Системы видеонаблюдения в нефтегазовом комплексе: Безопасность производственных структур и защита персональных данных

Шакир Мехтиев[1], Тахмасиб Фаталиев[2], Аяз Мехтиев[3]
[1,2,3]Институт информационных технологий, Баку, Азербайджан
[1,3]*depart11@iit.science.az*, [2]*depart3@iit.science.az*

***Аннотация*— Четвертая промышленная революция, или Industry 4.0 произвела кардинальные изменения в области критических систем, в том числе и в нефтегазовом комплексе. Нефтегазовому комплексу присущи обширная и дорогостоящая инфраструктура объектов для производства, хранения и доставки конечной продукции. Обеспечение безопасности этих объектов является сложной задачей, поскольку любые нарушения в цепочке технологических процессов, вызванные как техническими причинами, так и преднамеренными попытками причинить ущерб или кражей оборудования наносят значительный финансовый урон. Также возрастают риски для жизни и здоровья персонала этих предприятий и экологические риски для окружающей среды. Однако, решая общие проблемы безопасности и надежности, системы видеонаблюдения параллельно создают проблему защиты персональных данных, которые являются основополагающими факторами универсальных прав человека. В статье рассматриваются проблемы применения систем видеонаблюдения в нефтегазовом комплексе, реализуемом на основе концепции Industry 4.0 и предлагаются рекомендации по защите персональных данных.**

Ключевые слова— Industry 4.0; нефтегазовый комплекс; риски; видеонаблюдение; персональные данные

I. Введение

Целью четвертой промышленной революции Industry 4.0. является достижение более высокого уровня операционной эффективности и производительности, а также автоматизации [1]. Системы видеонаблюдения и обработки изображений, используемые в различных отраслях промышленности, становятся одним из компонентов подобного автоматизированного производства. На всех этапах производства, от инспекции сырья, мониторинга производства, обнаружения дефектов и обеспечения качества и стандартов, эти системы помогают достичь высокой экономической эффективности. Это стало возможным благодаря новым видеосенсорам, наноматериалам и таким технологиям, как киберфизические системы, интернет вещей, искусственный интеллект и др. Технически новые интеллектуальные системы видеонаблюдения регистрируют активность и рабочее состояние, результаты проверок, предлагают интеллектуальные решения по преодолению трудностей и передают их в виде информации персоналу на очки дополненной реальности (например, Microsoft Hololens).

Следует отметить, что системы видеонаблюдения широко используются для защиты критических инфраструктур. Под защитой критической инфраструктуры понимаются меры по обеспечению безопасности взаимозависимых систем, сетей и активов, лежащих в основе служб, жизненно необходимых для функционирования общества. Нефтегазовый комплекс (НГК) также относится к подобным критическим инфраструктурам. Нефть и газ по-прежнему являются наиболее важными источниками энергии, прямо или косвенно, обеспечивают занятость большому количеству людей и вносят значительный вклад в государственный бюджет. Перебои с поставками нефти и газа негативно проявляются и в транспортной сфере, создавая неудобства и трудности людям в их ежедневной деятельности.

Принимая во внимание риски и проблемы обеспечения защиты персонала, дорогостоящей инфраструктуры и производственных процессов, задачи, решаемые системами видеонаблюдения в НГК, весьма актуальны. Однако, решая общие проблемы безопасности и надежности, системы видеонаблюдения параллельно создают проблему защиты персональных данных (ПД), которые являются основополагающими факторами универсальных прав человека.

II. Краткие Сведения о Системах Видеонаблюдения

Видеонаблюдение (Video surveillance) — это технологическая система, состоящая из множества видеокамер, которые подключены к замкнутому контуру телевидения (closed circuit television, CCTV). Первоначально изображения с видеокамер отправлялись в мониторинговый центр, где оператор перед экраном осуществлял непрерывный контроль за происходящими событиями без возможности их анализа в будущем. Это было существенным недостатком подобных систем. Появившиеся в середине XX в. видеомагнитофоны смогли

DOI: 10.25045/NCInfoSec.2019.22

решить эту проблему. Операторам более не требовалось проводить все время перед экраном монитора, вся информация записывалась на магнитную пленку. Однако, из-за чрезвычайно высокой стоимости первые видеомагнитофоны не нашли широкого распространения в системах видеонаблюдения. Ситуация существенно изменилась в 1970-х гг., когда были представлены видеокассеты формата Video Home System (VHS) [2]. Популярность видеосистем стала расти, и ими оснащались в первую очередь вокзалы, аэропорты, банки, магазины, автозаправки и другие объекты, в наибольшей степени подверженные воздействию внешних угроз. Дальнейший прогресс систем видеонаблюдения связан с появлением интернета, цифровых камер с высоким разрешением, облачных хранилищ, искусственного интеллекта и т.п.

В настоящее время системы видеонаблюдения стали реальностью современного общества. По аналогии с концепцией Industry 4.0 можно предположить, что сейчас эти системы вступили в эру Video Survielance 4.0. По некоторым данным только в Лондоне установлено 500000 видеокамер, а средний человек, живущий в Лондоне, будет записан на камеру 300 раз за один день [3]. Подобная тенденция роста систем видеонаблюдения и количества видеокамер характерна для США, Китая, Японии и большинства стран. Трудно представить объемы информации, записанной камерами наблюдения в общественных местах, или перехвата видеочатов через Интернет (Skype, WhatsApp, Viber и др.).

Отметим, что при сравнении обычного наблюдения с видеонаблюдением последнее имеет ряд преимуществ:

- архивация изображений и возможность последующего их анализа;
- ночное видение;
- масштабирование;
- автоматическое слежение;
- обнаружение деталей и признаков, невидимых человеческим глазом;
- интеллектуальное распознавание лица и голоса человека, вплоть до его эмоционального состояния;
- доступность видеоархива через интернет из любой точки мира.

В то же самое время видеонаблюдение в общественных местах затрагивает такую сенситивную сферу, как ограничения в передвижении, право на частную жизнь, вопросы идентификации личности и, в целом, ПД.

III. Системы Видеонаблюдения как Составная Часть Безопасности Нефтегазового Комплекса

Известно, что технологические процессы в структуре НГК выполняются последовательно в трех секторах, которые обычно называют *Upstream, Midstream и Downstream* [4]. Эти три сектора охватывают сферы добычи нефти и газа от морских разведочных и буровых платформ до береговых нефтяных скважин, транспортировку сырья посредством трубопроводов до нефтеперерабатывающих заводов, переработку сырья в конечный продукт и его доставку потребителям. Подобная многогранная деятельность создает множество проблем общей безопасности. Как правило, участки нефтегазовых месторождений охватывают огромные территории, могут быть расположены в труднодоступных местах на суше или в открытом море и часто подвержены неблагоприятным условиям окружающей среды. Эти объекты имеют много ключевых областей, которые могут стать целями для проникновения посторонних лиц. Результатом таких действий могут стать акты саботажа, умышленной порчи технического оборудования, кражи или, в худшем случае, диверсии или террористического акта. Поэтому функционирование большинства объектов НГК требует постоянного мониторинга и дистанционного контроля, так как любое небольшое нарушение в работе каждого объекта может привести к сбою всей системы в целом и, как следствие, к экономическим и даже человеческим потерям и экологическим катастрофам. Поэтому уровень безопасности должен быть максимальным. В то же время, безопасность приходится обеспечивать на технически сложных и больших (например, нефтеперерабатывающие предприятия) и протяженных (нефтепроводах) объектах. Распределенная архитектура идеально подходит для обеспечения безопасности на крупных и протяженных объектах, а ее универсальность позволяет решать весь спектр задач обеспечения безопасности, связанных с деятельностью НГК. При этом из единого центра мониторинга можно контролировать все объекты, вплоть до самых удаленных. Комплексная система безопасности способна объединить видеонаблюдение, охранно-пожарную сигнализацию, систему охраны периметра, систему контроля и управления доступом, аудио контроль в согласованно работающую инфраструктуру. Благодаря этому комплекс различных систем безопасности превращается в единую информационную среду, в которой можно реализовать функции обработки и интеллектуального анализа информации, обладающую способностью гибко реагировать на различные события. Как показывает опыт эксплуатации систем видеонаблюдения существуют множество эффективных решений подобных систем для НГК. Рассмотрим некоторые реализованные из них.

A. Система видеонаблюдения на офшорном месторождении

В [5] приведена система видеонаблюдения для офшорного месторождения с охватом более 300 буровых установок для разведки и добычи на море. Система контролирует буровые площадки, посадочную площадку для вертолетов, оснащена специализированными подводными камерами. Система способна идентифицировать задымления, разливы нефти, нежелательные движения на буровой площадке, производится автоматическая запись и хранение событий. Также возможен общий мониторинг процесса и дополнительный удаленный (на суше) доступ к прямой трансляции.

Б. Система видеонаблюдения нефтеперерабатывающего завода

Здесь эта система осуществляет общий мониторинг и предназначена для обнаружения и упреждения

подозрительных событий, неисправностей, аварий и краж. В дополнение к этому специализированные камеры способны непрерывно отслеживать производственные процессы во взрывоопасных, токсичных и высокотемпературных средах, где пребывание персонала невозможно. Возможности тепловизорных камер позволяют контролировать изменения температуры, осуществлять интеллектуальную аналитику, и, благодаря интеграции с системами пожарной и газовой сигнализации, можно заблаговременно предпринять упреждающие меры безопасности. В целом концепция Industry 4.0 на подобных предприятиях (например, система управления TDC 3000 компании Honeywell) позволила повысить производительность почти в 10 раз [6].

B. Мониторинг трубопроводов

Стандартные подходы к мониторингу нефте- и газопроводов дополняются видеонаблюдением с дронов. Сигналы с датчиков наблюдения и обнаружения утечек используются для идентификации текущего состояния трубопроводов и оценки экологической обстановки [7]. Система обнаружения утечек и дроны компании Asea Brown Boveri Ltd. обеспечивают точность до 3000 раз выше, чем у устаревших систем [6]. Качественные изображения в режиме реального времени позволяют оперативно обнаруживать нефтяные разливы и выявлять несанкционированную деятельность в охраняемых зонах.

Г. Техническое обслуживание

Существенный эффект может дать использование систем видеонаблюдения в техническом обслуживании. Так, например, известно, что интеллектуальные камеры Tattile могут быть подключены к большинству компонентов и систем, участвующих в процессе создания промышленной ценности, а также к сетям предприятия и интернету [8]. Вместо того, чтобы реагировать на обнаружение дефектов, интеллектуальные камеры стали инструментами анализа, которые используют статистические методы и методы обработки больших данных, чтобы получать информацию из изображений и применять их в масштабах всего предприятия.

Например, можно определить, когда какая-либо часть оборудования выйдет из строя до того, как обслуживающая бригада обнаружит проблему. Система распознает предупреждающие знаки, использует данные для создания графиков упреждающего обслуживания оборудования до возникновения проблемы. Изображения, записанные по частям, можно сравнить с тысячами других, хранящихся в облаке, чтобы определить корреляции и тенденции. В то же самое время для достижения большего эффекта видеонаблюдение может быть объединено с другой мониторинговой системой — беспроводной сенсорной сетью (Wireless Sensor Network, WSN). WSN помогает получать физическую информацию с объектов мониторинга: тепловые, химические, магнитные, вибрационные и другие характеристики [9]. Интеграция обеих технологий делает возможным создание интеллектуальной системы технического обслуживания.

Таким образом, рассмотренные примеры показывают, что системы видеонаблюдения играют существенную роль в обеспечении безопасности и надежности предприятий и процессов в НГК.

IV. Конфиденциальность и Защита Персональных Данных в Системах Видеонаблюдения

Согласно Общим положениям о защите данных (General Data Protection Regulation, GDPR) к ПД можно отнести любую информацию, относящуюся к идентифицированному или идентифицируемому физическому лицу [10]. Любые операции, выполняемые с ПД или с наборами ПД, независимо от того, выполняются ли они автоматическими средствами, такими как сбор, запись, организация, структурирование, хранение, адаптация или изменение, поиск, консультация, использование, раскрытие путем передачи, распространение или иное предоставление, выравнивание или комбинация, ограничение, удаление или уничтожение– квалифицируются, как обработка ПД. Таким образом, очевидно, что проблемы с ПД могут возникать во всех сферах деятельности и во всех аспектах жизни в целом, поскольку информацию, с помощью которой можно идентифицировать физическое лицо, можно найти практически везде, в том числе и в системах видеонаблюдения. Следует принять во внимание, что использование системы видеонаблюдения на предприятии влечет за собой обработку ПД в том случае, если лицо можно опознать.

Видеокамеры сегодня моментально устанавливают личность человека, его пол и возраст. Был разработан алгоритм с применением нейросетей для повышения общественной безопасности и выявления преступников, который уже активно применяется и в бизнесе. Технология распознавания лиц вошла в национальный стандарт России «Smart city» [11].

Следует отметить, что идентификация личности возможна и по его другим признакам, например, форма тела, одежда, имеющиеся при себе вещи и т.д. Факт видеосъемки работника на рабочем месте уже есть обработка ПД. Однако, априори такие ПД работника являются конфиденциальной информацией, поскольку это информация о физическом лице, и их обработка без согласия соответствующего лица не допускается, кроме случаев, четко определенных законом [12].

С практической позиции, очевидно, что во избежание лишних недоразумений между работодателем и работником должно быть составлено письменное согласие на обработку ПД. Как альтернативный можно будет рассмотреть вариант, когда в помещении ведется открытая видеосъемка и установлены на видном месте предупредительные таблички о видеонаблюдении (тогда можно говорить о молчаливом согласии).

Аналогичные угрозы ПД возникают и при использовании дронов в целях мониторинга инфраструктуры НГК, топографических съемок и экологической инспекции местности. В этом случае проводимые операции создают риски непреднамеренной

обработки ПД. Так, например, может произойти захват изображений людей на заднем плане. Здесь под задним планом понимаются близлежащие места жительства, зоны отдыха, транспортные средства и т. д. Следует отметить, что в июле 2019 года Европейский совет по защите данных (The European Data Protection Board, EDPB) принял проект Руководства по обработке ПД с помощью видеоустройств (Guidelines on processing personal data through video devices) [13]. В нем указано, что видеозапись отдельного лица сама по себе не может рассматриваться как биометрические данные, если она не была специально и технически обработана для содействия идентификации личности (т.е. для распознавания лиц). Обработка биометрических данных представляет собой проблему, если отдельные лица не согласились на получение своих биометрических данных и представлены в отснятом материале.

Еще одна опасность утечки информации может произойти из-за того, что дроны собирают информацию одним из двух способов: записи хранятся на борту (например, на карте памяти или жестком диске) либо передаются обратно на центральное устройство, где они затем сохраняются. Оба метода имеют уязвимости. Если дрон с бортовым хранилищем данных будет потерян или захвачен несанкционированным третьим лицом, то же самое будет и с информацией, которую он несет. Если дрон передает информацию через беспроводное соединение, это соединение можно перехватить и использовать для доступа или изменения информации при передаче. Для устранения этих уязвимостей следует использовать адекватные меры защиты, такие как защита паролем и шифрование.

Таким образом, можно отметить, что системы видеонаблюдения представляют угрозу для ПД. Поэтому при реализации этих систем наряду с основными требованиями следует учесть и приведенные выше рекомендации по защите ПД.

Заключение

Системы видеонаблюдения, интегрированные с другими системами безопасности и разработанные с использованием высококачественных и надежных средств, могут снизить риски в потенциально критических областях, в том числе и в НГК. Возросшие потоки ПД сделали актуальной защиту сенситивной информации в них, в решении которой должны быть задействованы как программно-технические средства, так и нормативно-правовые документы. При осуществлении видеонаблюдения должны быть приняты меры, рекомендованные ЕС и законами страны.

Благодарности

Данная работа выполнена при финансовой поддержке Фонда науки Государственной нефтяной компании Азербайджана SOCAR- **Контракт № 03 LR-AMEA.**

Литература

[1] Y. Lu, “Industry 4.0: A survey on technologies, applications and open research issues,” Journal of Industrial Information Integration, no. 6, pp. 1-10, 2017.

[2] Y. Shiraishi, “History of Home Videotape Recorder Development,” SMPTE Journal, vol. 94, no. 12, pp. 1257-1263, dec. 1985.

[3] How many CCTV cameras in London? 2017/10/16. https://www.caughtoncamera.net/news/how-many-cctv-cameras-in-london/

[4] R. M. Alguliyev, T. Kh. Fataliyev, Sh. A. Mehdiyev, “The industrial internet of things: the evolution of automation in the oil and gas complex,” SOCAR Proceedings, no. 2, pp. 66-71, 2019.

[5] IP CCTV Solutions. https://www.rolloos.com/media/2224/201702-rolloos-campro-ip-cctv-solutions.pdf.

[6] G. Sharma, “How Industry 4.0 is Reshaping Oil and Gas Recruitment”. 2019/02/19. https://www.rigzone.com/news/how_industry_40_is_reshaping_oil_and_gas_recruitment-19-feb-2019-158187-article/

[7] Ш. Мехтиев, А. Мехтиев, “Некоторые вопросы безопасности применения дронов,” 4-я Республиканская конференция по информационной безопасности, сс. 91-94, 2018.

[8] The Kepler I is the new range of Tattile smart cameras based on embedded artificial intelligence (AI). https://www.tattile.com/vision-solutions/kepler/

[9] Р. Алгулиев, Т. Фаталиев, Б. Агаев и Т. Алиев, “Сенсорные сети: состояние, решения и перспективы,” Телекоммуникации, № 4, сс. 27-33, 2007.

[10] General Data Protection Regulation (GDPR). https://gdpr-info.eu/.

[11] Под наблюдением умной камеры. https://rspectr.com/articles/497/pod-nablyudeniem-umnoj-kamery

[12] К. Сааре, Камеры на рабочих местах часто используются для неправильных целей. https://www.tooelu.ee/ru/Novosti&nID=2029

[13] GDPR Update — EDPB video surveillance guidelines. https://dentons.boekel.com/en/insights/alerts/2019/september/3/gdpr-update-edpb-video-surveillance-guidelines

VIDEO SURVEILLANCE SYSTEMS IN THE OIL AND GAS COMPLEX: INDUSTRIAL SAFETY AND PERSONAL DATA PROTECTION

Shakir Mehdiyev[1], Tahmasib Fataliyev[2], Ayaz Mehdiyev[3]

[1,2,3]Institute of Information Technology of ANAS, Baku, Azerbaijan

[1,3]depart11@iit.science.az, [2]depart3@iit.science.az

Abstract— The fourth industrial revolution, or Industry 4.0, made dramatic changes in the field of critical systems, including the oil and gas complex. The oil and gas complex has an extensive and expensive infrastructure of facilities for the production, storage and delivery of final products. Ensuring the safety of these facilities is a complex task, since any violations in the process chain caused by both technical reasons and deliberate attempts to cause damage or theft of equipment cause significant financial damage. The risks to the life and health of the personnel of these enterprises and the environmental risks to the environment also increase. However, solving common problems of security and reliability, video surveillance systems simultaneously create the problem of protecting personal data, which are fundamental factors of universal human rights. The article discusses the problems of using video surveillance systems in the oil and gas complex, implemented on the basis of the Industry 4.0 concept, and offers recommendations for protecting personal data.

Keywords— *Industry 4.0; oil and gas complex; risks; video surveillance; personal data*