Гаджимагомедов Шарухан Гаджимагомедович

студент

ФГБОУ ВО «Донской государственный технический университет»

г. Ростов-на-Дону, Ростовская область

ИСПОЛЬЗОВАНИЕ СИСТЕМ ВИДЕОНАБЛЮДЕНИЯ И ИХ ПЕРСПЕКТИВЫ: ПОЛЬЗА ЭКОНОМИКЕ

Аннотация: *в статье рассмотрен вопрос использования систем видеонаблюдения, перспективы их использования, и роль, которую они выполняют.*

Ключевые слова*: система видеонаблюдения, безопасность, конфиденциальность, функции систем видеонаблюдения.*

Видеонаблюдение – это очень важная система, обеспечивающая безопасность. Очень много преступлений сейчас раскрывается с помощью системы видеонаблюдения.

Прямое видеонаблюдение беспрерывно осуществляется. Оператор в это время сидит и наблюдает все картины с монитора. Эффективность такого видеонаблюдения зависит от следующих факторов:

1) ответственная работа оператора, его заинтересованность в работе;

2) психологическое и физиологическое состояние оператора;

3) число камер. Рекомендуется использовать не более 4 шт.

4) качество фотографий.

Прямое видеонаблюдение эффективно только в том случае, если оператор внимательно и ответственно выполняет свою работу.

В настоящее время системы видеонаблюдения имеют огромный спрос и быстро распространяются. Они устанавливаются для безопасности и порядка. Современные видеокамеры обладают специальными программами, которые могут распознать лица. Даже во время пандемии COVID-19, когда люди носили маски, процент распознавания лиц оставался высоким. Он составлял 98%.

Системы видеонаблюдения важны тем, что они помогают вычислить нарушения правил дорожного движения, поведение и даже настроение людей [4].

Системы видеонаблюдения помогают распознавать лица и особенности тела преступников. С изобретением систем видеонаблюдения совершить преступление и не быть пойманным стало практически невозможно.

Как же мы можем избежать того, чтобы наблюдатели не злоупотребляли наблюдением?

Каждого человека можно отслеживать на регулярной основе. Более того, анализ информации в этом случае может привести к утечке информации о личных данных, касающихся места жительства, работы и учебы, проблем со здоровьем и т. д.

Даже если мы доверяем правоохранительным органам защиту нашей личной информации, все равно есть наблюдатели, которые могут злоупотреблять своими полномочиями.

Специальных протоколов сохранения конфиденциальности, которые созданы для защиты личной информации от утечки, недостаточно.

Таким образом, существует два способа решения проблемы:

1) ограничьте время и местоположение доступа к камерам;

2) ограничьте то, что можно увидеть в отдельных кадрах [1].

В первом случае, например, наблюдатель может иметь доступ только к тем камерам, которые установлены в радиусе километра в пределах его местоположения, или может получить доступ к камерам только в свое официальное рабочее время.

Во втором поле зрения ограничено на основе высокоуровневой семантической информации, полученной из содержимого видеопотока, таким образом, наблюдатель не будет иметь неограниченного доступа к данным, поскольку он сможет просматривать только данные, аналогичные семантическому содержанию того, что ему разрешили смотреть.

Второй случай является более гибким и подходящим для наблюдателя по сравнению с первым, имеющим дело с физическим контекстом. Тем не менее, наблюдатель может видеть дополнительную информацию. Например, полицейский может посмотреть записи, на которых какая-то машина ускорилась. В этом случае его интересует только регистрационный номер автомобиля, однако он может видеть всех людей в машине или близлежащие машины, в то время как только один из них нарушает закон [2].

Эти два подхода не исключают друг друга и могут использоваться вместе как своего рода гибрид.

Кроме того, мы не должны забывать о хакерах. Они могут взломать облако или получить доступ к камерам и их аналитической системе. Более того, что, если они взломают систему анализа и используют синтетические носители, чтобы поменять лицо человека, совершающего преступление?

В настоящее время эти программы несовершенны, и квалифицированный ИТ-специалист может обнаружить подобные манипуляции, но технологии развиваются, и это вызывает серьезную озабоченность по поводу подделки доказательств в будущем.

Учитывая все связанные с этим риски, я думаю, что системы наблюдения стоят того, чтобы развиваться, расширяться, чтобы не оставлять слепых зон в городе. Это поможет снизить преступность и обезопасить граждан.

Рассмотрим классификацию систем видеонаблюдения. Систему видеонаблюдения разделяют на [3]:

1) аналоговые – видеонаблюдение в маленьких помещениях. Запись с камер сохраняются на видеомагнитофон. Такая система видеонаблюдения хороша простотой использования, качеством и ценой. Минусом этой системы видеонаблюдения является необходимость постоянного обновления запчастей;

2) цифровые – используются для контролирования особо больших территорий. Преимуществ у этой системы куча: долгое хранение наблюдений, легкая и простая передача информации, быстрый доступ к данным, повышение каче-

ства изображения. Минусом такой системы является достаточно высокая стоимость.

По назначению системы видеонаблюдения делятся на:

1) наружное видеонаблюдение;

2) внутреннее видеонаблюдение;

3) скрытое видеонаблюдение.

По расположению системы видеонаблюдения делятся на:

1) стационарные;

2) мобильные.

По методу передачи сигнала системы видеонаблюдения делятся на:

1) проводные;

2) беспроводные.

Из всего вышесказанного следует, что система видеонаблюдения играет очень важную роль в безопасности окружающих. Я считаю, что все эти системы должны постоянно развиваться и расширяться, потому что именно эти системы помогают в борьбе с преступностью и хулиганством.

Список литературы

1. Ворона В.А. Технические средства наблюдения в охране объектов / В.А. Ворона, В.А. Тихонов. – М.: Горячая линия – Телеком, 2010. – 184 с.

2. Торокин А.А. Инженерно-техническая защита информации: учеб. пособ. / А.А. Торокин. – М.: Гелиос АРВ, 2005. – 960 с.

3. Синилов В.Г. Системы охранной, пожарной и охранно-пожарной сигнализации: учебник для нач. проф. образования / В.Г. Синилов. – М.: Академия, 2010. – 512 с.

4. Дамьяновски В. Библия видеонаблюдения / Дамьяновски В. // Security Focus. – 2022 – С. 348–352.