базисы, используемые для каждого бита и если выбранные базисы совпали, биты считаются правильными и из них формируется общий секретный ключ, который может быть использован для дальнейшего шифрования сообщений. Возможные действия Евы в протоколе BB84 включают попытки перехвата битов через квантовый канал, однако ей сложно успешно прочитать сообщение, так как она не может влиять на выбор поляризации, и неправильные угадывания поляризации могут испортить данные, предупредив Алису и Боба о попытках перехвата. Активная атака на классический (открытый) канал связи может быть эффективным способом атаки, где Ева может представиться за Алису и перехватить сообщение, не вызывая подозрений, поэтому для надежности обмена информацией к каналам предъявляют следующие требования: информацию из квантового канала можно изменять, но нельзя подслушивать, информацию из открытого канала можно прослушивать, но нельзя изменять.

Протокол B92, предложенный в 1992 году, представляет собой метод квантовой криптографии, аналогичный протоколу BB84. В отличие от BB84, B92 использует только два квантовых состояния фотонов: вертикальную (0º) и диагональную (45º) поляризации. Протокол B92 не стал заменой BB84 из-за ряда недостатков, уменьшенную эффективность использования фотонов для генерации ключа и ряд трудностей в практической реализации, таких как оптические потери, а также высокие экономические затраты [1].

Протокол E91 представляет собой квантовый протокол распределения ключей, основанный на использовании запутанных пар фотонов. При реализации протокола отправитель создает пары фотонов в максимально запутанном состоянии и отправляет один фотон из каждой пары своему партнеру. Путем согласованных измерений Алисы и Боба на своих фотонах они сформируют общий секретный ключ [2].

Литература

1. Филиппов М. А., Кротова Е. Л. «Квантовая криптография. Протоколы квантовой криптографии // Вестник УрФО. Безопасность в информационной сфере. – 2017, № 4. – С.33-34.

2. Квантовая криптография – Википедия [Электронный ресурс]/ Википедия – свободная энциклопедия. – Режим доступа: https://ru.wikipedia.org/wiki/Квантовое_распределение_ключей – Дата доступа: 19.03.2024.

А. С. Демиденко
(ГГУ имени Ф. Скорины, Гомель)
Науч. рук. **О. М. Дерюжкова**, канд. физ.-мат. наук, доцент

ВЛИЯНИЕ БЕСПЛАТНЫХ ДЕЦЕНТРАЛИЗОВАННЫХ СЕТЕЙ ОБМЕНА ДАННЫМИ В БЕЛОРУССКОМ ОБЩЕСТВЕ И БИЗНЕСЕ

В 2000-х годах подключение сетевых технологий к абонентам привлекло внимание не только к использованию глобальной сети Интернет для доступа к мультимедийным возможностям, но и к потенциалу использования различных дополнительных функций в своих целях. Так для коммерческих организаций программно-сетевая связь его филиалов в единую сеть представляет особый интерес к обороту данных и его контролю, для быстрого и детального анализа данных представляющих в дальнейшем финансовую выгоду. Напротив же, тот кто использует «интернет для дома», был бы не против иметь доступ к своей домашней локальной сети для подключения к устройствам в составе умного дома.

С такими задачами призваны справляться централизованные и децентрализованные сети. Для централизованной сети основой является сетевая архитектура «клиент –

сервер», когда каждое устройство в сети получает данные и функциональные возможности от основного управляющего устройства. В децентрализованной сети каждый её участник имеет определённый доступ только к тем участникам, которые позволяют к ним подключиться.

В основном в Республике Беларусь большинство коммерческих структур для предоставления доступа к основным своим информационным ресурсам, используют выделенный провайдером в глобальной сети интернет – статический IP-адрес (рисунок 1). Такое решение предполагает ряд преимуществ и недостатков. Например, в качестве преимущества можно отметить возможности создания собственного WEB-сервера и VPN-сервера, а вот недостатками являются стоимость использования такого IP-адреса и его потенциальная уязвимость при кибератаках, так же на такую структуру особенно влияет скорость и бесперебойность предоставляемой услуги от провайдера.

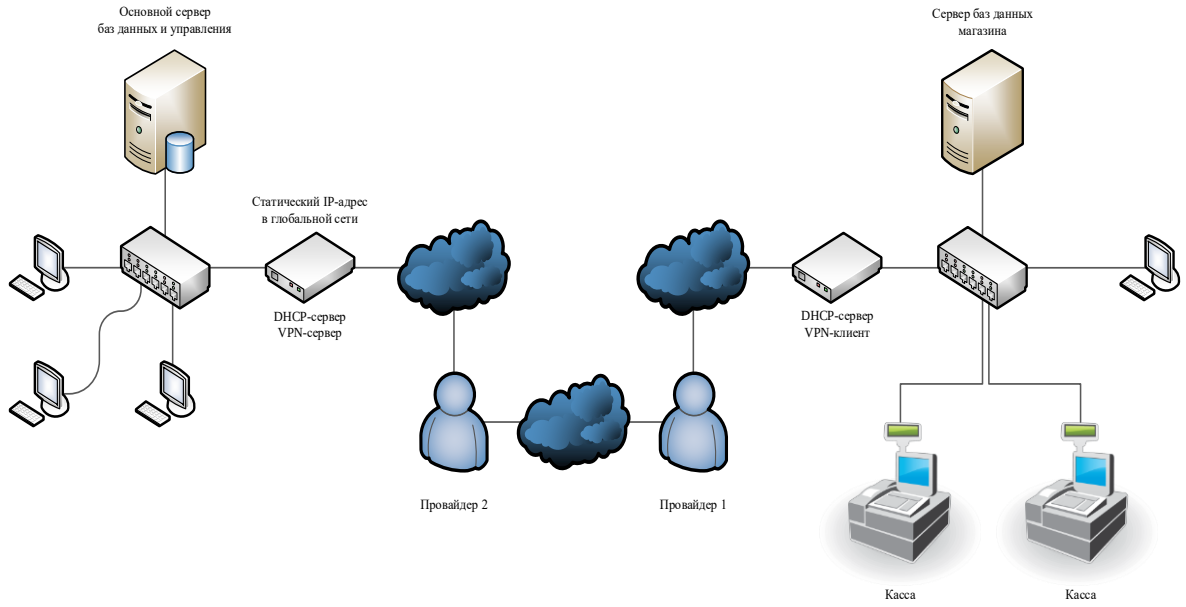

Рисунок 1 – Схема сети торговой организации

Альтернативой для связи между собой двух и более устройств при неполадках приведённой ранее системы являются бесплатные системы предоставления децентрализованной сети обмена данными. Таким образом, рассмотрим некоторые из них, которые могли бы быть применимы на практике в качестве альтернативы.

“Syncthing” – это бесплатное кроссплатформенное приложение для децентрализованной синхронизации файлов между устройствами. При создании новой папки в “Syncthing” данные автоматически синхронизируются между всеми подключенными устройствами, даже находящимися в разных сетях и далеко друг от друга [1]. Так, например, при использовании данного приложения без наличия в организации собственного статического IP-адреса в интернете, “Syncthing” позволяет использовать из выделенной папки различные файлы и данные из файлов в режиме “online” (рисунок 2). Такая же система будет интересна и обычным пользователям, для которых важна глобальная децентрализованная синхронизация данных между устройствами.

“ZeroTier” – это бесплатное кроссплатформенное решение, которое позволяет создавать децентрализованную частную сеть. Устройства напрямую соединяются друг с другом, что обеспечивает более высокую скорость, меньшую задержку и большую надежность. Для практического применения “ZeroTier”, стоит упомянуть, что создание такой сети возможно только после простой регистрации на сайте www.zerotier.com и установки приложения на устройство, которое хочет присоединиться к сети.

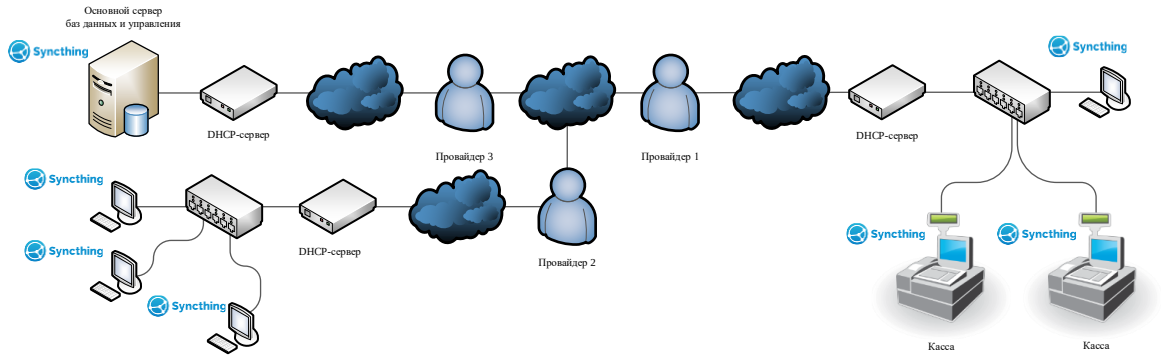

Рисунок 2 – Модифицированная схема сети торговой организации
с использованием “Syncthing”

Само приложение требует ввода ID-сети и разрешения доступа на сайте. “ZeroTier” автоматически децентрализованно выдает IP-адреса как DHCP-сервер, поэтому связь между устройствами осуществляется по имени устройства; а также по статическим IP-адресам, изменяемым в локальном сетевом интерфейсе “ZeroTier” либо через личный аккаунт на сайте www.zerotier.com (рисунок 3) [2].

Применение “ZeroTier” обычными пользователями домашних сетей представляет потенциальный интерес к его использованию для устройств интернет вещей в составе умного дома, а также в доступе к информационным данным и показателям с датчиков. Примечательно, что в использовании сетевых накопителей данных, как в самих устройствах (QNAP, Synology, WD), так и в программно-аппаратных комплексах (OpenWRT, DD-WRT) уже есть предустановка для использования “ZeroTier” в качестве децентрализованной системы сетевого доступа [3].

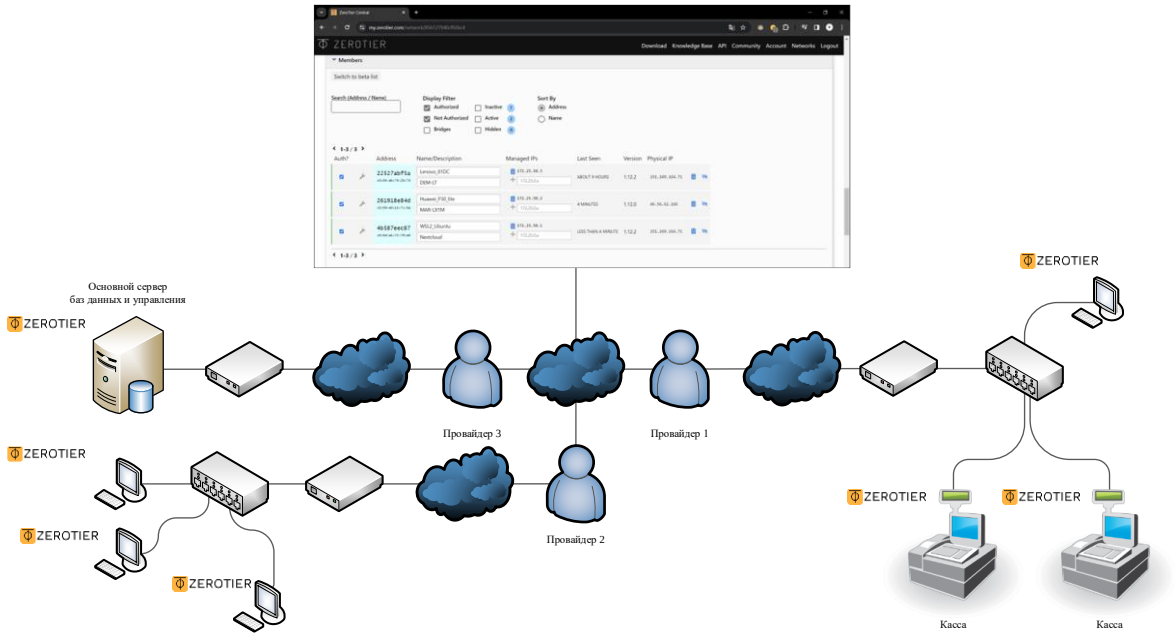

Рисунок 3 – Модифицированная схема сети торговой организации
с использованием “ZeroTier”

Таким образом, существует реальный практический интерес к мгновенному доступу из любой точки глобальной сети интернет. Перспективы применения децентрализованных сетей обмена данными, предоставляемых бесплатно в кроссплатформенных приложениях, уже имеют значительное влияние на современное белорусское общество и бизнес в целом.

Литература

1. Syncthing [Электронный ресурс] // Свободная энциклопедия Wikipedia. – URL: https://ru.wikipedia.org/wiki/Syncthing. – Дата доступа: 13.03.2024.
2. ZeroTier [Электронный ресурс] // Wikipedia, the free encyclopedia. – URL: https://en.wikipedia.org/wiki/ZeroTier. – Дата доступа: 13.03.2024.
3. Zerotier [Electronic sourse] // Adam Ierymenko. – URL: https://www.zerotier.com. – Дата доступа: 13.03.2024.

А. П. Денисов
(ГГУ имени Ф. Скорины, Гомель)
Науч. рук. **А. Н. Купо**, канд. физ.- мат. наук, доцент

РАЗРАБОТКА ПРОГРАММНО-АППАРАТНОГО КОМПЛЕКСА ДЛЯ УПРАВЛЕНИЯ МОДУЛЬНОЙ СИСТЕМОЙ

Автоматизированные модульные системы полива представляют собой инновационные решения для обеспечения эффективного и оптимального полива растений. С их помощью можно автоматизировать процесс полива, учитывая различные факторы, такие как потребности растений, погодные условия и влажность почвы. Однако, для удобного и эффективного управления такими системами необходимо разработать специализированное мобильное приложение, которое предоставит пользователям удобный инструмент для контроля и управления поливом.

В предыдущей версии устройства были использованы два процессора: ESP8266 и Arduino Mega. ESP использовалась для взаимодействия с мобильным приложением, а Arduino – для исполнения всех остальных функций. По данной причине, устройство обладало существенным недостатком – невозможностью обновить программу в ESP8266, поэтому для текущей версии была разработана приведенная ниже схема (рисунок 1).

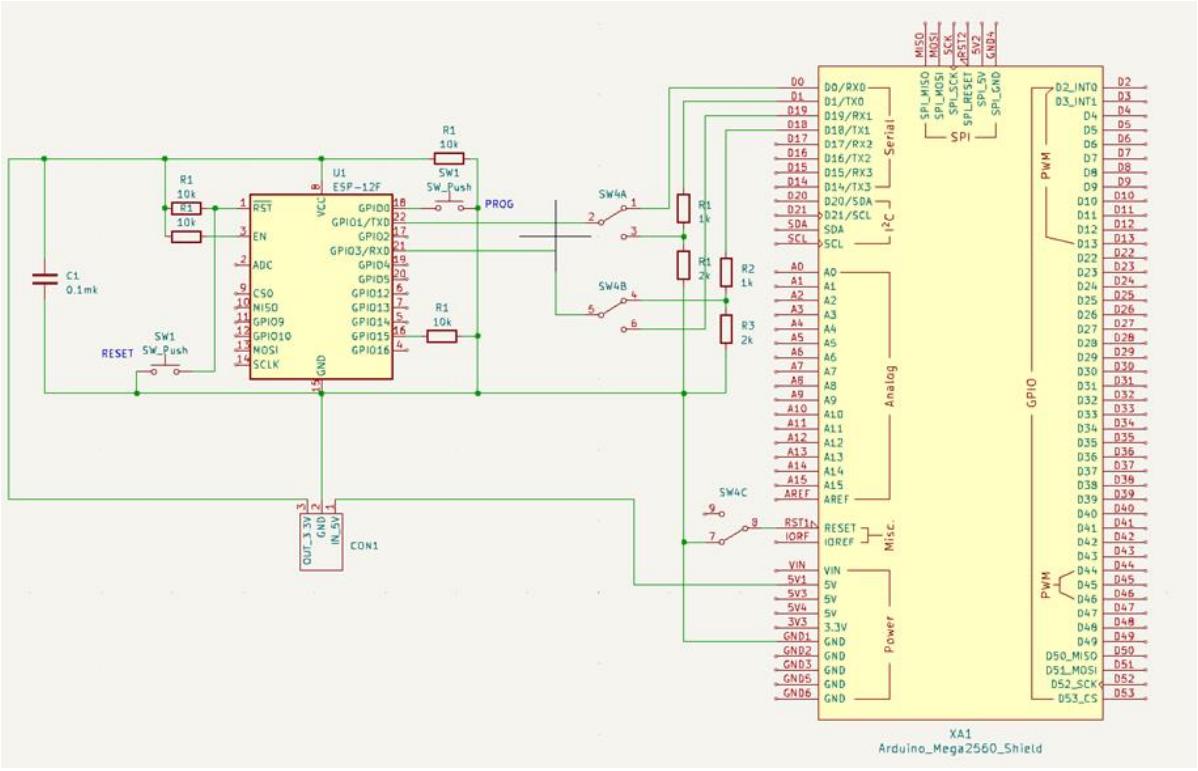

Рисунок 1 – Принципиальная схема устройства