Международный союз электросвязи

МСЭ-Т X.1453

(01/2022)

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ,
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ
И БЕЗОПАСНОСТЬ

Безопасные приложения и услуги (2) –
Безопасность приложений (2)

Угрозы и требования безопасности для систем управления видео

Рекомендация МСЭ-Т X.1453

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	X.1–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	X.200–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	X.300–X.399
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	X.600–X.699
УПРАВЛЕНИЕ В ВОС	X.700–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	X.850–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ	
Общие аспекты безопасности	X.1000–X.1029
Безопасность сетей	X.1030–X.1049
Управление безопасностью	X.1050–X.1069
Телебиометрия	X.1080–X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (1)	
Безопасность многоадресной передачи	X.1100–X.1109
Безопасность домашних сетей	X.1110–X.1119
Безопасность подвижной связи	X.1120–X.1139
Безопасность веб-среды (1)	X.1140–X.1149
Безопасность приложений (1)	X.1150–X.1159
Безопасность одноранговых сетей	X.1160–X.1169
Безопасность сетевой идентификации	X.1170–X.1179
Безопасность IPTV	X.1180–X.1199
БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА	
Кибербезопасность	X.1200–X.1229
Противодействие спаму	X.1230–X.1249
Управление определением идентичности	X.1250–X.1279
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (2)	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1319
Безопасность умных электросетей	X.1330–X.1339
Сертифицированная электронная почта	X.1340–X.1349
Безопасность интернета вещей (IoT)	X.1350–X.1369
Безопасность интеллектуальных транспортных систем (ИТС)	X.1370–X.1399
Безопасность технологии распределенного реестра (DLT)	**X.1400–X.1429**
Безопасность приложений (2)	X.1450–X.1459
Безопасность веб-среды (2)	X.1470–X.1489
ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ	
Обзор кибербезопасности	X.1500–X.1519
Обмен информацией об уязвимости/состоянии	X.1520–X.1539
Обмен информацией о событии/инциденте/эвристических правилах	X.1540–X.1549
Обмен информацией о политике	X.1550–X.1559
Эвристические правила и запрос информации	X.1560–X.1569
Идентификация и обнаружение	X.1570–X.1579
Гарантированный обмен	X.1580–X.1589
Киберзащита	X.1590–X.1599
БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ	
Обзор безопасности облачных вычислений	X.1600–X.1601
Проектирование безопасности облачных вычислений	X.1602–X.1639
Передовой опыт и руководящие указания в области облачных вычислений	X.1640–X.1659
Обеспечение безопасности облачных вычислений	X.1660–X.1679
Другие вопросы безопасности облачных вычислений	X.1680–X.1699
КВАНТОВАЯ СВЯЗЬ	
Терминология	X.1700–X.1701
Квантовый генератор случайных чисел	X.1702–X.1709
Структура безопасности QKDN	X.1710–X.1711
Проектирование безопасности QKDN	X.1712–X.1719
Методы обеспечения безопасности QKDN	X.1720–X.1729
БЕЗОПАСНОСТЬ ДАННЫХ	
Безопасность больших данных	X.1750–X.1759
Защита данных	X.1770–X.1789
БЕЗОПАСНОСТЬ СЕТЕЙ IMT-2020	X.1800–X.1819

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Рекомендация МСЭ-Т X.1453

Угрозы и требования безопасности для систем управления видео

Резюме

Система управления видео (VMS) – это ядро систем видеонаблюдения, используемых для обеспечения общественной безопасности, мониторинга дорожного движения и т. п. По сути VMS принимает видеосигналы от видеокамер и позволяет пользователю просматривать видеоизображение в режиме реального времени или в записи. В настоящее время в VMS добавляется все больше и больше интеллектуальных функций, включая анализ видеоизображения и управление доступом.

Поскольку VMS подключена к сети, она подвержена всевозможным угрозам, с которыми сталкиваются интернет-службы, и легко может стать целью кибератак.

В Рекомендации МСЭ-Т X.1453 анализируются угрозы безопасности для VMS на основе серверной платформы, работающей в IP-сети, и определяются требования безопасности для противодействия выявленным угрозам.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1453	07.01.2022 г.	17-я	11.1002/1000/14802

Ключевые слова

Структура безопасности, требование безопасности, система управления видео.

* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL http://handle.itu.int/, после которого укажите уникальный идентификатор Рекомендации.
Например, http://handle.itu.int/11.1002/1000/11830-en.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним в целях стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения Исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" (shall) или некоторые другие обязывающие выражения, такие как "обязан" (must), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещения об интеллектуальной собственности, защищенной патентами/авторскими правами на программное обеспечение, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к соответствующим базам данных МСЭ-Т, доступным на веб-сайте МСЭ-Т по адресу http://www.itu.int/ITU-T/ipr/.

СОДЕРЖАНИЕ

Рекомендация МСЭ-Т X.1453

Угрозы и требования безопасности для систем управления видео

1 Сфера применения

В настоящей Рекомендации определяются угрозы и требования безопасности для системы управления видео (VMS) на основе серверной платформы, которая принимает видеосигналы от видеокамер, представляющих собой один из типов устройств интернета вещей (IoT), и позволяет пользователям просматривать видеоизображение в режиме реального времени или в записи. Настоящая Рекомендация охватывает следующие темы:

– анализ архитектуры VMS на базе серверной платформы;

– анализ угроз безопасности, с которыми сталкиваются такие VMS;

– требования безопасности для противодействия выявленным угрозам.

2 Справочные документы

Указанные ниже Рекомендации МСЭ-Т и другие справочные документы содержат положения, которые путем ссылок на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие справочные документы могут подвергаться пересмотру; поэтому всем пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других справочных документов, перечисленных ниже. Перечень действующих на настоящий момент Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статус Рекомендации.

Отсутствуют.

3 Определения

3.1 Термины, определенные в других документах

В настоящей Рекомендации используется следующий термин, определенный в других документах.

3.1.1 система видеонаблюдения (video surveillance system) [b-ITU-T H.626]: Услуга электросвязи, ориентированная на технологию применения видео (включая изображение и звук), используемую для дистанционного сбора мультимедийных сигналов (например, аудио, видео, изображений, сигналов тревоги и т. д.) и их представления конечному пользователю в удобной для него форме через управляемую широкополосную сеть с гарантированными уровнями качества, безопасности и надежности.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определен следующий термин.

3.2.1 система управления видео (video management system): Важная часть любой системы видеонаблюдения, которая позволяет просматривать видеоизображение с нескольких видеокамер, записывать и анализировать видеопотоки, а также подает предупредительные сигналы о взломе и обнаружении движения.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

DDoS	Distributed Denial of Service	Распределенный отказ в обслуживании
IDS	Intrusion Detection System	Система обнаружения вторжений
IoT	Internet of Things	Интернет вещей

IP	Internet Protocol	Протокол Интернет
IPS	Intrusion Prevention System	Система предотвращения вторжений
NVR	Network Video Recorder	Сетевой видеорегистратор
VMS	Video Management System	Система управления видео

5 Соглашения

В настоящей Рекомендации:

ключевые слова "**требуется, чтобы**" означают требование, которому необходимо неукоснительно следовать и отклонение от которого не допускается, если будет сделано заявление о соответствии настоящей Рекомендации;

ключевое слово "**рекомендуется**" означает требование, которое рекомендуется, но не является абсолютно необходимым; таким образом для заявления о соответствии настоящей Рекомендации это требование не является обязательным.

6 Система управления видео

В последние несколько лет во всем мире быстро развивается технология IoT. Системы видеонаблюдения на основе интернета вещей позволяют пользователям наблюдать за действиями, происходящими в удаленном месте, и записывать нужные фрагменты видеоизображения. Сценарии использования этих систем широко варьируются – от правоприменительной деятельности и предотвращения преступности до обеспечения безопасности на транспорте и мониторинга дорожного движения. VMS представляет собой ядро систем видеонаблюдения, используемых для систем общественной безопасности и мониторинга дорожного движения. По сути VMS получает видеосигнал от видеокамер и позволяет пользователям просматривать видеоизображение в режиме реального времени или в записи. В настоящее время в VMS добавляется все больше и больше интеллектуальных функций, включая анализ видеоизображения и управление доступом.

Поскольку VMS подключена к сети, она подвержена всевозможным угрозам, с которыми сталкиваются интернет-службы, и может стать целью кибератак.

Типичная система видеонаблюдения на основе интернета вещей состоит из нескольких видеокамер системы безопасности, VMS и клиентских устройств, на которых пользователь может просматривать видеоизображение. VMS позволяет записывать и просматривать видео в режиме реального времени с нескольких видеокамер системы безопасности, получать сигналы тревоги, управлять видеокамерами и извлекать видеозаписи из архивов. VMS на основе IoT отличаются более широкими возможностями и большей гибкостью по сравнению с аналоговыми системами и позволяют пользователю управлять устройствами, входящими в систему видеонаблюдения, находясь в любом месте сети.

VMS поддерживают множество различных функций:

– одновременный просмотр;
– запись видеоизображения и звука;
– поиск и воспроизведение видеоизображений;
– интеллектуальный анализ видеоизображений;
– управление видеокамерами;
– управление событиями;
– управление сигнализацией.

Для сетевых VMS имеются аппаратные платформы двух типов – VMS на основе серверной платформы с одним или несколькими серверами, на которых работает программа управления видео, и VMS на основе сетевого видеорегистратора (NVR). VMS – это комбинация из программного обеспечения и видеооборудования. Программное обеспечение для управления видео может быть установлено на оборудовании NVR или на серверном оборудовании. Программное обеспечение для управления видео, установленное на NVR, используется для решения простых задач, таких как запись и мониторинг

видеоматериалов в ограниченном пространстве, в то время как программное обеспечение для управления видео, установленное на сервере, удаленно управляет множеством видеокамер, расположенных в разных местах, обеспечивает хранение видеоматериалов и управление ими, а также выполняет интеллектуальный анализ видеоизображений в целях автоматического обнаружения событий. Обычно VMS на основе NVR – это VMS с использованием только одного NVR, а VMS на основе сервера – это VMS с одним или несколькими серверами, которая контролирует множество видеокамер и предоставляет расширенные услуги анализа. Настоящая Рекомендация посвящена только VMS на основе серверных платформ.

Для анализа безопасности VMS определяется архитектура, описывающая все объекты, связанные с видеонаблюдением на основе VMS, и проясняющая отношения между ними. Функциональная архитектура VMS для приложений видеонаблюдения показана на рисунке 1.

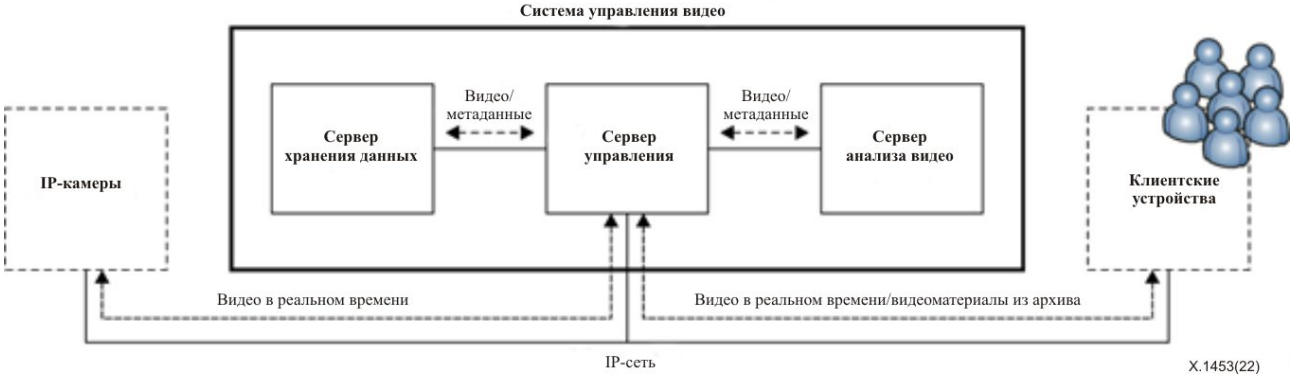

Рисунок 1 – Упрощенная архитектура функциональной VMS

Системы видеонаблюдения работают с объектами пяти основных типов: видеокамерами, серверами хранения данных, серверами управления, серверами анализа видео и клиентскими устройствами. VMS в ядре системы видеонаблюдения состоит из сервера управления, сервера хранения данных и сервера анализа видео. Между объектами, показанными на рисунке 1, существует четыре вида взаимосвязей: между видеокамерой и сервером управления, между сервером управления и клиентским устройством, между сервером управления и сервером хранения, а также между сервером управления и сервером анализа видео.

VMS подключается к камерам и клиентским устройствам через сеть. Сервер управления, сервер хранения данных и сервер анализа видео обычно находятся в одной и той же сети. Клиентские устройства, как правило, подключаются к открытой сети, такой как интернет, для расширенного дистанционного мониторинга.

Центральной частью VMS является сервер управления. Он управляет всеми структурными элементами в системах видеонаблюдения, включая настройки видеокамер и параметры хранения видеоматериалов. Сервер хранения записывает видео с камер, которые к нему подключены, и хранит метаданные, созданные сервером анализа видео. Сервер анализа видео анализирует движущиеся объекты в видеопотоке и создает метаданные для описания выявленных действий и событий. Сервер анализа видео генерирует метаданные двух типов – метаданные событий и метаданные предупредительных сигналов. Каждое событие и каждый предупредительный сигнал состоят из нескольких сообщений с метаданными, содержащих различные атрибуты, связанные с обнаруженным сегментом изменения или движения в видеопотоке.

7 Угрозы безопасности

7.1 Угрозы для интерфейса между сервером управления и видеокамерой

Основная задача интерфейса между сервером управления и видеокамерой – прием видеосигнала от камеры, настройка параметров камеры и управление камерами (поворот, наклон и масштабирование). Основной целью злоумышленников являются данные, передаваемые через эти интерфейсы. Злоумышленник может причинить ущерб VMS, перехватывая, фальсифицируя и воспроизводя данные.

Другой целью злоумышленников является нарушение работы VMS путем запуска распределенной атаки типа отказ в обслуживании (DDoS) против видеокамер и сервера управления.

Интерфейс между сервером управления и камерой подвержен следующим угрозам.

- Несанкционированный доступ. Атака заключается в получении доступа к видеокамере путем использования чужой учетной записи или каким-либо иным способом. Несанкционированный доступ к камере может привести к раскрытию конфиденциальной информации, модификации видео и незаконному использованию ресурсов. Например, получив доступ к видеокамере, злоумышленник может незаконно собирать видеоданные и осуществлять видеонаблюдение в режиме реального времени, что ведет к проблемам нарушения конфиденциальности.
- Перехват данных в сети. Атака заключается в перехвате видеоданных из сети и считывании видеоконтента в поисках конфиденциальной информации, такой как изображения лиц и номера автомобилей.
- Отказ в обслуживании. Попытка запустить вредоносный код на сервере управления или камерах для перегрузки целевого устройства большим объемом данных или запросов на обслуживание. С помощью этой атаки работа VMS может быть замедлена или остановлена.
- Фальсификация видеоданных. Злоумышленник блокирует видеоданные, а затем передает на сервер управления фальсифицированные видеоданные. Атака может привести к нарушению нормальной работы VMS.
- Фальсификация данных управления. Злоумышленник блокирует данные управления, предназначенные для настройки параметров камеры, а затем отправляет на камеры фальсифицированные данные управления. Такая атака может привести к нарушению нормального выполнения функций управления камерой.
- Внутренние угрозы. В процессах с участием людей всегда существует риск того, что они будут действовать злонамеренно или неосторожно, подвергая риску VMS. Пользователи, использующие пароль администратора или оставляющие регистрационные данные в небезопасном месте, неосторожные или недостаточно обученные пользователи либо недовольные пользователи, предпринимающие злонамеренные действия, всегда будут представлять серьезную угрозу.

7.2 Угрозы для интерфейса между сервером управления и клиентским устройством

Основная задача интерфейса между сервером управления и клиентским устройством – предоставление интерфейсов для просмотра видео в режиме реального времени и доступа к записанным видеоматериалам.

Интерфейс между сервером управления и клиентским устройством подвержен следующим угрозам.

- Несанкционированный доступ. Атака заключается в получении доступа к клиентскому устройству путем использования чужой учетной записи или каким-либо иным способом. Несанкционированный доступ к клиентскому устройству может привести к раскрытию конфиденциальной информации и незаконному использованию ресурсов. Например, получив доступ к клиентскому устройству, злоумышленник может незаконно собирать видеоданные и осуществлять видеонаблюдение в режиме реального времени, что ведет к проблемам нарушения конфиденциальности.
- Перехват данных в сети. Атака заключается в перехвате видеоданных из сети и считывании видеоконтента в поисках конфиденциальной информации, такой как изображения лиц, номера автомобилей, и любой другой закрытой информации.
- Отказ в обслуживании. Попытка запустить вредоносный код на сервере управления или клиентских устройствах для перегрузки целевого устройства большим объемом данных или запросов на обслуживание. С помощью этой атаки работа VMS может быть замедлена или остановлена.
- Фальсификация видеоданных. Злоумышленник блокирует видеоданные, а затем отправляет фальсифицированные видеоданные на клиентские устройства. Атака может привести к нарушению нормальной работы VMS.

- Фальсификация данных управления. Злоумышленник блокирует данные управления, предназначенные для настройки параметров камеры, а затем отправляет на сервер управления фальсифицированные данные управления. Такая атака может помешать пользователю осуществлять обычные функции видеонаблюдения.
- Внутренние угрозы. В процессах с участием людей всегда существует риск того, что они будут действовать злонамеренно или неосторожно, подвергая риску VMS. Пользователи, использующие пароль администратора или оставляющие регистрационные данные в небезопасных местах, неосторожные или недостаточно обученные пользователи либо недовольные пользователи, предпринимающие злонамеренные действия, всегда будут представлять серьезную угрозу.

7.3 Угрозы для интерфейса между сервером управления и сервером хранения данных

Основная задача интерфейса между сервером управления и сервером хранения данных – предоставление интерфейсов для записи/просмотра видео и метаданных.

Сервер управления и сервер хранения данных обычно расположены в одной и той же сети или соединены через выделенную линию. Даже если к сети общего пользования подключен только сервер управления, хакер может использовать уязвимости его системы безопасности для получения незаконного доступа к серверу хранения данных.

Интерфейс между сервером управления и сервером хранения данных подвержен следующим угрозам.

- Несанкционированный доступ. Атака заключается в получении доступа к серверу управления путем использования чужой учетной записи или каким-либо иным способом, чтобы получить доступ к данным, хранящимся на сервере хранения данных. Несанкционированный доступ к серверу хранения данных может привести к раскрытию конфиденциальной информации и незаконному использованию ресурсов.
- Раскрытие данных. Атака заключается в незаконном получении доступа к видеоконтенту, хранящемуся на сервере, и считывании конфиденциальной информации, такой как изображения лиц, номерные знаки и т. д. Злоумышленник может раскрыть данные, которые не были защищены.
- Введение и изменение данных. Атака заключается в незаконном изменении сохраненных видеоданных путем введения в них искаженных данных, что снижает надежность видеоинформации.
- Внутренние угрозы. В процессах с участием людей всегда существует риск того, что они будут действовать злонамеренно или неосторожно, подвергая риску VMS. Пользователи, использующие пароль администратора или оставляющие регистрационные данные в небезопасных местах, неосторожные или недостаточно обученные пользователи либо недовольные пользователи, предпринимающие злонамеренные действия, всегда будут представлять серьезную угрозу.

7.4 Угрозы для интерфейса между сервером управления и сервером анализа видео

Основная задача интерфейса между сервером управления и сервером анализа видео – передача видеоданных и метаданных для анализа движущихся объектов в целях описания действий и событий, обнаруженных на сервере анализа видео.

Сервер управления и сервер анализа видео обычно расположены в одной и той же сети или соединены через выделенную линию. Даже если к сети общего пользования подключен только сервер управления, хакер может использовать уязвимости его системы безопасности для получения незаконного доступа к серверу анализа видео.

Интерфейс между сервером управления и сервером анализа видео подвержен следующим угрозам.

- Несанкционированный доступ. Атака заключается в получении доступа к серверу управления путем использования чужой учетной записи или каким-либо иным способом, чтобы получить доступ к данным, хранящимся на сервере анализа видео. Несанкционированный доступ к серверу анализа видео может привести к неисправностям, что снижает надежность сервера анализа видео.

- Раскрытие данных. Атака заключается в незаконном получении доступа к видеоконтенту, хранящемуся на сервере, и считывании конфиденциальной информации, такой как изображения лиц и номерные знаки. Злоумышленник может раскрыть данные, которые не были защищены.
- Введение и изменение данных. Атака заключается в незаконном изменении сохраненных видеоданных или метаданных путем введения в них искаженных данных, что снижает надежность сервера анализа видео. Например, незаконно получив доступ к серверу управления, злоумышленник может получить разрешения для неавторизованного лица путем замены сохраненных данных авторизованного лица данными неавторизованного лица.
- Внутренние угрозы. В процессах с участием людей всегда существует риск того, что они будут действовать злонамеренно или неосторожно, подвергая риску VMS. Пользователи, использующие пароль администратора или оставляющие регистрационные данные в небезопасных местах, неосторожные или недостаточно обученные пользователи либо недовольные пользователи, предпринимающие злонамеренные действия, всегда будут представлять серьезную угрозу.

7.5 Взаимосвязь между угрозами безопасности и объектами внутри/вне VMS

Угрозы безопасности нацелены на определенные места между объектами, изображенными на рисунке 1. Взаимосвязь угроз безопасности и объектов внутри/вне VMS показана в таблице 1, где кружок в ячейке означает, что объект связан с конкретной угрозой безопасности.

Таблица 1 – Связь между требованиями безопасности и объектами

Объекты / Угрозы	Между VMS и камерами	VMS		Между VMS и клиентскими устройствами
		Между сервером управления и сервером хранения данных	Между сервером управления и сервером анализа видео	
Перехват данных в сети	○			○
Несанкционированный доступ	○	○	○	○
Отказ в обслуживании	○			○
Раскрытие данных		○	○	
Введение и изменение данных	○	○	○	○
Внутренние угрозы	○	○	○	○

8 Требования безопасности

8.1 Конфиденциальность

Конфиденциальность гарантирует, что содержание данных не может быть прочитано неавторизованными объектами. Даже в тех случаях, когда некоторые данные бывают перехвачены и раскрыты злоумышленником, их конфиденциальность может быть обеспечена.

Конфиденциальные данные должны быть защищены как при хранении, так и при передаче. К конфиденциальным данным относятся видеоданные, данные команд, управляющих работой камер, и данные, хранящиеся на сервере хранения.

- Конфиденциальность должна гарантировать, что видеоданные, передаваемые по сети, не будут прочитаны неавторизованными объектами.
- Конфиденциальность должна гарантировать, что передаваемые по сети данные команд, управляющих работой камер, не будут прочитаны неавторизованными объектами.
- Рекомендуется, чтобы конфиденциальность гарантировала невозможность прочтения данных, хранящихся на сервере хранения и сервере анализа видео, неавторизованными объектами.

8.2 Целостность

Целостность гарантирует, что переданные данные не отличаются от исходных. Требуется, чтобы исходные сохраненные данные не изменялись после авторизованного доступа.

- Требуется, чтобы целостность гарантировала, что видеоданные, передаваемые камерами, представляют собой исходные данные без фальсификации.
- Рекомендуется, чтобы целостность гарантировала, что сохраненные видеоданные представляют собой исходные данные без фальсификации.
- Рекомендуется, чтобы целостность гарантировала, что видеоданные, экспортированные для целей уголовного расследования и т. п., представляют собой исходные данные, которые не были изменены.

8.3 Аутентификация пользователей и устройств

Аутентификация требуется для подтверждения идентичности пользователей и устройств. Аутентификация подтверждает подлинность заявленной идентификационной информации объектов, участвующих в процессе видеонаблюдения, и обеспечивает уверенность в том, что неавторизованный объект не пытается выдавать себя за авторизованный объект.

- Требуется, чтобы аутентификация пользователей гарантировала, что пользователь является законным администратором, которому разрешен доступ к серверам VMS для централизованного управления видео.
- Требуется, чтобы аутентификация пользователей гарантировала, что пользователь является законным пользователем клиентского устройства, которому разрешен удаленный просмотр видеоданных.
- Рекомендуется, чтобы аутентификация устройств гарантировала, что устройство является законным клиентским устройством, которому разрешено дистанционно подключаться к VMS.
- Рекомендуется, чтобы аутентификация устройств гарантировала, что видеокамера представляет собой законную камеру, которой разрешено подключаться к VMS.

8.4 Управление доступом

Управление доступом должно гарантировать, что доступ к соответствующим ресурсам, участвующим в видеонаблюдении, имеют только авторизованные пользователи. Хотя администраторы входят в привилегированную группу, членам которой разрешено техническое обслуживание системы видеонаблюдения и управление ею, рекомендуется, чтобы каждому отдельному пользователю предоставлялись разные права доступа.

- Требуется, чтобы управление доступом гарантировало, что только авторизованные пользователи получают доступ к серверу управления в соответствии с их привилегиями доступа в системе видеонаблюдения. Доступ может предоставляться для видеонаблюдения в режиме реального времени, воспроизведения видеозаписей и дистанционного управления камерами.
- Требуется, чтобы управление доступом гарантировало, что только авторизованные пользователи клиентских устройств получают доступ к видеонаблюдению в соответствии с их привилегиями доступа. Доступ может предоставляться для видеонаблюдения в режиме реального времени и воспроизведения видеозаписей.

8.5 Предотвращение вторжений

Предотвращение вторжений должно защищать объекты VMS, сохраненные видеоданные и услуги от попыток внутреннего и внешнего несанкционированного доступа. Предотвращение вторжений в VMS может осуществляться логическими и физическими методами. Логический метод предотвращения вторжений защищает системные ресурсы от атак с использованием сети на базе IP. Метод физического предотвращения вторжений защищает системные ресурсы от несанкционированного физического доступа.

- Требуется, чтобы логическое предотвращение вторжений гарантировало защиту системных ресурсов от атак с использованием сети на базе IP, обеспечивая нормальную работу системы видеонаблюдения. К системам сетевой безопасности, используемым для логического предотвращения вторжений, относятся системы обнаружения вторжений (IDS) и системы

предотвращения вторжений (IPS). Предпочтительнее использовать специализированную систему обеспечения безопасности сети, нежели систему, реализованную внутри VMS.

- Требуется, чтобы физическое предотвращение вторжений гарантировало, что только законные пользователи, идентифицированные методами аутентификации, могут войти в центр обеспечения безопасности, где установлена VMS.

8.6 Взаимосвязь между требованиями безопасности и угрозами безопасности

Взаимосвязь между требованиями безопасности и угрозами безопасности показана в таблице 2, где кружок в ячейке означает, что для устранения или смягчения конкретной угрозы должно быть выполнено конкретное требование безопасности.

Таблица 2 – Взаимосвязь между требованиями и угрозами безопасности

			Требования безопасности				
			Конфиденциальность	Целостность	Аутентификация пользователей/ устройств	Управление доступом	Предотвращение вторжений
Угрозы безопасности	VMS	Несанкционированный доступ			○	○	
		Раскрытие данных	○				
		Изменение/введение данных		○			
		Внутренние угрозы			○	○	
		DoS					○
	Между VMS и камерами	Несанкционированный доступ			○	○	
		Перехват данных	○				
		DoS					○
		Изменение/введение данных		○			
		Внутренние угрозы			○	○	
	Между VMS и клиентскими устройствами	Несанкционированный доступ			○	○	
		Перехват данных	○				
		DoS					○
		Изменение/введение данных		○			
		Внутренние угрозы			○	○	

Библиография

[b-ITU-T H.626] Recommendation ITU-T H.626 (2019), *Architecture requirements for video surveillance system.*

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Принципы тарификации и учета и экономические и стратегические вопросы международной электросвязи/ИКТ
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Окружающая среда и ИКТ, изменение климата, электронные отходы, энергоэффективность; конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация, а также соответствующие измерения и испытания
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	**Сети передачи данных, взаимосвязь открытых систем и безопасность**
Серия Y	Глобальная информационная инфраструктура, аспекты протокола Интернет, сети последующих поколений, интернет вещей и умные города
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2022 г.