5. НАСТРОЙКА МАСШТАБИРУЕМОСТИ И БЕЗОПАСТНОСТИ СИСТЕМЫ

5.1 Конфигурирование параметров безопасности системы

Безопасность системы разделяется на 3 физический, сетевой, программный.

Реализация безопасности системы на физическом уровне заключается в осуществлении следующих пунктов:

– ограничен физический доступа в помещение, где расположен сервер–обработчик, путём запирающих устройств, ключи к которым находятся только у системного администратора, начальника отдела, курирующего данную системы;

– ограничен физический доступ к промежуточному сетевому оборудованию системы (коммутаторы, маршрутизаторы и т.п.), путём размещения их в помещениях/распределительных коробах, имеющих системы запирания и ключевой доступ;

– ограничен физический доступа к узлам подключения и настройки камер, путём монтажа, не допускающего доступ, без использования специализированных инструментов – внутренняя проводка;

– ограничен физический доступа к узлам питания всех элементов системы – прокладка линий питания напрямую в щиты электропитания, которые в свою очередь имеют запирающие устройства.

Сетевой уровень безопасности подразумевает отключения возможностей доступа к серверу–обработчику не через http порт, а также доступа к ip адресам камер и промежуточного оборудования, для этого выполняются следующие действия:

– у коммутаторов отключено использование не задействованных физических портов;

– включен фаервол на серверах–обработчиках, а также на сервере веб–интерфейса и базы данных;

– добавления в реестр разрешённых ip адресов – на сервере обработчике в реестр добавляются только ip адреса камер, с которых получает данные сервер, а также свеянного с ним сервера веб–интерфейса, также добавлен один ip адресс компьютера системного администратора;

– при развёртывании контейнеров в docker в файлах Dockerfile контейнеров в поле «ports» указывается ip адрес – 127.0.0.1, чтобы к

контейнерам был доступ только с хостинговой машины, кроме контейнера отвечающего за web часть системы;

– у промежуточного сетевого оборудования включено использование «white–list» ip адресов, в этот же список добавить только ip адреса устройств, используемых в системе;

– на сервере–обработчике для контейнеров, обрабатывающих данные с камер создана отдельная внутренняя сеть в «Docker», на сервере веб–интерфейса для контейнеров тоже создана отдельная подсеть в «Docker».

Программный уровень безопасности веб-интерфейса заключается в использовании механизма авторизации. При необходимости задействовать напрямую backend часть, то запрос на авторизацию вернёт ключ, который нужно будет отсылать в заглавии при каждом следующем запросе, для подтверждения полномочий на обработку запроса.

Так же в контейнерах, которые обрабатывают изображения с камер, будет использоваться специально созданный пользователь в базе данных, чтобы контейнер имел доступ только к необходимой информации. Данный пользователь будет обладать только следующими разрешениями: чтение списка биометрии лиц, добавление информации, об опознанном лице.

Так же благодаря использованию фреймфорка, исключена возможность атак с использование SQL–инъекций.

5.2 Проектирование вариантов масштабируемости и интеграции системы

Масштабируемость, в электронике и информатике, означает способность системы, сети или процесса справляться с увеличением рабочей нагрузки (увеличивать свою производительность) при добавлении ресурсов (обычно аппаратных). Масштабируемость – важный аспект электронных систем, программных комплексов, систем баз данных, маршрутизаторов, сетей и т. п., если для них требуется возможность работать под большой нагрузкой. Система называется масштабируемой, если она способна увеличивать производительность пропорционально дополнительным ресурсам. Масштабируемость можно оценить через отношение прироста производительности системы к приросту используемых ресурсов. Чем ближе это отношение к единице, тем лучше. Также под масштабируемостью понимается возможность наращивания дополнительных ресурсов без структурных изменений центрального узла системы [18].

В системе с плохой масштабируемостью добавление ресурсов приводит лишь к незначительному повышению производительности, а с некоторого «порогового» момента добавление ресурсов не даёт никакого полезного эффекта.

Она может быть:

– горизонтальной – разбиение системы на более мелкие структурные компоненты и разнесение их по отдельным физическим машинам (или их группам), и (или) увеличение количества серверов, параллельно выполняющих одну и ту же функцию. Масштабируемость в этом контексте означает возможность добавлять к системе новые узлы, серверы для увеличения общей производительности. Этот способ масштабирования может требовать внесения изменений в программы, чтобы программы могли в полной мере пользоваться возросшим количеством ресурсов;

– вертикальной – увеличение производительности каждого компонента системы с целью повышения общей производительности. Масштабируемость в этом контексте означает возможность заменять в существующей вычислительной системе компоненты более мощными и быстрыми по мере роста требований и развития технологий. Это самый простой способ масштабирования, так как не требует никаких изменений в прикладных программах, работающих на таких системах.

В разрабатываемой системе в основном используется горизонтальное масштабирование. Оно заключено в увеличении числа обрабатываемых. Данное действие может повлечь замену части оборудования либо увеличении его количество далее будут рассмотрены несколько наиболее вероятных вариантов масштабирования.

Добавление новых камер, на этажи, где уже развёрнута сеть – в данном случае затрагиваются следующие части системы:

– коммутатор, размещенный на этаже – у него могут закончится свободные порты подключения, тогда возможны 2 варианта:

– Замена коммутатора, на аналогичный по параметрам, но с большим числом подключаемых портов;

– Установка дополнительно коммутатора на этаже, который придётся либо подключать к уже установленному на этаже коммутатору. Либо подключить к серверному коммутатору, однако если у серверного не будет доступных портов, его тоже придётся заменить на схожий, но с большим числов портов.

– сервера–обработчики – для новой камеры необходимо будет разворачивать контейнер с программой обработчиком, но у серверов может

уже быть использован весь запас функциональности, в данном возможно 2 варианта действий:

– добавление ещё одного сервера–обработчика, что также может повлечь замены серверного коммутатора, при отсутствии свободных портов в оном.

– Увеличение производительности отдельного сервера обработчика, путём замены процессора и увеличения ОЗУ, однако материнская плата сервера может не поддерживать более производительные процессоры, что повлечёт за собой замену материнской платы из–за чего придётся перенастраивать весь сервер. Данный вариант действия является менее приоритетным.

Если все вышеизложенное действия по масштабированию связаны также с добавлением в систему ещё одной двери для контроля, до это также вызывает проблемы с добавлением контроллера этой двери в локальную сеть, т.к. у коммутатора контроллеров могу закончится порты, что потребует его замены на другую модель, с большим числом портов.

В качестве вертикального масштабирования используется замена вычислительных мощностей, на более производительные аналоги. А именно, замена материнской платы сервера, замена центрального процессора, замена оперативной памяти. Замена одного их перечисленных компонентов сервера может повлечь замену других компонентов.

Например, замена оперативной памяти может потребовать замену материнской платы, т.к. новая оперативная память может обладать более высокой частой памяти, нежели та частота, которую может поддерживать материнская плата. Так же схожая ситуация возникает, при решении, о замене оперативной памяти на более новое поколение, т.к. с каждым новым поколением частота памяти сильно возрастает.

Аналогичная ситуация складывается и при решении, о замене центрального процессора на более производительный. В разрабатываемом проекте ключевыми параметрами для процессора являются:

– максимальная частота – от данного параметра зависит скорость обработки данных, получаемых от камеры;

– максимальное количество потоков – параметр, который в проекте накладывает ограничения на количество обрабатываемых камер.

Т.к. максимальное число потоков процессора напрямую зависит от количества ядер процессора, то соответственно при росте числа ядер – возрастает число поддерживаемых потоков, что напрямую сказывается на

производительности процессора. На рисунке 21 мы можем видеть график роста производительности процессора при возрастании числа его ядер

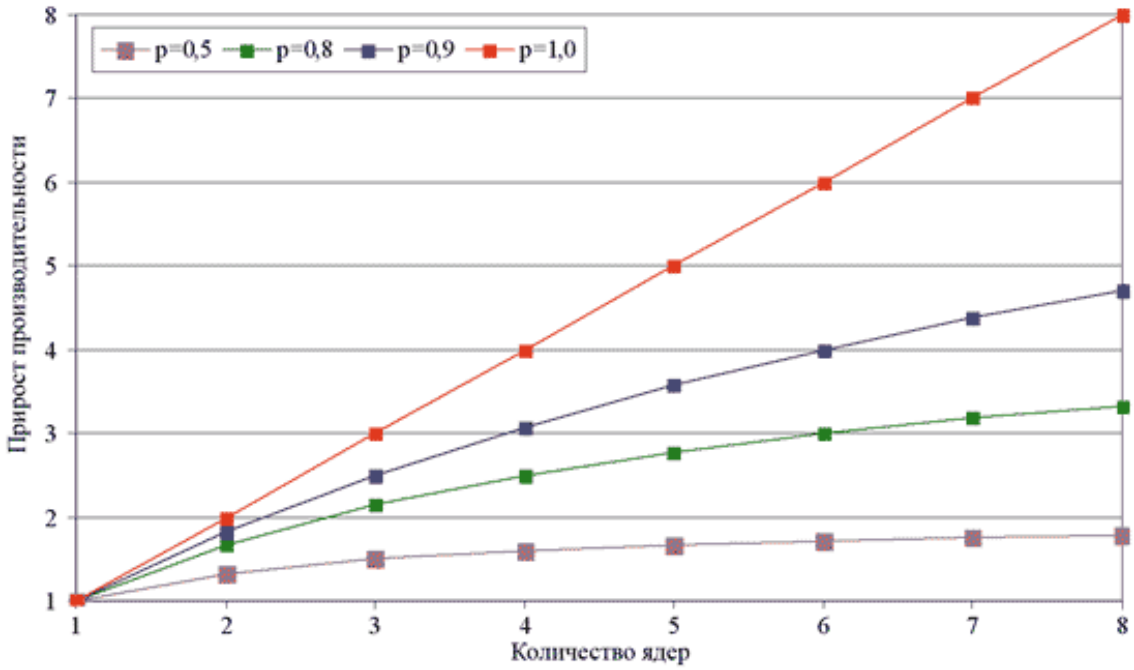

Рисунок 21 – График зависимости прироста производительности от числа ядер процессора.

Оба параметра взаимосвязаны, т.к. даже если заменять процессор на более производительный, но имеющий то же число максимальных потоков, то общая производительность системы не особо возрастёт. Однако, при замене, новый процессор выбирать исходя из увеличения количестве поддерживаемых потоков [19].

Интеграция данной системы затрагивает множество спектров работы предприятия, а т.к. система помогает решать задачи в двух сферах (безопасности и учёте рабочего времени сотрудников), то она затрагивает все спектры функционирования предприятия, но также это зависит от целей, ради которых внедряется данная система. Далее в данном пункте об интеграции системы будет рассмотрена исходя из этих целей.

Независимо от целей введения системы, потребуется интеграция системы в компьютерную сеть предприятия, это необходимо для осуществления доступа к базе данных системы с не хостинговой машины. Так же, системе нужен будет доступ в интернет, для скачивания необходимого программного обеспечения, но этот доступ необходим только на этапе установки и наладки система, а также при необходимости обновления программного обеспечения системы.

Необходимым является создание пользовательских учетных записей в базе данных для осуществления системы контролируемого доступа. Самым важным является добавление в базу данных системы изображений допущенных сотрудников.

При введении системы ради целей безопасности, то важным является интеграция системы в систему безопасности предприятия, это осуществляется разработкой программы, сканирующей базу данных системы на наличии людей в помещении, а также создание ролей для доступа в базу данных, обладающей необходимыми полномочиями (например, добавление записи, что помещение очищено, когда не сработала фиксация лица, вышедшего из помещения).

Так же, если необходимо использовать систему для использования её базы данных, для осуществления доступа в помещения, но интеграция заключается лишь в добавлении специализированной роли в базу данных системы, а также осуществить связь по сети предприятия между системами.

Если же система необходима для учета рабочего времени сотрудников, то для этого необходима интеграция базы данных системы в систему учета рабочего времени сотрудников, для чего необходимо создать в базе данных специализированную роль\и, а в системе учета рабочего времени лишь использовать «коннектор» подходящий под базу данных вводимой системы. Так же для этого можно использовать api–запросы, позволяющие получить туже информацию, что присутствует в веб–интерфейсе.

Вывод: Безопасность системы строится на использование встроенного функционала используемого оборудования и программного обеспечения. Для безопасности системы ограничивается доступ по каналам связи, также создание отдельных подсетей внутри общей сети системы позволяет для разграничения доступа к различным компонентам системы. Система поддерживает вертикальное и горизонтальное масштабирование. Горизонтальное выражено в виде увеличение количества оборудования, задействованного при расширении сети наблюдаемых проходов в помещения, что может вызвать замену уже использующегося оборудования. Вертикальное масштабирование заключается в повышении вычислительных мощностей оборудования, а именно серверов–обработчиков и сервера базы данных и веб–интерфейса. Вертикальное масштабирование выраженно в виде замены комплектующих серверов на более производительные варианты. Разрабатываемая система может быть интегрирована в другие систем предприятия, путём создания отдельных профиле доступа в базе данных системы и обеспечения физического доступа к базе данных.