

На правах рукопису

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Одеська національна академія харчових технологій
Навчально-науковий інститут холоду,
кріотехнологій та екоенергетики
Факультет інформаційних технологій та кібербезпеки

**XVII Всеукраїнська науково-технічна конференція
молодих вчених, аспірантів та студентів**

**“СТАН, ДОСЯГНЕННЯ І ПЕРСПЕКТИВИ
ІНФОРМАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ”**

Матеріали конференції. Частина 2



Одеса
19 квітня 2017 р.

Стан, досягнення і перспективи інформаційних систем і технологій / Матеріали XVII Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Одеса, 19 квітня 2017 р. - Одеса, Видавництво ОНАХТ, 2017 р. - 80 с.

Збірник включає матеріали доповідей її учасників, які об'єднані по секціях кафедр: комп'ютерної інженерії (КІ), інформаційних технологій та кібербезпеки (ІТтаКБ).

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Голова – д.т.н., проф., **Єгоров Б.В.**, ректор ОНАХТ.

Співголови :

Поварова Н.М. – к.т.н., доц., проректор з наукової роботи,
Косой Б.В. – д.т.н., проф., в.о. директора ННІХКтаЕ ОНАХТ,
Котлик С.В. – к.т.н., доц., декан ФІТта КБ ОНАХТ,
Волков В.Е. – д.т.н., проф., директор НМАіР ОНАХТ,
Хобін В.А. – д.т.н., проф., завідувач кафедри АВП ОНАХТ,
Невлюдов І.Ш. – д.т.н., проф., завідувач кафедри КІАтаМ ХНУРЕ,
Мельник А.О. – д.т.н., проф., завідувач кафедри ЕОМ НУ “Львівська політехніка”,
Тарасенко В. П. – д.т.н., проф., завідувач кафедри СКС НТУУ «Київський політехнічний інститут»,
Жуков І. А. – д.т.н., проф., завідувач кафедри КСтаМ НАУ,
Сулімова Ю. – координатор IT–Cluster Odessa.

Члени оргкомітету:

Плотніков В. М. – д.т.н., проф., завідувач кафедри інформаційних технологій та кібербезпеки ОНАХТ,
Артеменко С.В. – д.т.н., проф., в.о. завідувача кафедри комп'ютерної інженерії ОНАХТ,
Князєва Н.О. – д.т.н., проф. кафедри комп'ютерної інженерії ОНАХТ,
Бойцова О.С. – заступник декана ФІТта КБ ОНАХТ,
Шамрай О.А. – к.т.н., доц. кафедри ТДтаВЕ ОНАХТ.

Матеріали подано українською, російською та англійською мовами.
Редактор збірника Шамрай О.А.

2. Додонов О.Г. Живучість інформаційних систем. [Текст] / А.Г. Додонов, Д.В. Ланде – К.: Наук. думка, 2011. – 256 с. – ISBN 978-966-00-0973-9
3. Князева Н.О. Метод забезпечення структурної живучості телекомунікаційної мережі [Текст] / Н.О. Князева. – International Journal Information technologies and knowledge. – 2014 p., С. 152-165.

ОБЛАЧНЫЕ ТЕХНОЛОГИИ В СИСТЕМАХ ВИДЕОНАБЛЮДЕНИЯ

Иовчев И.П., студент группы 541, ОНАПТ

Руководитель: ассистент каф. КИ Монахова К.И.

Сегодня уже невозможно представить себе жизнь без современных технологий, включающих в себя, в том числе, и системы видеонаблюдения. Эта область техники развивается настолько стремительно, что разговоры о преимуществах цифрового видеонаблюдения над аналоговым уходят в прошлое. В последнее время приобрёл популярность новый сервис – облачное видеонаблюдение.

Облачное видеонаблюдение – это интернет-сервис, который позволяет хранить, просматривать и сохранять видеозаписи с видеокамеры, установленной у пользователя благодаря подключению через интернет к серверам, хранящим данные. А так же, облачное видеонаблюдение – это возможность подключения неограниченного количества пользователей к неограниченному количеству устройств в любой точке планеты.

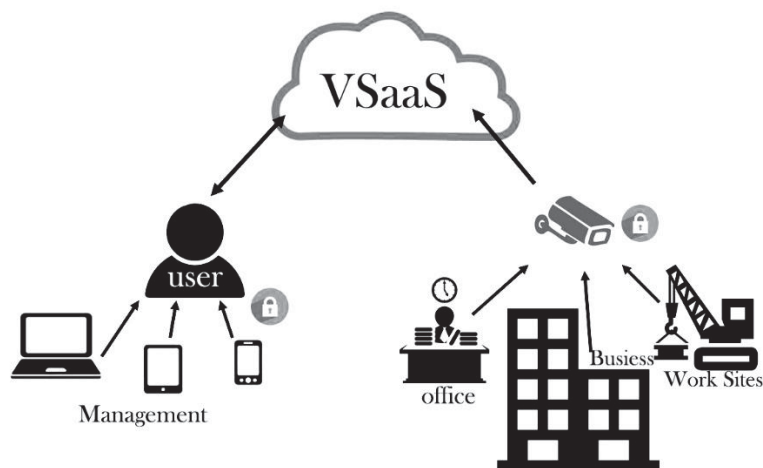


Рисунок 1 – Структурная схема облачного видеонаблюдения

В системах видеонаблюдения существует 2 основных типа облачных адресов:

- Облачный сервис без возможности хранения данных;
- Облачный сервис с возможностью хранения данных;

Облачный сервис без возможности хранения данных, предоставляется на безвозмездной основе производителем оборудования и не требует сложной настройки. Для его использования достаточно всего лишь приобрести определён-

ное видеооборудование, обеспечить ему выход в интернет и установить на устройство просмотра необходимое программное обеспечение.

Особенностями данного типа, являются:

- простота подключения;
- автономная система с поддержкой подключения через облако;
- поддержка работы с видеорегистраторами и IP камерами;
- удаленный доступ к архиву системы;
- возможность удаленного управления системой;
- возможность вести онлайн запись на ПК или КПК;
- нет возможности хранения в облаке.

Облачный сервис второго типа, представляет возможность хранения данных на удаленном сервере, тем самым исключая необходимость в локальном устройстве хранения, а так же обеспечивает повышенную защиту от злоумышленников.

Особенностями данного тип, являются:

- возможность хранения данных (высокая надежность хранения данных);
- простота подключения;
- дополнительные возможности (аналитика, уведомления, публичная трансляция) [1].

Несмотря на все преимущества, у облачного видеонаблюдения есть свои недостатки. К ним можно отнести внесение абонентской платы за пользование услугами облачного хранилища, скорость интернета, кодировка изображения, способы хранения данных. Ведь именно от этих факторов зависит хорошая работоспособность системы видеонаблюдения.

Облачные технологии имеют и такой параметр ненадёжности, как уязвимость Интернет-соединения, возможность сбоев в сети. Плохое интернет-соединение непременно плохо влияет на удалённый доступ к камере и к файлам, которые находятся в «облаке». Кроме того, это соединение обеспечивает провайдер услуг связи, а значит, в отношения между поставщиком услуг видеонаблюдения и клиентом вмешивается третья сторона, что также делает систему безопасности менее надёжной.

В системах видеонаблюдения используются множество форматов сжатия изображения: *MJPEG (Motion JPEG)*, *H.264*, *MPEG4*. Каждый из данных форматов имеет свои «плюсы», но на данный момент популярным является – *H.264*.

H.264 – хорошо сжимает видео без ущерба для его качества, слабо нагружает сеть и подходит для больших объемов видео. Недостатком данного кодировщика является то, что от центрального процессора требуется достаточное количество ресурсов [2].

Современные облачные системы наблюдения постоянно модернизируются и оснащаются разнообразными функциями, что позволяет максимально удобно использовать возможности оборудования.

Таким образом, системы видеонаблюдения, которые используют облачные технологии, несмотря на выделенные недостатки, являются гибкими, удобными, простыми в развертывании и обслуживании, современным решением для построения системы безопасности предприятия и других объектов.

Список литературы

1. Облачные системы видеонаблюдения [Электронный ресурс]. – Режим доступа: <http://www.vsaas.com/> - Название с экрана.
2. *Video Surveillance as a Service* [Электронный ресурс]. – Режим доступа: <http://www.iwnetworks.com/main/video-surveillance-service> - - Название с экрана.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПРОТОКОЛОВ МАРШРУТИЗАЦИИ В AD-HOC СЕТЯХ

Казак Ю.С., аспирантка кафедры Компьютерная инженерия ОНАПТ

В настоящее время сети передачи данных продолжают активно развиваться, в том числе все большее распространение получает такой их класс, как сети Ad-hoc. Это одноранговые беспроводные сети передачи данных с переменной топологией и отсутствием четкой инфраструктуры, где каждый узел может выполнять функции маршрутизатора и принимать участие в ретрансляции пакетов данных. Подобные сети могут применяться во время военных действий, в структурах МЧС, в системах транспорта и различных силовых структурах [4].

За счет постоянного изменения структуры сети могут возникнуть проблемы с маршрутизацией, так как изменяются возможные пути доставки информации между узлами. Существующие на данный момент протоколы маршрутизации можно классифицировать следующим образом [1-6].

По типу используемых для маршрутизации данных: топологические и географические.

По принципу работы: проактивные или табличные (англ. proactive, table-driven), реактивные или работающие по запросу (англ. reactive, on-demand), гибридные (англ. hybrid).

По критерию определения оптимальности маршрута: протоколы вектора расстояния (англ. distance-vector, hop-count), протоколы со сложной метрикой маршрутов или протоколы состояния каналов (англ. link-state).

По наличию поддержки нескольких маршрутов до одного адресата: однопутевые (англ. single-path) и многопутевые (англ. multi-path).

Данная классификация, в общем, отражает основные подходы, которые сложились к настоящему времени при анализе проблемы маршрутизации в самоорганизующихся сетях [6]. В существующих работах [1-6] выявлены некоторые существенные характеристики, влияющие на выбор протокола маршрути-