ТЕХНИЧЕСКИЙ ОБЗОР

Цифровизация и кибербезопасность систем контроля физического доступа

Исследование систем и протоколов, позволяющих компаниям в полной мере использовать все возможности систем контроля доступа, создавая более разумный и безопасный мир

Август 2021

AXIS COMMUNICATIONS

Содержание

1 Краткая информация

Развитие облачных технологий меняет облик индустрии физической безопасности и вынуждает установщиков идти в ногу со временем, чтобы остаться в бизнесе. По всей видимости, системы контроля доступа переходят в сферу компетенции глобальных технологических компаний, что вызывает ожидания большей экономической выгоды, поскольку системы становятся все более интеллектуальными, масштабируемыми и ориентированными на периферийные устройства.

Такая эволюция, наряду с потенциалом для интеграции с другими корпоративными системами, также означает, что кибербезопасность должна играть еще большую роль в разработке и развертывании систем, особенно когда для них используется уже существующая инфраструктура. Преодоление технических барьеров, таких как последовательная архитектура, отсутствие MAC-адресов и т. д., является важным шагом в переходе к цифровым системам контроля доступа, способным удовлетворить сегодняшние и будущие требования.

Внедрение и обеспечение безопасности цифровой системы контроля доступа также означает использование передового опыта для обеспечения ее максимальной защиты. Необходимо оценить и протестировать каждый компонент системы, будь то устройство, поставщик или протокол — все они должны быть надежными и заслуживающими доверия. Также необходима постоянная осведомленность об угрозах и способах снижения опасностей, связанных с обнаруживаемыми уязвимостями и ошибками.

Особое внимание следует уделять поставщикам, чьи устройства вы собираетесь подключить к своей сети. Серьезный поставщик должен предоставить и обнародовать свои процессы для защиты предлагаемых им продуктов, например опубликовав руководство по усилению безопасности, предоставив специальные инструменты, которые упрощают управление сетевыми устройствами и их защиту и т. п. Кроме того, желательно, чтобы поставщик проявлял честность и открытость в отношении своей стратегии управления обнаруженными уязвимостями и ошибками.

2 Введение: Будущее систем контроля доступа

С развитием облачных технологий в сфере физической безопасности появился новый подход к развертыванию и использованию систем. Конечным пользователям и покупателям нужны интеллектуальные интегрированные и более ориентированные на бизнес решения с возможностями видеонаблюдения и контроля доступа, которые бы намного превосходили возможности традиционных и уже устаревших технологий.

Многие поставщики построили прочную бизнес-модель на основе своего опыта, услуг и знаний в области физической безопасности. Однако возможности подключения к сети и интернет вещей (IoT) означают постоянно меняющиеся условия, требующие от поставщиков и установщиков систем физической безопасности изучения языка информационных технологий, использования открытых платформ, IP-технологий и интеграции программного обеспечения, чтобы адаптироваться к изменениям рынка и оставаться конкурентоспособными.

По всей видимости, инициатива быстро переходит от поставщиков электронных систем контроля и управления доступом (СКУД) к глобальным технологическим компаниям, получившим возможность формировать индустрию безопасности в направлении, которое бросает вызов ее традиционному функционированию. Создание умных зданий и городов открывает широкие возможности, в связи с чем ожидается быстрый рост рынка современных систем контроля доступа, ведь простота развертывания и степень развитости современных технологий дают умной среде множество преимуществ.

Стремление к внедрению систем СКУД, использующих облачные сервисы, не вызывает удивления: крупные технологические компании уже продемонстрировали успешное применение облачных технологий за время глобальной пандемии COVID-19. У таких компаний есть возможности, масштабы и творческий потенциал, позволяющие добиться радикальных изменений, в том числе и в сфере физической безопасности, и, осознавая ценность облачных технологий, компании рассчитывают использовать их для удовлетворения своих требований к безопасности и бизнесу.

Однако многие производители просто не готовы к этим изменениям на рынке и по-прежнему следуют бизнес-моделям, основанным на негибких запатентованных разработках. Переход к интеллектуальным решениям физической безопасности разительно контрастирует с этим традиционным подходом, что может создать определенные трудности. Хотя такие перемены не могут произойти в одночасье и новые решения с использованием облачных технологий еще не получили широкого распространения, этот яркий новый мир открывает новое поколение инженеров, которые только начинают работать в нашей сфере.

Таким образом, будущее СКУД и физической безопасности в целом будет основано на ожиданиях большей экономической выгоды. Системы контроля доступа станут точками сбора данных, а дверные контроллеры — интеллектуальными устройствами ввода-вывода. QR-коды для управления посетителями и биометрическое распознавание лиц будут все чаще управляться периферийными устройствами — с помощью аналитики в камере или датчике. Будущее СКУД обещает быть сложным, но интересным временем для тех, кто готов принять его и помочь сформировать его; это реальная возможность использовать инновационную деятельность для создания более разумного и безопасного мира.

В этом документе исследуются аспекты, имеющие особую важность для систем контроля доступа, в том числе многие принципиальные особенности таких систем. Также рассматриваются соображения о передовом опыте в отношении поставщиков, а также дается информация и предложения для конечных пользователей, чтобы помочь им уверенно ставить задачи поставщикам и принимать более осознанные решения о покупке.

3 Проблемы развивающегося рынка систем контроля доступа

Когда рассматриваются системы контроля физического доступа (СКУД), как правило, основное внимание уделяется факторам риска, связанным с предоставлением или блокировкой физического доступа. Важное значение имеет сбалансированный подход к проектированию системы контроля физического доступа с учетом оценки потенциальной угрозы.

В настоящее время, когда компании постоянно совершенствуют защиту своих объектов с помощью все более сложных решений электронного контроля доступа, эти системы позволяют быстро и эффективно управлять доступом в масштабах всей компании, оставляя цифровой след, который можно исследовать и при необходимости контролировать. Кроме того, эти системы можно полностью интегрировать с другими решениями, например с системами управления персоналом и посетителями.

При таком объединении систем, дающем ценную информацию, которая помогает принимать решения как в бизнесе, так и в сфере безопасности, а также контролировать доступ, решающее значение приобретает тщательная оценка зрелости компании в области кибербезопасности. Поскольку преступники становятся все более изощренными и постоянно появляются новые угрозы, стоит задача снизить риск клонирования учетных данных для доступа, а также риск внутрисистемных угроз и внешних кибератак.

При этом сама архитектура системы представляет собой проблему. Многие традиционные системы контроля доступа (СКУД) построены на устаревшей инфраструктуре. В условиях конвергенции технологий безопасности, обычно использующих эту инфраструктуру, поставщикам предстоит адаптировать свое оборудование для подключения к таким корпоративным сетям, а также осознать важность кибербезопасности и изменения обстановки в сфере безопасности, требующие тщательной оценки множества рисков, которым подвергается предприятие, и защиты от таких рисков.

Кибербезопасность должна быть ключевым фактором при разработке новых систем охраны и безопасности. Технологии контроля доступа являются неотъемлемой частью любого решения физической безопасности и поэтому должны производиться в соответствии с признанными принципами кибербезопасности, отчетностью об инцидентах и передовыми методами. Важно признать, что уровень защищенности сети определяется уровнем защищенности ее самого слабого звена. **Система, в которой это не учитывается,** становится уязвимой. Неготовность принять наличие слабых мест в системе, сообщить о них и предпринять необходимые меры в конечном итоге отрицательно скажется на способности системы обеспечивать надлежащий уровень физической безопасности.

3.1 Обеспечение кибербезопасности (зрелость в области кибербезопасности)

Увеличение роли IT-индустрии начинает менять характер и методы оценки, развертывания и обслуживания технологий. Ключевым моментом для заинтересованных сторон в сфере информационных технологий является оценка прочности системы кибербезопасности компании с акцентом на знания поставщика о кибербезопасности. Это знание также называют киберзрелостью. Киберзрелость предполагает хорошее понимание ландшафта угроз и мер по снижению рисков. Обширная документация и руководства по кибербезопасности, уже разработанные для сетевых камер, также могут применяться к системам СКУД, поскольку проблемы, оценки и объяснения киберрисков и потенциальных атак одинаково актуальны для этих продуктов.

3.2 Будущее архитектуры систем безопасности

Современные устройства контроля доступа подключаются через сетевые кабели и разъемы RJ45. Сети обеспечивают питание контроллеров доступа, а также передачу данных между устройствами и центральными системами управления. Определяющим фактором для контроля доступа является переход к системам на основе протокола TCP/IP. С момента появления в 2013 году первого дверного контроллера с поддержкой IP-технологий (AXIS A1001) архитектура PACS постоянно развивается, и теперь она предлагает множество усовершенствованных функций, которые были бы невозможны при использовании устаревших технологий.

Примеры таких инноваций включают считыватели QR-кодов для бесконтактного контроля доступа, распознавание лиц за счет интеграции с сетевыми камерами, а также считывание автомобильных номерных знаков. Все эти функции взаимодействуют с базами данных СКУД, позволяя периферийным устройствам принимать решения о предоставлении доступа или отказе в нем. Среди главных преимуществ IP-систем — низкие затраты на установку, простая настройка и легкость управления устройствами. Удобная интеграция с другими устройствами означает перспективное решение, обеспечивающее простое (по принципу «подключи и работай») подключение новых технологий и сервисов безопасности по мере их появления.

3.3 Сравнение IP-систем с традиционными системами контроля физического доступа

Преимущества IP-технологий будут реализованы в современных системах контроля доступа, особенно в бесконтактных системах, которые, как ожидают конечные пользователи, должны стать стандартом. Также пользователи хотели бы, чтобы эти системы были адаптированы к использованию смартфонов и планшетов и не только с мобильными идентификаторами. Каким образом отрасль будет предоставлять более качественные, более полезные и экономящие время и деньги системы контроля доступа? Сможет ли отрасль идти в ногу с циклами внедрения инноваций, за которыми стоят крупные технологические компании? Таковы проблемы, стоящие перед поставщиками систем.

До сих пор эти возможности не использовались, возможно, потому, что традиционные системы СКУД зависят от дверных контроллеров, установленных последовательно и подключенных кабелями RS-485 к центральному устройству или серверу. Большинство систем также являются проприетарными, что означает, что дверной контроллер «заблокирован» и им можно управлять только через программное обеспечение, указанное поставщиком. Это ограничивает конечного пользователя одним поставщиком оборудования и программного обеспечения, к тому же из-за сложности таких систем для их установки и настройки часто требуется квалифицированный персонал.

При расширении традиционных систем контроля доступа процесс осложняется тем, что типичный центральный контроллер предназначен для работы с определенным количеством дверей, а нестандартные конфигурации требуют больших затрат из-за ограниченной гибкости системы. Например, добавление лишь одной дополнительной двери может привести к неоправданно высоким затратам.

Сетевые технологии позволяют развернуть намного более простую и легкую в установке архитектуру СКУД, отличающуюся большей гибкостью и возможностью настройки. IT-специалисты предпочитают использовать в сетевых системах контроля доступа сетевые устройства. Включение этих специалистов в процесс проектирования СКУД в будущем является ключевым моментом, поскольку они могут обеспечить использование IP-устройств, которые также важны для снижения стоимости расширения системы и станут одним из требований для будущих проектов управления доступом.

3.4 Открытые протоколы

Будущее систем СКУД зависит от готовности производителей делиться своими навыками и умениями на форуме открытого протокола. Существует очевидное сопротивление этой открытости, поскольку многие разработчики систем контроля доступа, похоже, отдают предпочтение процессу, который привязывает конечных пользователей к их продукции, и тем самым гарантируют себе будущий доход. Однако в долгосрочной перспективе такой подход является проигрышным. Пользователи ожидают большего от своих решений и для этого готовы делиться своими данными.

Разработчики систем и поставщики оборудования для контроля доступа редко располагают ресурсами и IT-технологиями, позволяющими им предложить все решения в рамках комплексной системы физической безопасности. Многие, кажется, действительно не подозревают, что их товары и услуги быстро затмеваются новыми инновационными решениями, которые угрожают как их бизнес-модели, так и их положению на рынке СКУД. Возможности новейших систем и скорость современных инноваций таковы, что контроллеры доступа скоро станут ненужными — их заменят интеллектуальные устройства ввода-вывода.

Открытость позволяет создавать устройства для небольших систем контроля доступа, где простота имеет ключевое значение и где цена покупки и установки должна быть конкурентоспособной. Эти же устройства затем могут быть при необходимости адаптированы для более крупных и технически сложных систем. Такая гибкость является отличительной чертой современных средств обеспечения

безопасности и гарантирует, что системы, приобретенные сегодня, сохранят свою актуальность и в будущем, даже в условиях роста бизнеса и изменения требований пользователя.

Более подробную информацию об открытости и открытых технологиях можно найти на веб-сайте ONVIF *www.onvif.org*, отраслевой организации, созданной для разработки и продвижения концепции открытых стандартов.

4 Технические препятствия на пути к принятию новых технологий

Необходимо учитывать множество факторов с точки зрения технических соединений, интерфейсов и устройств, которые делают возможным цифровой контроль доступа. Переход от традиционных систем к облачным может привести к разным последствиям. В следующих разделах подробно описаны те моменты, которые необходимо учитывать, чтобы помочь существующей технологии и связанным с ней процессам не стать препятствием для модернизации и внедрения новых решений.

4.1 Контроллеры RS-485

Одним из важных факторов является развертывание контроллера RS-485 и потенциальный риск установки полуинтеллектуальных устройств, которые редко, если вообще когда-либо, имеют MAC-адрес, что затрудняет их идентификацию. RS-485, также известный как TIA-485(-A) или EIA-485, представляет собой стандарт, определяющий электрические характеристики генераторов и приемников для использования в системах последовательной связи. Электрическая сигнализация сбалансирована, многоточечные системы поддерживаются. Однако RS-485 определяет только физический уровень (генератор и приемник). Он не указывает и не рекомендует какой-либо протокол передачи данных.

Обратите внимание, что отсутствие MAC-адреса или принятие последовательной архитектуры само по себе не означает проблем с надежностью или негативным воздействием на работу системы контроля доступа: такие разработки были основным элементом СКУД более 30 лет. Тем не менее представить рост требований в сфере безопасности сложно, если каждое средство контроля в системе СКУД не является интеллектуальным и не может рассматриваться индивидуально. Мы утверждаем, что только полностью интеллектуальные системы и полностью доступные устройства могут в будущем принести реальную пользу. Необходимо отметить, что «полностью доступный» не означает низкий уровень кибербезопасности: как раз наоборот.

4.1.1 Открытый протокол контролируемых устройств (протокол OSDP)

Принятый Международной электротехнической комиссией (МЭК) новый метод связи, повышающий безопасность СКУД, — это открытый протокол контролируемых устройств (OSDP), стандарт связи для СКУД, разработанный Ассоциацией индустрии безопасности (SIA) для улучшения взаимодействия между устройствами контроля доступа и безопасности. OSDP использует 128-битное шифрование, поддерживает многоточечную установку и контролирует соединения, сообщая о проблемах считывания. Также следует отметить, что протокол OSDP поддерживает считыватели карт, дверные замки, контакты цепи сигнализации и функции запроса на выход, используя всего 2 провода, а не несколько соединений, которые ранее требовались для каждой двери. Как сообщается на веб-сайте SIA: «Протокол OSDP утвержден в качестве международного стандарта Международной электротехнической комиссией в мае 2020 года и опубликован как IEC 60839-11-5 в июле 2020 года. Протокол OSDP будет постоянно совершенствоваться, чтобы сохранять свои лидирующие позиции в отрасли».

4.2 Важность устройств с MAC-адресом

MAC-адрес — это уникальный аппаратный адрес сетевого адаптера или устройства. Применительно к IT-сетям MAC-адрес важен не менее IP-адреса. MAC-адрес однозначно идентифицирует компьютер в локальной сети и необходим для работы сетевых протоколов, в частности TCP/IP. MAC-адрес жестко запрограммирован в устройстве, и, хотя его можно подделать через операционную систему, делать это не рекомендуется. Более того, адрес должен быть защищен вашей системой безопасности.

Архитектура семейства протоколов TCP/IP и другие основные сетевые архитектуры обычно используют модель взаимодействия открытых систем OSI, в которой средства взаимодействия делятся на уровни. MAC-адреса функционируют на уровне канала передачи данных (уровень 2 в модели OSI) и позволяют компьютерам однозначно идентифицировать себя в сети. Фильтрация MAC-адресов добавляет дополнительный уровень безопасности. Прежде чем разрешить какому-либо устройству присоединиться к сети, маршрутизатор проверяет его MAC-адрес по списку одобренных адресов. Если адрес клиента есть в списке маршрутизатора, доступ предоставляется, в противном случае — запрещается.

4.2.1 Технология Power over Ethernet (PoE)

Технология PoE предлагает два преимущества, актуальные для всех областей ее применения: экономию средств на установку и гибкие варианты размещения устройств. PoE позволяет передавать данные и питание по одному кабелю, что означает возможность упростить архитектуру системы по сравнению с традиционными схемами. Стоит отметить, что многие системы контроля доступа рекламируются как использующие IP-технологии.

5 Отличительные черты передового опыта

Управление контролем доступа — важный компонент эффективного руководства потоком людей и ограничения допуска там, где это необходимо. Прошли те времена, когда запирание двери или установка шлагбаума были достаточными формами контроля доступа. Теперь компаниям требуются более совершенные системы контроля и управления доступом, чтобы улучшить отношения с клиентами и обеспечить постоянную безопасность людей. Применение основанного на передовом опыте подхода к комплексному контролю доступа выходит за рамки выбора правильных инструментов. Такой подход должен распространяться еще и на выбор правильной архитектуры, внедрение высококачественных технологий, соблюдение правильных процедур и протоколов, а также побуждение персонала и заинтересованных сторон к выработке надлежащего отношения и поведения.

5.1 Управление заинтересованными сторонами и конвергентный подход к безопасности

В то время как в технологической среде наблюдается тенденция к использованию объединенной инфраструктуры, которая позволит внедрять технологии, необходимые для бесперебойной работы компаний, нам также необходим объединенный («конвергентный») процесс принятия решений. Мы уже видели успешные примеры, когда конвергентный подход к безопасности разрушал стены и позволял объединять усилия разных команд. Такая конвергенция представляется как никогда актуальной именно сегодня, когда в корпоративных сетях сосуществуют бок о бок традиционные физические и электронные средства защиты.

Крайне важно, чтобы подразделения физической защиты могли полагаться на технологии, которые отвечают производственным требованиям их компании и устраняют связанные с ними риски, и в то же время поддерживают политики IT-безопасности и гарантируют, что физические устройства

не станут лазейкой в корпоративной сети. Объединение усилий всех заинтересованных сторон позволяет обеспечить физическую и кибербезопасность.

5.2 Чего ожидать от партнеров, продавцов и поставщиков

Необходимо обеспечить, чтобы третьи стороны понимали, как важно применять передовой опыт в сфере безопасности ко всей их деятельности, а также чтобы эти стороны действовали с учетом конкретных потребностей. Отношения с третьими сторонами имеют ключевое значение для создания эффективной цепочки поставок и выстраивания прочных и надежных связей.

Основные соображения при оценке третьих сторон и их влияния на цепочку поставок:

- Партнеры понимают и признают риски, связанные с кибербезопасностью
- Партнеры способны продемонстрировать зрелый подход к кибербезопасности и наличие соответствующих процессов и инструментов
- Они понимают значение нормативных и законодательных требований для своих предложений
- Они способны продемонстрировать, как будут реализовать требования клиента по соответствию нормативам
- Кибербезопасность - это не технология, а процесс; партнер может продемонстрировать процесс управления жизненным циклом, способный защитить предприятие клиента.

5.3 Управление безопасностью: процессы руководства и управления поставщиками

Как и любые другие эффективные виды обеспечения безопасности, кибербезопасность характеризуется степенью обеспечиваемой защиты. Речь идет о надлежащей защите сети IP-камер на всех уровнях: от выбора продукции и партнеров до установленных требований.

5.3.1 Стандарты и директивы

ISO 27001 — менеджмент информационной безопасности. ISO/IEC 27001 — это система управления безопасностью, включающая следующие требования:

- Систематическое изучение рисков информационной безопасности организации с учетом угроз, уязвимостей и воздействий
- Разработка и внедрение последовательного и всеобъемлющего пакета средств управления информационной безопасностью и/или других форм управления рисками (таких как предотвращение или передача рисков) для устранения тех рисков, которые считаются неприемлемыми
- Принятие общего процесса управления для обеспечения того, чтобы средства управления информационной безопасностью продолжали удовлетворять потребности организации в информационной безопасности на постоянной основе.

5.3.2 Cyber Essentials Plus

Cyber Essentials — это поддерживаемая правительством Великобритании и отраслевыми организациями схема сертификации, которая позволяет организациям защитить себя от распространенных сетевых угроз. Сертификат Cyber Essentials является эффективным показателем

компании, хорошо осознающей проблемы кибербезопасности, а также оценкой ее политики и процедур. При этом рассматриваются следующие аспекты:

- Безопасная конфигурация
- Контроль доступа и администрирование
- Защита от вредоносного ПО
- Управление исправлениями
- Брандмауэр и интернет-шлюзы

Для производителей технологий первой линией защиты должно быть снижение риска, связанного с их собственными системами. Начиная с 1 октября 2014 года правительство требует, чтобы все поставщики, участвующие в тендерах на заключение контрактов на обработку конфиденциальной и персональной информации, были сертифицированы в соответствии со схемой Cyber Essentials.

5.3.3 Безопасность в архитектуре, безопасность по умолчанию

Предложенная уполномоченным по камерам наблюдения в 2019 году концепция **«Безопасность в архитектуре, безопасность по умолчанию»** устанавливает минимальные требования для производителей систем и компонентов камер видеонаблюдения. Данный стандарт требует, чтобы производители применяли комплексный подход к решению проблем безопасности через поиск первопричин, а не устранение симптомов, и прилагали все необходимые усилия, чтобы уменьшить общий ущерб всей системе или ее компоненту.

Концепция «Безопасность в архитектуре, безопасность по умолчанию» предполагает долгосрочные технические усилия, направленные на то, чтобы в программное и аппаратное обеспечение встраивались базовые элементы безопасности. Более того, концепция охватывает столь же сложную задачу обеспечения доступности и востребованности этих базовых элементов на рынке.

Чтобы поддержать наши технологии, компания Axis объединила концепцию «Безопасность в архитектуре, безопасность по умолчанию» с Национальной стратегией кибербезопасности, реализовав следующие функции:

- Запрос пароля
- Индикатор надежности пароля
- Шифрование по протоколу HTTPS
- Стандарт 802.1x
- Удаленный доступ ОТКЛЮЧЕН (прохождение NAT)

6 Руководства и инструменты (процессы поставщиков)

Когда дело касается обеспечения безопасности сети, организации часто реализуют несколько технических средств контроля, чтобы создать «многоуровневую защиту», которая помогает свести к минимуму единые точки отказа и уязвимости. Однако есть важный процесс, который часто упускают из виду, — «усиление защиты системы», которое включает в себя внесение изменений в настройки системы по умолчанию, чтобы система была надежнее защищена от угроз информационной

безопасности. Кроме того, этот процесс помогает сократить количество внутренних уязвимостей, существующих во всех системах.

6.1 Руководство по усилению безопасности производства

Для всех подключенных к сети устройств (рабочих станций, серверов и т. п.) должен быть предусмотрен процесс усиления безопасности системы. Поскольку каждый производитель знает конфигурацию своей системы, как никто другой, он должен нести ответственность за предоставление партнерам и пользователям всей необходимой информации для защиты целостности их устройств и для установки этих устройств у конечного пользователя. Руководство по усилению безопасности должно содержать технические советы для всех, кто занимается развертыванием решений для охранного видеонаблюдения. В руководстве должна быть определена базовая конфигурация, а также предоставлена исчерпывающая информация о том, как бороться с возникающими угрозами.

В проектировании, разработке и тестировании своих устройств все поставщики должны применять передовой опыт в обеспечении кибербезопасности, позволяющий свести к минимуму возможные изъяны, которыми могут воспользоваться злоумышленники. Однако для защиты сети, устройств и сервисов, которые она поддерживает, требуется активное вовлечение всех участников цепочки поставки вплоть до конечного заказчика. Безопасность сетевой среды зависит от пользователей, технологических процессов и оборудования. Качественное руководство по усилению безопасности должно следовать версии 6.1 руководства по информационной безопасности CIS Controls, ранее известного как «Топ-20 самых важных защитных мер информационной безопасности» американского института SANS.

6.2 Управление устройствами

Диспетчер устройств — это локальный инструмент, который обеспечивает простой экономичный и безопасный способ управления подключенными устройствами. Для установщиков и системных администраторов диспетчер является высокоэффективным средством решения всех основных задач, связанных с установкой, обеспечением безопасности и обслуживанием устройств.

Инвентаризация устройств/система управления активами:

- Политика управления учетными данными и паролями
- Эффективная установка обновлений прошивки и приложений
- Применение средств управления кибербезопасностью — управление HTTPS и загрузка сертификатов IEEE 802.1x, управление учетными записями и паролями
- Управление жизненным циклом сертификатов — управление всеми основными задачами по установке, обеспечению безопасности и эксплуатации
- Простая и быстрая настройка новых устройств — настройка резервного копирования и восстановления
- Подходит для систем на объектах любых размеров — это может быть система видеонаблюдения, установленная как на одном охраняемом объекте, так и на нескольких объектах

6.3 Проблемы, связанные с OEM- и ODM-производителями

Производители оригинального оборудования (OEM) перепродают продукцию другой компании под своим собственным именем и торговой маркой. Производитель оригинального дизайна (ODM) самостоятельно разрабатывает и производит продукт, а затем продает его другой компании, которая продает его под своей торговой маркой. Такие производители позволяют компаниям заняться изготовлением товаров, не открывая реальное производство.

Решение производителей осуществлять OEM- или ODM-производство продукта другого поставщика имеет много плюсов. Во-первых, так устраняются любые производственные риски и затраты, и организация может сосредоточиться на продажах и маркетинге. Это одна из основных причин, по которой многие производители камер в индустрии безопасности занимаются OEM- или ODM-производством своей фирменной продукции.

Такая ситуация создает несколько проблем, и одна из самых очевидных — проблема кибербезопасности. Если один производитель выпустит продукцию с уязвимостью, это может повлиять на всех остальных торговых посредников и партнеров по всей цепочке поставок, а также затруднить обеспечение ее полной прозрачности. При значительном количестве OEM- и ODM-производителей конечный пользователь, проявивший должную осмотрительность и отказавшийся от технологий определенного производителя, может невольно использовать эти технологии под другим брендом, совершенно этого не осознавая.

6.4 Микропроцессорный чип

Очевидно, что стандартные микропроцессорные чипы, устанавливаемые в устройства, становятся мишенью хакеров, и при этом обнаруживается множество уязвимостей. Одна из основных причин этого — масштабируемость, которую они создают за счет единственной выявленной уязвимости. Недавние примеры включают ошибки Meltdown и Spectre: две связанные атаки по сторонним каналам на современные микропроцессоры. Эти уязвимости позволяют получить незаконный доступ к данным с использованием непривилегированного кода.

Уязвимыми (в той или иной степени) оказалось большинство устройств, от смартфонов до оборудования в центрах обработки данных. Основные поставщики операционных систем выпустили исправления, которые устраняют эти проблемы, хотя некоторые части исправлений необходимо устанавливать через OEM-производителя, поскольку они содержат платформозависимые элементы. Национальный центр кибербезопасности (NCSC) рекомендует вносить исправления как можно скорее.

6.5 Стратегия защиты прошивки

Прошивка с цифровой подписью имеет важное значение для конечных пользователей и снижает некоторые потенциальные риски взлома устройств на этапе логистики и/или распространения. При распространении к прошивке добавляется подпись, которую иногда называют хешем. Процессор вычисляет собственный хеш и загружает только тот образ прошивки, хеш которого соответствует хешу, подписанному сертификатом, которому он доверяет.

6.6 Контроль за уязвимостями

Продолжающийся рост киберпреступности и связанных с ней рисков заставляет многие организации уделять больше внимания информационной безопасности. Частью таких усилий по минимизации рисков информационной безопасности должен быть процесс контроля за уязвимостями, который позволит организации постоянно получать информацию об уязвимостях ее информационной среды и

связанных с ними рисках. Только путем выявления и устранения уязвимостей в информационной среде можно предотвратить проникновение злоумышленников в сети и кражу информации.

Важно, чтобы производители обеспечивали контроль за уязвимостями, включая процессы обнаружения и устранения уязвимостей во всех системах, а также предотвращения появления новых уязвимостей во время процессов преобразований и развертывания новых систем. Все проблемы, связанные с рисками, которые поставщик принимает на себя, должны быть доведены до сведения конечного пользователя и согласованы с ним. Если не придерживаться этого принципа, злоумышленники смогут эксплуатировать уязвимости в системах, проводя кибератаки против компании и ее поставщиков.

Обновления для исправления уязвимостей должны устанавливаться своевременно и только посредством утвержденного процесса, чтобы предотвратить любые нарушения безопасности. Если по какой-либо причине системы поставщиков не могут быть обновлены, необходимо принимать меры для защиты уязвимых систем. Все изменения должны производиться в соответствии с принятой поставщиком процедурой управления изменениями.

6.7 Уведомления с рекомендациями по безопасности

Рекомендации по безопасности помогают снизить риски, связанные с известными уязвимостями. Рекомендации по безопасности могут ссылаться на официальный общий перечень уязвимостей и рисков (CVE) или другие отчеты об уязвимостях и включают описание уязвимости, оценку рисков, советы и информацию о том, когда будет доступен сервисный релиз. Большинство производителей используют модель непрямых продаж и партнерскую программу.

Уведомления с рекомендациями по безопасности позволяют клиентам, не зарегистрированным в партнерской программе производителя, получать соответствующие уведомления о кибербезопасности при первой же возможности и при их передаче по каналу. Это важный инструмент для конечных пользователей, у которых установлено оборудование, но у которых нет договора с компанией, которая изначально произвела установку.

6.8 Модель Building Security in Maturity Model (BSIMM)

BSIMM (Создание безопасности в зрелой модели) — это модель измерения безопасности программного обеспечения, созданная для того, чтобы помочь организациям сравнить свою систему обеспечения безопасности ПО с другими системами. BSIMM помогает оценить процессы, действия, роли и обязанности в следующих областях:

- Проверка процессов проектирования и архитектуры
- Проверка кода
- Проверка на наличие известных уязвимостей
- Запуск стандартного инструмента сканирования уязвимостей, который может находить уязвимости из общего перечня уязвимостей и рисков (CVE) в пакетах с открытым исходным кодом

6.9 Долгосрочная поддержка

Долгосрочная поддержка — это политика управления жизненным циклом продукта, при которой стабильная версия программного обеспечения поддерживается дольше, чем стандартная версия. В рамках программы долгосрочной поддержки прошивки клиенты получают только исправления для

обеспечения стабильности, производительности и безопасности ПО. Поставщики предоставляют программу долгосрочной поддержки прошивки на срок до 10 лет с момента вывода устройства на рынок.

Ожидается, что программа долгосрочной поддержки будет существовать параллельно, но независимо от действующей активной поддержки программного обеспечения. Одно из ключевых преимуществ долгосрочной поддержки — возможность сохранить интеграцию с третьими сторонами, имеющими отношение к исходной версии прошивки.

6.10 Обучение и сотрудничество

Одна из ключевых областей, которую следует учитывать при выборе любого поставщика технологий, — это предоставление им обучения и поддержки. По мере изменения проблем, с которыми сталкиваются канал и отрасль, особенно в области кибербезопасности, производителям следует стремиться к заблаговременному поиску решений и обеспечивать рынок необходимыми материалами и контентом. Примеры такой поддержки:

- Бесплатные очные курсы по кибербезопасности
- Онлайн-тренинг по кибербезопасности
- Онлайн-тест по кибербезопасности
- Руководство по усилению безопасности
- Политика контроля за уязвимостями
- Передовой опыт в обеспечении кибербезопасности
- Базовые понятия и термины кибербезопасности

7 Создание кибергигиенического профиля: дальнейшие шаги и соображения

Качественная кибергигиена включает в себя идентификацию, приоритизацию и реагирование на риски, связанные с ключевыми услугами и продуктами организации. Внедрение передового опыта в области кибергигиены поможет предотвратить утечки данных и неправильную конфигурацию системы, а также минимизировать связанные с этим риски для бизнеса. Также важно заручиться согласием заинтересованных сторон по наиболее важным областям угроз, чтобы сосредоточиться на основных целях управления рисками.

Хотя здесь представлен далеко не исчерпывающий список, следующие соображения помогут повысить эффективность борьбы с киберугрозами.

7.1 Поставщики

Проверка регистрации и сертификатов

Проверяйте соответствующие регистрационные свидетельства и сертификаты: например, запрашивайте подтверждение соответствия стандартам ISO 9000 и других сертификатов качества. Установите, предназначена ли продукция поставщика для использования в корпоративной сети.

Подтверждение использования передового опыта

Убедитесь, что выбранный поставщик может продемонстрировать передовой опыт в области кибербезопасности. Он должен предоставить руководство по кибербезопасности, в котором описаны меры физической и кибербезопасности, а также передовой опыт по защите сети.

Аудит поставщика

Прежде чем брать на себя какие-либо обязательства по покупке, проведите тщательный аудит. Проверьте условия заключения сделки, чтобы убедиться, что они ясны и прозрачны. С финансовой точки зрения важно узнать у поставщика, что будет с продуктом и поддержкой, если у компании возникнут проблемы.

Определение ресурсов для постоянной поддержки

Выясните, есть ли у поставщика ресурсы для продолжения создания решений, которые, по вашему мнению, вам понадобятся в будущем. Убедитесь, что поставщик имеет необходимый масштаб, охват и возможности, чтобы учитывать ваши требования в будущем.

Определение будущих потребностей бизнеса

Сосредоточьтесь на своих потребностях в будущем. Интеллектуальные устройства и решения могут улучшить и подготовить бизнес к будущему, поэтому, заключая соглашения об обслуживании и постоянной поддержке, вы должны быть уверены, что поставщик оправдает или даже превзойдет ваши ожидания.

Требование проверки этических норм ведения бизнеса

Проверьте наличие устойчивой деловой практики с соблюдением этических норм. Сотрудничество, основанное на взаимном доверии и общих целях, — это прочный фундамент для долгосрочных отношений. Действуют ли у поставщика системы экологического менеджмента, программа корпоративной социальной ответственности и политика этического выбора поставщиков?

7.2 Продукты и системы

Проявление должной осмотрительности

Проведите технический аудит системы и ее основных элементов, чтобы убедиться в ее эффективности и отсутствии каких-либо факторов, которые могут повлиять на ее функционирование. Убедитесь в доступности и четком изложении информации по оценке и снижению рисков.

Проверка договора на техническое обслуживание

Проверьте, что входит в договор, например включает ли договор на сервисное и техническое обслуживание обновление программного обеспечения и прошивки.

Защита подключенных устройств

Убедитесь, что ваша сетевая система физической безопасности надежно защищена. Системы охраны следует развертывать с учетом кибербезопасности, в том числе с возможностью изменения имени пользователя и пароля по умолчанию, установки новейшей версии прошивки, использования шифрования (в идеале HTTPS) и отключения удаленного доступа.

Запрос заявления о безопасности архитектуры системы

Поставщик должен быть готов предоставить вам заявление о безопасности архитектуры системы в качестве доказательства кибербезопасности сетевых устройств.

Оценка интеллектуальности системы

Полностью интеллектуальные сетевые устройства имеют MAC-адрес, объединены в сеть и составляют неотъемлемую часть архитектуры системы. Устройства без MAC-адреса не являются интеллектуальными, их нельзя индивидуально идентифицировать, защитить и ими нельзя управлять.

Оценка соответствия Общему регламенту о защите данных (GDPR)/Закону о защите данных

Регламент GDPR вступил в силу в 2018 году вместе с обновленным Законом о защите данных 1998 года. Убедитесь, что продукты и системы поддерживают возможность соблюдения Закона о защите данных 2018 года и GDPR.

T10168631/RU/M3.2/2108

О компании Axis Communications

Компания Axis вносит весомый вклад в формирование более разумного и безопасного мира, разрабатывая решения, которые повышают безопасность и эффективность бизнеса. Занимая в отрасли технологий сетевого видео ведущие позиции, компания Axis поставляет решения для видеонаблюдения, контроля доступа, сетевых домофонов и звукового сопровождения. Эффективность наших решений повышается благодаря приложениям интеллектуальной аналитики и высококачественному обучению.

Около 4000 специалистов компании Axis трудятся более чем в 50 странах мира, вместе с нашими партнерами по технологиям и по системной интеграции разрабатывая и внедряя решения задач, стоящих перед клиентами по всему миру. Компания Axis была основана в 1984 году. Штаб-квартира компании находится в городе Лунд, Швеция