- Угроза повышения привилегий.
- Угроза использования механизмов авторизации для повышения привилегий.
- Угроза доступа к защищаемым файлам с использованием обходного пути.
- Угроза использования информации идентификации/аутентификации, заданной по умолчанию.
- Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением.
- Угроза обхода некорректно настроенных механизмов аутентификации.
- Угроза подделки записей журнала регистрации событий.
- Угроза хищения аутентификационной информации из временных файлов cookie.

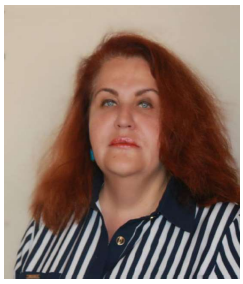
Полный перечень угроз перечислен в Банке данных угроз безопасности информации.

Вывод. Введение новых информационных технологий должно сопровождаться соответствующим развитием системы защиты информации от несанкционированного доступа. Обзор потенциальных каналов утечки информации, поможет разработчикам медицинской информационной системы учесть возможные угрозы и устранить их при планировании архитектуры МИС.

Список литературы:

1. ГОСТ Р ИСО/HL7 27932-2015 Информатизация здоровья. Стандарты обмена данными. Архитектура клинических документов HL7. Выпуск 2, Стандартинформ (Последняя редакция 2016 г.)
2. Матео Меуччи Руководство по тестированию OWASP // Цикл статей – 2015 г. – Вып.4, - 349 с.
3. Thomas Erl, Benjamin Carlyle, Cesare Pautasso, Raj Balasubramanian SOA with REST v. 5.1. — Prentice Hall, 2013. — 624 p. — ISBN 978-0-13-701251-0
4. Банк данных угроз информационной безопасности Федеральной службы по техническому и экспортному контролю // Угрозы [Электронный ресурс] Режим доступа к ресурсу: https://bdu.fstec.ru/threat, свободный. (Дата обращения 05.01.2020).
5. Методические рекомендации по обеспечению функциональных возможностей медицинских информационных систем медицинских организаций (МИС МО) (утв. Министерством здравоохранения РФ 1 февраля 2016 г.)

ПРИМЕНЕНИЕ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ В СИСТЕМЕ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ГОСТИНИЧНЫХ ПРЕДПРИЯТИЙ



Авилова Наталья Леонидовна
Доктор исторических наук, заместитель заведующего кафедрой по научной работе ,профессор кафедры «Туризм и гостиничное дело» Института туризма, рекреации, реабилитации и фитнеса ФГБОУ ВО «Российский государственный университет физической культуры, спорта, молодёжи и туризма (ГЦОЛИФК)»

Аннотация: *в статье рассматриваются проблемы построения и развития эффективной системы обеспечения безопасности в сфере гостиничных услуг, применения современных средств безопасности в области оборудование систем видеонаблюдения и кибербезопасности.*

Ключевые слова: *средства безопасности, технические средства защиты, и физические средства защиты, конфиденциальная информация, кибербезопасность, системы видеонаблюдения.*

Abstract: *the article deals with the problems of construction and development of an effective security system in the field of hotel services, the use of modern security equipment in the field of video surveillance and cybersecurity.*

Keywords: *security means, technical means of protection, and physical means of protection, confidential information, cybersecurity, video surveillance systems.*

Применение современных средств безопасности, наряду с профессиональными и компетентными действиями сотрудников службы безопасности гостиниц позволяют обеспечить рост финансово-экономической результативности гостиничного предприятия и повышению удовлетворенности.

В современных условиях безопасность гостиничных предприятий, обеспечивается за счет технических и физических средств защиты, безубыточной деятельности предприятия, а также, неразглашения конфиденциальной информации предприятия и его клиентов, и сохранение имущества.

Решение этих вопросов должно происходить с позиции системного подхода, который обеспечивает выявление проблемных зон и опасных угроз в деятельности гостиницы и предлагает дальнейшие меры по их устранению

Особенно острыми вопросами совершенствования системы безопасности гостиничного предприятия на сегодняшний

день являются вопросы оборудование систем видеонаблюдения и кибербезопасности.

Вопрос кибербезопасности был вынесен на широкое обсуждение в октябре 2016 года, когда огромное количество пораженных вирусами устройств, включая оборудование для систем видеонаблюдения, были использованы для DDoS-атак ботнетом Mirai [1].

Кибербезопасность имеет большое значение для производителей систем видеонаблюдения. С внедрением подключенных к сети интернет цифровых видеорегистраторов (DVR) и камер видеонаблюдения, системы видеонаблюдения утратили свою «закрытую» природу.

Сетевые технологии сделали видеонаблюдение более интеллектуальным, видеоархив доступным из любой точки мира, а системы видеонаблюдения в целом еще более масштабируемыми.

Некоторые текущие вопросы кибербезопасности возникают из-за недостатка образования в индустрии видеонаблюдения, часто медленно принимающей все лучшие достижения в сфере информационных сетей и подходы, уже применяемые в информационно-коммуникационных технологиях.

Действительно, слабые места защиты в системах, которые уже эксплуатировались, возникают, как правило, из-за дефолтных паролей или из-за старых прошивок. Многие установщики систем видеонаблюдения не меняют паролей, в силу привычки и непонимания важности этой процедуры.

Плюс ко всему, обновление патчей безопасности для устройств видеонаблюдения часто является трудоемким процессом, оборудование может быть от разных производителей, да и даже в рамках одного производителя часто не существует инструментов, позволяющих отслеживать актуальность прошивок.

Информационная безопасность для оборудования, последнее время всегда на первом месте в повестке дня на многих мероприятиях индустрии видеонаблюдения. Индустрия в целом предпринимает согласованные усилия для обучения пользователей и внедрения передового опыта с целью обеспечения безопасности сетевого оборудования в системах видеонаблюдения[2].

Тем не менее, изменение поведенческой модели часто является не таким быстрым процессом. Серьезные атаки, такие как те, что были в октябре 2016 года, по крайней мере, повышают интерес и внимание общественности к этой проблеме.

Выделение кибербезопасности, как отличительной характеристики продукта или монетизация сервиса защиты могут быть проблемой для поставщиков оборудования систем видеонаблюдения.

Прогресс в кибербезопасности может привести к возникновению у пользователей вопросов по информационной защите оборудования, которое уже установлено. Более того, есть опасения, что компания, рекламирующая информационную защиту своего оборудования, побудит хакеров к атакам на такое оборудование.

Продукты информационной защиты, предназначенные для сетевого оборудования систем видеонаблюдения, по-прежнему встречаются редко. Есть всего лишь несколько таких примеров, например, протокол DirectIP разработанный компанией IDIS [3].

Приложения для анализа видеоданных не являются новинкой для индустрии систем видеонаблюдения.

В течение некоторого времени видеоаналитика страдала из-за чрезмерно амбициозных разработчиков ПО, которые преувеличивали эффект, получаемый при помощи этой технологии.

В России возможности видеоаналитики представлены российскими разработчиками программного обеспечения и мировыми производителями, представляющими свои камеры видеонаблюдения со встроенными возможностями видеоаналитики.

Первые пользователи часто находили, что достоверность результатов анализа видеоданных была далека от обещанных результатов, что привело к потере доверия к рынку, в основном это касается приложений, осуществляющих распознавание лиц.

Доверие к рынку будет восстановлено новым поколением технологии видеоанализа – движимой технологией глубинного обучения, высокой производительностью вычислений, анализом большого объема данных.

Глубинное обучение – это быстро растущее направление в сфере искусственного интеллекта, оно может дать возможность компьютерам интерпретировать огромное количество данных. Используя многослойную систему нелинейной обработки данных, машина имеет возможность изучать признаки данных самостоятельно, без учителя или с частичным привлечением учителя [4].

При постоянном обучении, «подкармливаемой» массивными объемами данных, машины со временем автоматически могут увеличить точность анализа и классификацию.

Эти технологии улучшают эффективность развития оборудования, работающего с технологией VCA, повышают точность путем получения доступа к более быстрой обработке данных, а также дают возможность системе автоматически обучаться на протяжении всей длительности отснятого видео системой наблюдения материала. Способность технологии глубинного обучения самоприспосабливаться к анализу видео и ее требование меньшей корректировки алгоритма, произведет в будущем большой скачок в части использования, точности и широкого применения технологии анализа видеоданных.

Тем не менее, путь в массовое принятие технологии анализа видеоданных, базирующегося на глубинном обучении, не так прост. Огромное препятствие, которое встречают и поставщики систем видеонаблюдения и разработчики программного обеспечения, остается неизменным – в каждом случае план наблюдения будет разным. Даже с

адаптационным и обучающим алгоритмами широта возможного применения требует значительных усилий для решения задач.

Нательные камеры прочно заняли свое место в обязательной экипировке сотрудников правоохранительных органов во многих странах мира. И вопрос о широком распространении нательных камер среди сотрудников безопасности гостиниц уже не ставится под сомнение никем из экспертов, сейчас на первый план выходит вопрос «когда?» это произойдет.

Носимые на теле камеры меняют характер поведения человека, повышают материальную ответственность и уменьшают количество нежелательных действий.

Последние исследования, проведенные Институтом криминологии Кембриджского Университета, показали, что внедрение носимых камер для сотрудников полиции Бостона привело к снижению количества жалоб со стороны представителей общественности на 93% [1].

Легко представить потенциальные преимущества нательных камер: для сотрудников безопасности гостиниц и руководства в период кризисов, таких как вооруженный захват заложников или террористические акты.

Огромную помощь в видеонаблюдении могут оказать роботы . Еще в 2016 году было замечено значительное увеличение количества беспилотных транспортных решений, представленных на выставках по безопасности. В первую очередь это летающие дроны (автономные беспилотные летательные аппараты – АБПЛА) и наземные роботы (автономные беспилотные наземные транспортные средства – АБНТС).

Пока стационарное оборудование не будет способно обеспечить стопроцентный охват всей территории гостиничного комплекса, дроны и роботы способны выступать в качестве «мультипликаторов повышения эффективности» для содействия охранным подразделениям.

При этом беспилотные устройства осуществляют выполнение обычных рутинных задач, а персонал службы охраны выполняет более специфические, требующие участия человека задачи.

Есть две основные функции, предусмотренные для дронов и роботов в коммерческой безопасности: обход и сигнализация. И дроны, и роботы могут быть использованы для предварительно программируемого обхода объекта, для постоянного круглосуточного патрулирования.

Огромное влияние на эффективность использования системы оказывает то, насколько легко пользователи могут взаимодействовать с программным обеспечением управления видеонаблюдением [5].

Простота использования – это все, когда речь идет о ежедневных операциях, начиная от обязательной подготовки новых операторов, расходов, относящихся к криминалистическому анализу видео, операций экспортирования видео доказательств или даже непосредственного реагирования на чрезвычайные ситуации – простота использования первостепенна.

В скором будущем управление видеонаблюдение в гостиничных комплексах может оказаться на границе великих, еще более неожиданных изменений, связанных с интегрированием ботов искусственного интеллекта (AI).

Боты искусственного интеллекта – это программные продукты, которые используют искусственный интеллект для обеспечения взаимодействия пользователя с системой, с помощью речи или мгновенных сообщений.

Боты могут автоматизировать задачи или выполнять рутинные операции. Иногда их называют AI ассистенты. В обширной индустрии программного обеспечения широкое использование AI ботов это следующий этап эволюции, следующий за взрывом прикладных программ.

Интеграция AI ботов как путь к взаимодействию между всеми видами программного обеспечения гостиничных комплексов должна стать небывалой по своей значимости тенденцией. Это должно фундаментально изменить механизм, по которому сотрудник отдела службы безопасности гостиниц взаимодействует с софтом каждый день.

На современном этапе развития уровня технологий ключевое значение приобретает правильный выбор технических средств систем безопасности, с последующим правильным их проектированием, монтажом и обслуживанием.

Список литературы:

1. Демурин В. Б. Современные автоматизированные системы управления гостиницами и их функциональные возможности // Молодой ученый. – 2017. – №8. – С. 162-166.
2. Ивлев Н.А. Совершенствование системы безопасности в гостиничном бизнесе / Н.А. Ивлев, В.А. Чернобровкин // Международный студенческий научный вестник. – 2017. - №10. – С.1-6.
3. Мартиросян Т.А. К вопросу о содержании понятия «безопасность»/ Т.А. Мартиросян // Стратегия гражданской защиты: проблемы и исследования. – Выпуск № 2. - Том 3. - 2017. – С.359-362.
4. Печерица Е.В. Комплексный подход к эффективному обеспечению экономической безопасности на предприятиях сферы сервиса и туризма / Е.В. Печерица, Я.С. Тестина // Фундаментальные исследования. – 2018. – № 7-1. – С. 167-170.
5. Чудновский А.Д. Безопасность бизнеса в индустрии туризма и гостеприимства / А.Д. Чудновский, Ю.М. Белозерова. – М.: Инфра-М, 2016. – 336 с.
6. Федоров Р.Г. Гостиничный бизнес как составляющая современной индустрии туризма / Р.Г. Фёдоров // Молодой ученый. - 2018. - №4. - С. 307-311.