно попереднього або початкового стану об'єкта, що спостерігається, і який прийняти за еталон.

Розглянемо перелік функцій, якими повинні володіти кібернетичні системи відеоспостереження для забезпечення безпеки об'єктів підприємства критичної інфраструктури: 1) Організувати автоматизований контроль доступу автомобілів на територію об'єкта, що спостерігається; 2) Організувати автоматизований контроль доступу людей в приміщення об'єкта, що спостерігається; 3) Забезпечувати безперервну відео трансляцію і запис незважаючи на форс-мажорні ситуації; 4) Створювати покрити більшу зону спостереження об'єкта меншою кількістю камер; 5) Скоротити вартість системи відеоспостереження об'єкта; 6. Отримувати негайні повідомлення на монітор, смартфон або електронну пошту: про відсутність співробітника на своєму робочому місці; про перетин будь-ким контрольної лінії або периметра; про появу людини в забороненому місці; про фіксацію відсутності спеціального одягу, наприклад. каски на голові працівника; про виявлення диму або вогню на території об'єкта; про будь-яких аномально гучних звуках в зоні відеоспостереження на території об'єкта; про виявлення несправності камер відеоспостереження об'єкта; 7) Виконувати автоматично відео аналітику щодо: розпізнавання автономерів, розпізнавання осіб; резервування каналу з відображенням; управління PTZ-камерами; розгортки fisheye камер: контролю активності персоналу; трекінгу; виявлення осіб; відсутності заданих засобів захисту на особі; появи диму і вогню; появи гучного звуку та ознак саботажу.

Розглянемо приклади побудови деяких функції.

Розпізнавання автономерів. Застосовується для автоматизації контролю пропуску автомобільного транспорту на територію об'єкта. Ця функція дозволяє (Рис.1): додавати в

базу даних «білі» і «чорні» номери автомобілів; зберігати час і дату розпізнавання, номерний знак а також відео фрагмент проїзду автомобіля, номер якого зафіксований камерою; вивантажувати списки номерів в формати XLS і CSV.

Рис. 1 - Розпізнавання автономерів

За допомогою системи «Розпізнавання автономерів» можливо: запобігати несанкціоноване проникнення транспортних засобів на територію об'єкта; організувати автоматичне відкривання шлагбаума при в'їзді / виїзді автомобілів з території об'єкта. Таким чином, створюється можливість забезпечити безпеку об'єкта, а також знизити витрати на забезпечення безпеки.

Розпізнавання осіб. Застосовується для автоматизації та контролю доступу людей на територію об'єкта. Ця функція дозволяє (Рис.2): інтегрувати модуль з системою контролю і управління доступом (СКУД) до об'єкта; створювати базу фото осіб зі статусами «довірена» і «чорний список»; отримувати автоматичні повідомлення на монітор, телефон, e-mail про спроби проникнення осіб, які не мають прав доступу; шукати фрагменти з виявленим особою в відео-архіву, шукати людей в відео-архіву по фотографіях.

Рис. 2 - Розпізнавання осіб

За допомогою системи «Розпізнавання осіб» можна контролювати допуск персонал в усі приміщення об'єкта, а саме: забезпечити автоматичний допуск на територію та до приміщень об'єкта працівників, які мають дозвіл на це і контролювати час їх перебування там; запобігати проникненню на територію і в приміщення об'єкта осіб, які не мають на це дозволу. Таким чином, створюється можливість забезпечити високий рівень безпеки працівників та інфраструктури на основі біометричних методів контролю.

Резервування каналу з відображенням. Дозволяє забезпечувати відео потік і запис відео незалежно від форс-мажорних ситуацій. Ця функція дозволяє встановлювати спеціальний модуль на кожній камері, запис з якої критично важлива. Якщо сервер разом з камерами, на

яких встановлено модуль, вийде з ладу, ці камери будуть переведені на резервний сервер автоматично. Це забезпечить постійну передачу відеопотоку і запобіжить втрату архіву, поки сервер знаходиться у відключеному стані (Рис.3).

Рис. 3 - Резервування каналу з відображенням

Завдяки «Резервуванню каналу з відображенням» видсютня втрата жодної хвилини відео потоку. Є можливість отримувати все оповіщення на смартфон або на електронну пошту, не дивлячись на проблеми з сервером. Таким чином, створюється можливість забезпечити безперервне отримання інформації для організації безпеки працівників і не допускати збитків майну, інфраструктурі об'єкта.

Управління PTZ-камерою. Використання і управління PTZ-камерами дозволяє забезпечувати велику гнучкість системи відеоспостереження об'єкта. Ця функція дозволяє (Рис. 4): повертати PTZ-камеру в потрібному напрямку з використанням джойстика або клавіатури; збільшувати або зменшувати зображення з камери за допомогою оптичного зуму; управляти фокусом камери в автоматичному або ручному режимі; налаштовувати сценарії для PTZ-камери.

Рис. 4 - Управління PTZ-камерою

Завдяки функції «Управління PTZ-камерами» є можливість: замінити кілька звичайних камер і забезпечити при цьому достатнє охоплення зон спостереження; фіксувати навіть дрібні деталі зображень з камери; фокусувати камеру на бажаному об'єкті спостереження. Таким чином, створюється можливість забезпечити збільшити гнучкість системи відеоспостереження та вирішувати завдання, які не під силу звичайним камерам.

Розгортка fisheye-камерами (риб'яче око). Дозволяє скорочувати вартість системи відеоспостереження за рахунок використання панорамних камер з більш широким охопленням. Ця функція дозволяє отримувати розширені зображення і керувати ними за допомогою джойстика або клавіатури: в режимі подвійного панорами - панорама розділена на дві частини, кожна 180 °; в режимі 4х90 ° зображення розділене на 4 осередки, кожна по 90 °; в віртуальному режимі PTZ, який симулює поведінку PTZ-камери (Рис.5).

Завдяки функції «розгортки fisheye-камер» є можливість замінити звичайні камери на одну камеру типу Fisheye з широким кутом огляду і бачити відразу кілька контрольованих зон з використанням лише однієї камери.

Контроль активності персоналу. Допомагає збільшувати ефективність працівників об'єкта, мінімізувати ризики, пов'язані з людським фактором. Ця функція дозволяє налаштувати до 6-ти контрольних областей моніторингу робочих місць працівників в поле зору кожної камери. Система фіксує рух або його відсутність в кожній контрольній зоні

діяльності в режимі реального часу. При відсутності руху понад установлений вами часу генерується негайне повідомлення на монітор, смартфон або на електронну пошту (Рис.6).

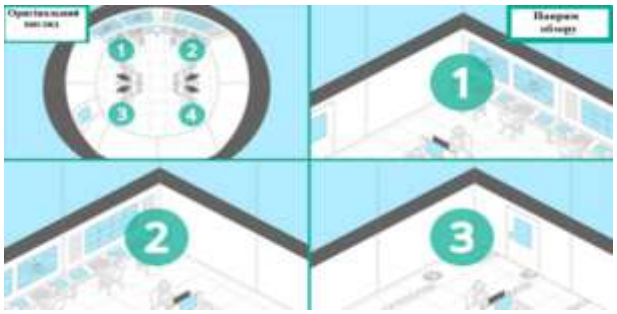

Рис. 5 - Управління PTZ-камерою

Рис. 6 - Контроль активності персоналу

Завдяки функції «Завдяки Контролю активності персоналу» можна приймати ефективні управлінські рішення, пов'язані з: оцінкою часу і якості роботи працівників; оптимізацією програм стимулювання працівників. Таким чином, створюється можливість забезпечити підвищення ефективності роботи персоналу і зменшити ризики небажаних, небезпечних ситуацій, пов'язаних з відсутністю працівників на робочому місці.

Контроль безпеки персоналу. Дозволяє знизити рівень виробничого травматизму і смертності працівників внаслідок порушення ними вимог охорони праці. Ця функція дозволяє ідентифікувати людину в кадрі і перевіряє наявність спецодягу, наприклад, каски на голові. У разі відсутності каски система автоматично передає повідомлення на комп'ютер, смартфон або електронну пошту. Всі події автоматично реєструються. Можна знайти фрагмент відео з порушенням в архіві в будь-який час (Рис.7).

Рис. 7 - Контроль безпеки персоналу

Завдяки функції «Контроль безпеки персоналу» не потрібно дивитися на монітор 24 години на добу. Завдяки детектор відсутності касок можна: мінімізувати випадки порушення правил охорони праці працівниками; запобігати отримання травм на робочому місці; уникати штрафів з боку регулюючих органів; розслідувати обставини випадків порушення правил охорони праці.

Трекінг. Визначення місця розташування рухомих об'єктів в часі за допомогою камери застосовується для мінімізації збитку майна, викликаного діями третіх осіб, а також для зниження ймовірності терористичних актів на території об'єкта. Ця функція дозволяє налаштувати (Рис. 8): мінімальний розмір об'єктів, рух яких необхідно відстежувати; максимальний зсув об'єкта від кадру до кадру - не більше 1/5 кадру.

Рис. 8 - Визначення місця розташування рухомих об'єктів в часі за допомогою камери

Завдяки функції «Трекінг» можна отримувати повідомлення на монітор, смартфон або електронну пошту кожен раз коли: об'єкт перетинає контрольну лінію (вторгнення на територію та інші); об'єкт переміщається по території; об'єкт знаходиться на території тривалий час. Також можна здійснювати пошук по архіву фрагментів відео, на яких об'єкт перетинає контрольну лінію або знаходиться в контрольній зоні. Крім того, можна заощадити ємність сервера, налаштувавши програму так, щоб запис починалася тільки в разі виникнення контрольного події. Таким чином, не обов'язково сидіти перед моніторами для відеоспостереження 24 години на добу. Завдяки трекінгу можна відправити службу безпеки в небезпечну зону для нейтралізації правопорушника і таким чином: забезпечити безпеку працівників; запобігти можливій терористичну атаку; захистити майно та інфраструктуру.

Виявлення заданих осіб. Допомагає мінімізувати збиток майна, знижувати ризики загрози життю і здоров'ю працівників. Ця функція дозволяє (Рис. 9): бачити все обличчя, які опинилися в зоні огляду камери відеоспостереження; отримувати автоматичні повідомлення про виявлення заданих осіб на монітор, смартфон або на електронну пошту; генерувати звіти про кожну людину, присутність якого було зафіксовано камерами, з точним часом його виявлення; зберігати виявлені особи в форматі JPG.

Рис. 9 - Виявлення заданих осіб

Завдяки функції «Виявлення заданих осіб» можна виявити обличчя людини в забороненій зоні і / або в заборонений для знаходження в зоні час. Таким чином, можна запобігати випадкам, які загрожують безпеці працівників і роботі інфраструктури. Крім цього, збережені в базі особи з відміткою про те, де і коли вони були зафіксовані, може допомогти у вирішенні інших завдань, розслідуванні інцидентів і т.п.

Детектор диму і вогню. Допомагає запобігати пожежі і, тим самим, уникати жертв, збитку здоров'ю працівників і майна. Ця функція дозволяє отримувати негайне повідомлення на монітор, смартфон або на електронну пошту (Рис.10).

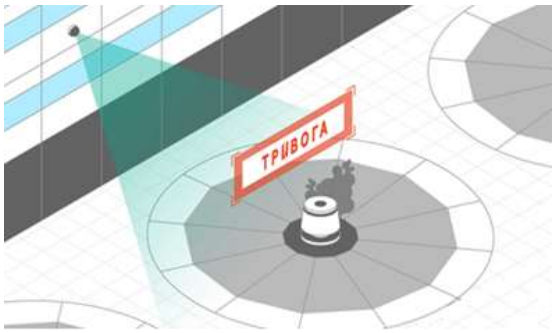

Рис. 10 - Детектор диму і вогню

Всі зафіксовані детектором випадки реєструються в Журналі подій для подальшого швидкого пошуку в архіві. Природно можна інтегрувати «Детектор диму і вогню» з системами пожежної сигналізації та пожежогасіння, щоб забезпечити їх спільну роботу.

Завдяки функції «Детектор диму і вогню» необов'язково сидіти перед моніторами для відеоспостереження 24 години на добу і можна: оперативне відреагувати на виникнення диму або вогню і зупинити поширення пожежі; оперативне поінформувати працівників, які перебувають у небезпечній зоні на території електростанції, для їх швидкої евакуації; визначати точні осередки і причини виникнення диму і вогню. Таким чином, можна забезпечувати збереження життя і здоров'я працівників, мінімізувати матеріальні збитки.

Детектор гучного звуку. Допомагає оперативне реагувати на форс-мажорні ситуації на території об'єкта, супроводжувані гучними звуками (постріли, вибухи). Ця функція дозволяє налаштувати рівень звуку, перевищення якого буде свідчити про виникнення форс-мажорній ситуації. Якщо рівень звуку перевищить заданий рівень, то генерується негайне повідомлення на монітор, смартфон або на електронну пошту. Крім цього, автоматично почнеться запис відео (Рис.11).

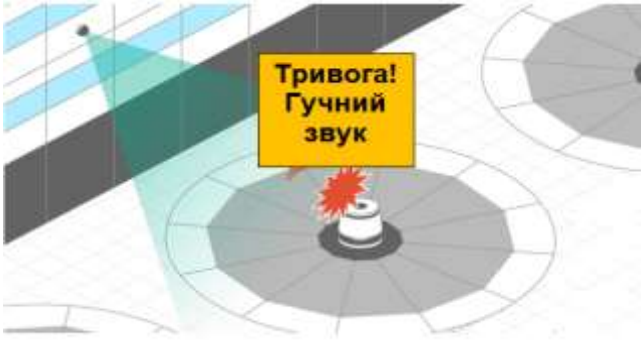

Рис. 11 - Детектор гучного звуку

Завдяки «Детектор гучного звуку» можна ідентифікувати джерело небезпеки. Таким чином, можна забезпечувати безпеку працівників, а також мінімізувати збиток майну, інфраструктурі.

Детектор саботажу. Допомагає скорочувати час простою системи відеоспостереження внаслідок непрацездатності камер системи відеоспостереження. Ця функція дозволяє налаштовувати в програмі наступні контрольні події (Рис.12): розфокусовці камери; відхилення камери від заданого положення; тривалий засвіти огляду камери; перекриття поля спостереження камери.

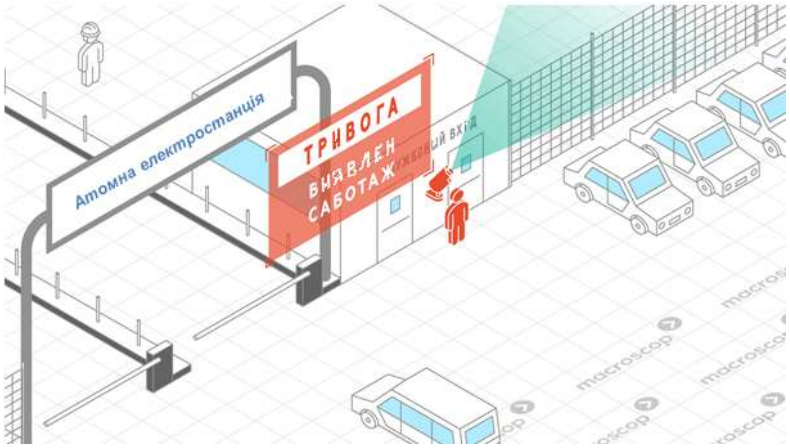

Рис. 12 - Детектор гучного звуку

Завдяки «Детектор саботажу» можна отримувати інформацію про непрацездатність системи відеоспостереження та оперативне її відновлювати. Коли виникає будь-яка з вказаних подій, відправляється негайне повідомлення на монітор, смартфон або на електронну пошту. Таким чином, ви можете безперервно забезпечувати безпеку працівників, а також майна, інфраструктури електростанції.

Висновки

Дослідження систем відеоспостереження за допомогою кібернетичного підходу дозволяє визначити особливості побудови кібернетичних систем відеоспостереження для забезпечення безпеки об'єктів підприємства критичної інфраструктури, а саме: головною відмінністю кібернетичних систем відеоспостереження від звичайних є здатність аналізувати дані про поточний стан об'єктів відносно попереднього або початкового стану об'єкта, що спостерігається, і який прийняти за еталон.

Кібернетичні системи відеоспостереження повинні виконувати наступний перелік функцій: 1) Організувати автоматизований контроль доступу автомобілів на територію об'єкта, що спостерігається; 2) Організувати автоматизований контроль доступу людей в приміщення об'єкта, що спостерігається; 3) Забезпечувати безперервну відео трансляцію і запис незважаючи на форс-мажорні ситуації; 4) Створювати покрити більшу зону спостереження об'єкта меншою кількістю камер; 5) Скоротити вартість системи відеоспостереження об'єкта; 6) Отримувати негайні повідомлення на монітор, смартфон або електронну пошту; 7) Виконувати автоматично відео аналітику щодо: розпізнавання автономерів, розпізнавання осіб; резервування каналу з відображенням; управління PTZ-камерами; розгортці fisheye-камер: контролю активності персоналу; трекінгу; виявлення осіб; відсутності заданих засобів захисту на особі; появи диму і вогню; появи гучного звуку та ознак саботажу.

Список використаної літератури

1. How-To: Python Compare Two Images – [Електронний ресурс] – 2018 – Режим доступу: https://www.pyimagesearch.com/2014/09/15/python-compare-two-images/ – Дата доступу: жовтень 2018.

2. MAE and RMSE — Which Metric is Better? – [Електронний ресурс] – 2018 – Режим доступу: https://medium.com/human-in-a-machine-world/mae-and-rmse-which-metric-is-better-e60ac3bde13d – Дата доступу: жовтень 2018.

3. Z. Wang, A. C. Bovik, H. R. Sheikh and E. P. Simoncelli. Image quality assessment: From error visibility to structural similarity // IEEE Transactions on Image Processing – 2004.

4. Skimage 0.14.1 docs– [Електронний ресурс] – 2018 – Режим доступу: http://scikit-image.org/docs/stable/ – Дата доступу: жовтень 2018.

5. Лутц Марк, Изучаем Python, 4-е издание. – Пер. с англ. – СПб.: Символ-Плюс, 2011. – 1280 с., ил..

6. Модуль tkinter. Создание графического интерфейса пользователя с помощью языка программирования Python – [Електронний ресурс] – 2018 – Режим доступу: http://kabinet-vplaksina.narod.ru /olderfiles/5/Modul_tkinter.pdf– Дата доступу: жовтень 2018.

7. Як працюють системи відеоспостереження – [Електронний ресурс] – 2018 – Режим доступу: http://www.atlant-holding.com.ua/ua/news/64-yak-pracyuyut-sistemi-videosposterezhennya – Дата доступу: жовтень 2018.

8. Системи аналогового відеоспостереження – [Електронний ресурс] – 2018 – Режим доступу: http://www.bsi-group.com.ua/ua/systems-security/view/Video_analog– Дата доступу: жовтень 2018.

9. Аналогові або цифрові камери відеоспостереження: на чому зупинитися? – [Електронний ресурс] – 2018 – Режим доступу: http://dovidkam.com/tehnika/analogovi-abo-cifrovi-kameri-videosposterezhennya-na-chomu-zupinitisya.html– Дата доступу: жовтень 2018.

10. IP відеоспостереження – [Електронний ресурс] – 2018 – Режим доступу: https://xn--80adgeboqrpy5j.com.ua/ip_videosposterejennya/ – Дата доступу: жовтень 2018.

11. Системи IP-відеоспостереження. Огляд – [Електронний ресурс] – 2018 – Режим доступу: https://valtek.com.ua/ua/system-integration/security-control-system/video-surveillance/ip-systems-review– Дата доступу: жовтень 2018.

12. Цифрові системи відеоспостереження – [Електронний ресурс] – 2018 – Режим доступу: https://www.vostok.dp.ua/ukr/infa1/sistemy_vidyeonab-lyudeniya/digital-video/ – Дата доступу: жовтень 2018.

13. Переваги відеоспостереження HD CCTV, HD-SDI– [Електронний ресурс] – 2018 – Режим доступу: https://xn--80adgeboqrpy5j.com.ua/perevagu_hd/ – Дата доступу: жовтень 2018.

14. Системи відеонагляду. Відмінність цифрової і аналогової системи відеоспостереження– [Електронний ресурс] – 2018 – Режим доступу: http://www.ohrana-ua.com/articles/801-sistemi-vdeonaglyadu-vdmnnst-cifrovoyi-analogovoyi-sistemi-vdeosposterezhennya.html – Дата доступу: жовтень 2018.

15. Системи безпеки для будинку – [Електронний ресурс] – 2018 – Режим доступу: http://kristall-systems.net.ua/ua/resheniya /security_systems_for_home/ – Дата доступу: жовтень 2018.

16. OpenCV documentation index – [Електронний ресурс] – 2018 – Режим доступу: https://docs.opencv.org/– Дата доступу: жовтень 2018.

17. 3.3. Scikit-image: image processing– [Електронний ресурс] – 2018 – Режим доступу: https://www.scipy-lectures.org/packages/scikit-image/index.html– Дата доступу: жовтень 2018.

18. Getting started with Scikit-image: image processing in Python– [Електронний ресурс] – 2018 – Режим доступу: https://www.geeksforgeeks.org/getting-started-scikit-image-image-processing-python/– Дата доступу: жовтень 2018.

Автори статті

Катков Юрій Ігорович – кандидат технічних наук, доцент, доцент кафедри комп'ютерних наук, Державний університет телекомунікацій, Київ, Україна.

Сєрих Сергій Олександрович – кандидат технічних наук, доцент кафедри Комп'ютерних наук, Державний університет телекомунікацій, Київ, Україна.

Шашлов Андрій Вікторович – бакалавр по напрямку Інформаційні технології і студент магістратури, Державного університету телекомунікацій, Київ, Україна.

Вергун Дмитро Сергійович - бакалавр по напрямку Інформаційні технології і студент магістратури, Державного університету телекомунікацій, Київ, Україна.

Authors of the article

Katkov Yuriy Igorovich – candidate of Science (technic), associate professor, associate professor Department of Computer Science, State University of Telecommunications, Kyiv, Ukraine.

Sierykh Sergiy Aleksandrovich - candidate of Science (technic), Associate Professor, Department of Computer Science, State University of Telecommunications, Kyiv, Ukraine.

Shashlov Andrii Viktorovich - student, State University of Telecommunications, Kyiv, Ukraine.

Verhun Dmytro Sergiyovich - student, State University of Telecommunications, Kyiv, Ukraine.

Дата надходження в редакцію: 29.07.2019 р. Рецензент: д.т.н., с.н.с. М.П. Трембовецький