ТЕХНОЛОГИЯ LI-FI КАК СРЕДСТВО ПОВЫШЕНИЯ БЕЗОПАСНОСТИ БЕСПРОВОДНОЙ КОРПОРАТИВНОЙ СЕТИ

Рычагов Кирилл Константинович

студент Самарского национального исследовательского университета имени академика С.П. Королева, РФ, г. Самара

Усков Максим Денисович

студент Самарского национального исследовательского университета имени академика С.П. Королева, РФ, г. Самара

Кузнецов Михаил Владимирович

научный руководитель, канд. техн. наук, доцент Самарского национального исследовательского университета имени академика С.П. Королева, РФ, г. Самара

Аннотация. В данной статье дана краткая характеристика Li-Fi технологии, проанализированы аспекты безопасности и уязвимости корпоративных сетей, реализованных с использованием Wi-Fi технологии, разработана концептуальная модель защищенной беспроводной сети с использованием Li-Fi технологии.

Abstract This article gives a brief description of the Li-Fi technology, analyzing the security aspects and vulnerabilities of corporate networks implemented using Wi-Fi technology; developing a conceptual model of a secure wireless network using Li-Fi technology.

Ключевые слова: технология Li-Fi, безопасность беспроводных сетей, уязвимости беспроводных сетей.

Keywords: Li-Fi technology, wireless network security, wireless network vulnerabilities.

Введение:

Очевидно, беспроводные технологии - это удобно для пользователей, поэтому их распространенность возрастает с каждым днем. Беспроводным сетям, основанным на Wi-Fi технологии, помимо вторжений из Интернета как минимум угрожает попытка "прощупывания" со стороны смежных помещений или площадей. В связи с этим развертывание беспроводной сети становится достаточно сложным вопросом с точки зрения информационной безопасности. Такую сеть вполне можно считать публичной, что повышает возможности реализации успешных атак злоумышленников. Таким образом, проблема заключается в поиске наименее уязвимой беспроводной технологии для использования в корпоративной сети. Целью данной работы является разработка концептуальной модели защищенной беспроводной сети организации.

Технология Li-Fi.

Технология Li-Fi появилась в 2010 году. Физик Харальд Хаас, преподающий в университете

Эдинбурга, основал проект «D-Light», а в 2011 году образовался «Li-Fi консорциум». В данной технологии используется видимый свет в открытом пространстве для передачи данных, обратная связь реализуется за счет ИК-излучения. На передатчик (LED-лампа) подается ток, модулирующий интенсивность света лампочки, при этом высокочастотная модуляция не заметна для человеческого глаза. Далее световой сигнал поступает на фотоприемник сетевого узла и преобразуется в электрический.

Основные преимущества технологии Li-Fi заключаются в отсутствии радиоволн, что позволяет использовать ее, например, на борту самолета или под водой (вода «глушит» радиосигналы), скорость передачи информации свыше 1Гбит/сек, а так же доступность и простота реализации.

Однако в этой технологии есть и очевидные недостатки: необходима прямая видимость между приемником и передатчиком, а при яркой засветке, например, солнечным светом, возможны ошибки при передаче данных.

Анализ проблемы избыточного покрытия.

В случае развёртывания сети Wi-Fi, злоумышленнику не составит особого труда получить доступ к сети за пределами контролируемой зоны (КЗ), если не обеспечена достаточная степень экранирования для поддержания необходимого уровня затухания сигнала на границах КЗ (рисунок 1).

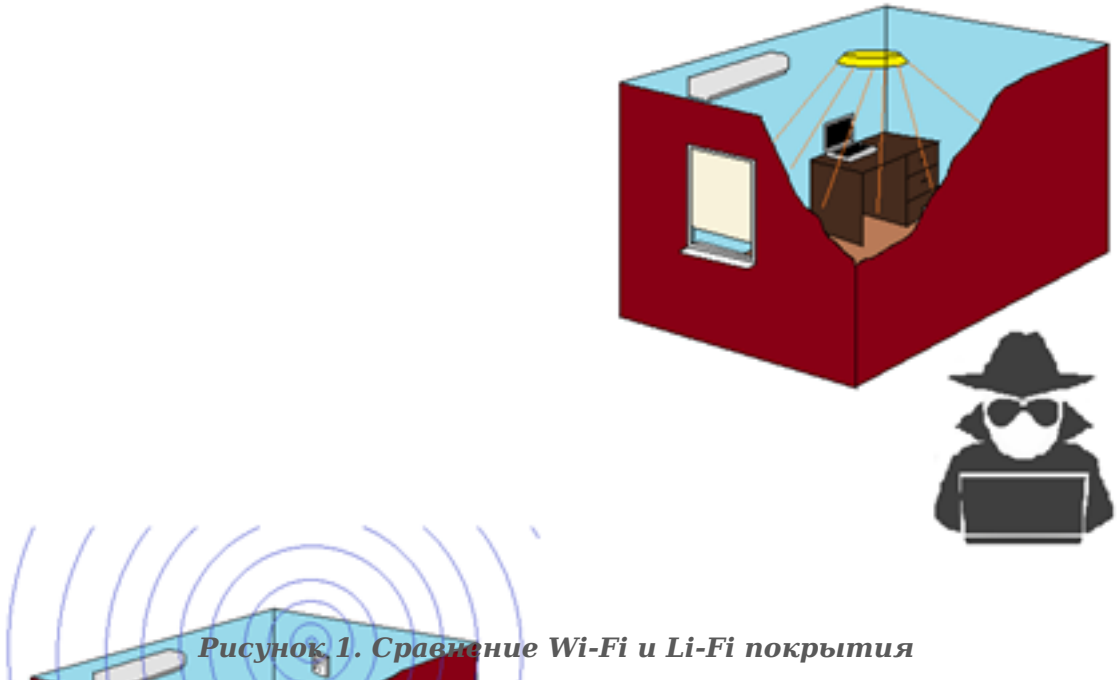

Рисунок 1. Сравнение Wi-Fi и Li-Fi покрытия

Решением данной проблемы будет уменьшение мощности сигнала или использование антенн заданной диаграммой направленности (рисунок 2), но проблема в том, что КЗ чаще всего имеет сложную пространственную архитектуру, что обычно затрудняет расчёт зоны покрытия радиосигнала.

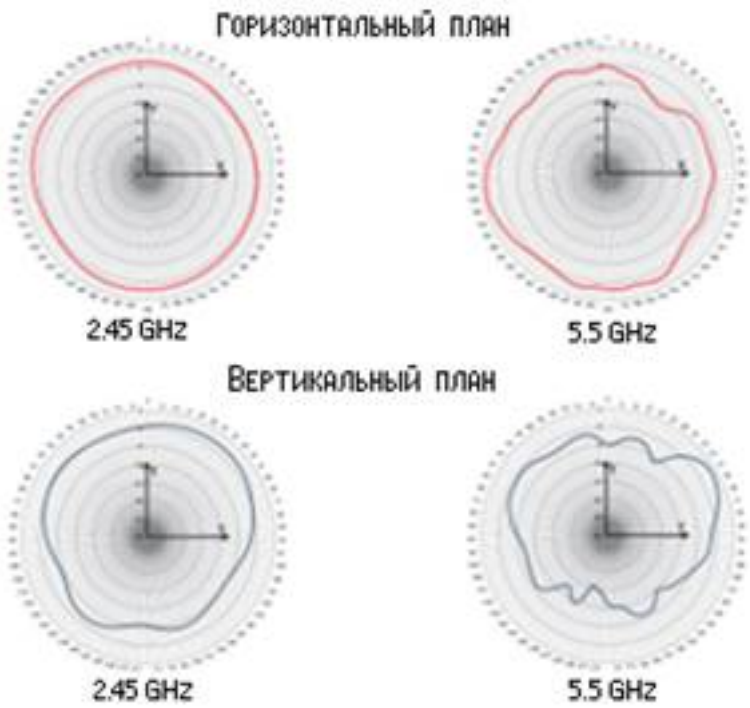

Рисунок 2. Пример диаграмм направленности Wi-Fi антенн, используемых для построения корпоративных сетей

При использовании технологии Li-Fi специальными LED-светильниками оборудуются только рабочие места легальных пользователей в КЗ. Таким образом, несанкционированный доступ

(НСД) извне практически невозможен при правильной модификации стеклопакетов, а именно использовании специальных фильтрующих покрытий.

Сценарии атак на беспроводные сети.

1) Развертывание поддельной точки доступа (ложный объект).

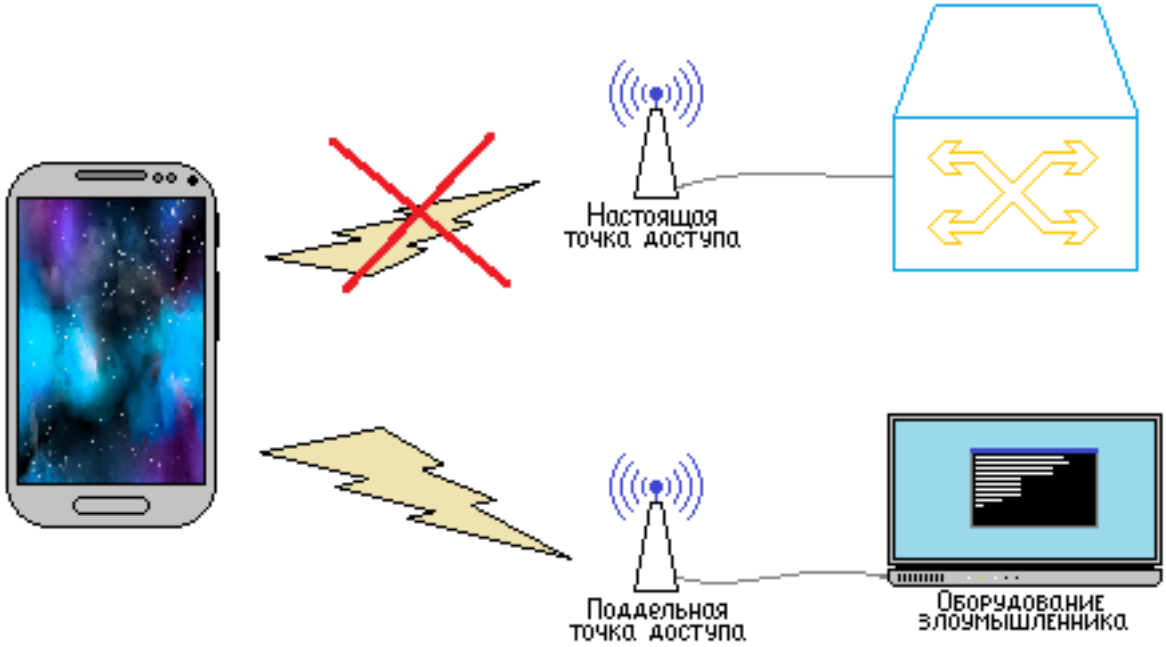

Рисунок 3. Развертывание поддельной точки доступа

Достаточно широко известная проблема стандарта Wi-Fi возникает при использовании уязвимого протокола аутентификации. Если у пользователя сохранена точка доступа и включено автоматическое подключение к Wi-Fi, кроме этого, на стороне пользователя не проверяется сертификат точки доступа (рисунок 3). Далее злоумышленник перехватывает значения хэш-сумм challenge – response, полученные при попытках аутентификации в поддельную сеть. Затем, путем анализа полученных аутентификационных данных за некоторое время работы поддельной точки доступа, методом перебора на оборудовании с высокой вычислительной мощностью, злоумышленник может получить пароль. Стоит отметить, что в случае с Wi-Fi ложной точке доступа достаточно быть в области контакта с пользовательскими устройствами. В случае же с Li-Fi, злоумышленнику практически невозможно получить доступ к монтажу ложной точки доступа, за исключением проникновения в КЗ в роли персонала или других сотрудников, проводящих ремонтные или диагностические работы.

2) НСД во внутреннюю сеть из гостевой.

Довольно часто в сети выделяют гостевой сегмент при отсутствии изоляции пользователей, сегментации внутренних сетей, и используя самые простые механизмы шифрования. Злоумышленник, получивший доступ к такой гостевой сети, имеет возможность атаковать устройство сотрудника, а затем через его аккаунт и внутреннюю локальную сеть. Стандартное решение данной проблемы включает в себя использование режима изоляции пользователей гостевой сети (настраивается на сетевом оборудовании), настройка запрета на использование гостевой сети сотрудниками компании, а также использование надежных механизмов шифрования.

3) Несанкционированные инсайдерские точки доступа.

Нередко пользователи организации используют для доступа в сеть собственные точки доступа (смартфоны или планшеты с функцией «режим модема»). В рамках организации данные точки доступа будут считаться несанкционированными. Вопрос защищенности таких «карманных» точек доступа лежит на самом владельце, в данном случае – сотруднике организации, и использование такой точки доступа ставит безопасность компании под угрозу. Злоумышленник может провести атаку на такую точку доступа и получить доступ к конфиденциальной информации сотрудника. Например, IP-адрес этого устройства. Может быть, что это IP-адрес крупного сотового оператора и с этого устройства был доступ к корпоративному аккаунту на сайте оператора, который осуществляется без ввода пароля. При этом доступ к личному кабинету позволял устанавливать переадресацию звонков, отправлять SMS-сообщения, а также получить доступ ко входящим SMS-сообщениям.

4) Использование механизма WPS (Wi-Fi Protected Setup).

Разработанный производителями Wi-Fi оборудования WPS стандарт упрощает подключение к беспроводной сети. С помощью WPS любой пользователь может быстро и просто настроить защищенную Wi-Fi сеть, не вникая в технические подробности и настройки шифрования. В данном механизме предусмотрено подключение с использованием PIN кода, который обычно печатается на наклейке роутера. Кроме этого, в настройках функции WPS можно задать PIN самому, с помощью которого так же можно подключать устройства, просто выбрав соответствующий способ подключения, и указав код. Опыт проведения тестов на проникновение международной компанией Positive Technologies в 2015 году говорит о том, что в 67% систем уровень защищенности беспроводных сетей оценивается как средний или ниже среднего. Среди выявленных недостатков стоит отметить использование механизма WPS для упрощения процесса настройки беспроводной сети («Статистика уязвимостей корпоративных информационных систем» 2016 года). Производят этот взлом при помощи вспомогательного ПО, подбирающего комбинацию PIN. Выходом в данной ситуации будет попросту не использовать этот упрощенный механизм доступа к Wi-Fi сети. Технология Li-Fi сейчас только начинает свое развитие, поэтому сложно сказать будет ли вообще реализован подобный механизм в Li-Fi Access Point. В любом случае, разработчикам стоит учитывать печальные с точки зрения безопасности недостатки WPS.

Проектирование концептуальной модели беспроводной сети.

На основе проведенного анализа была спроектирована следующая концептуальная модель с использованием технологии Li-Fi:

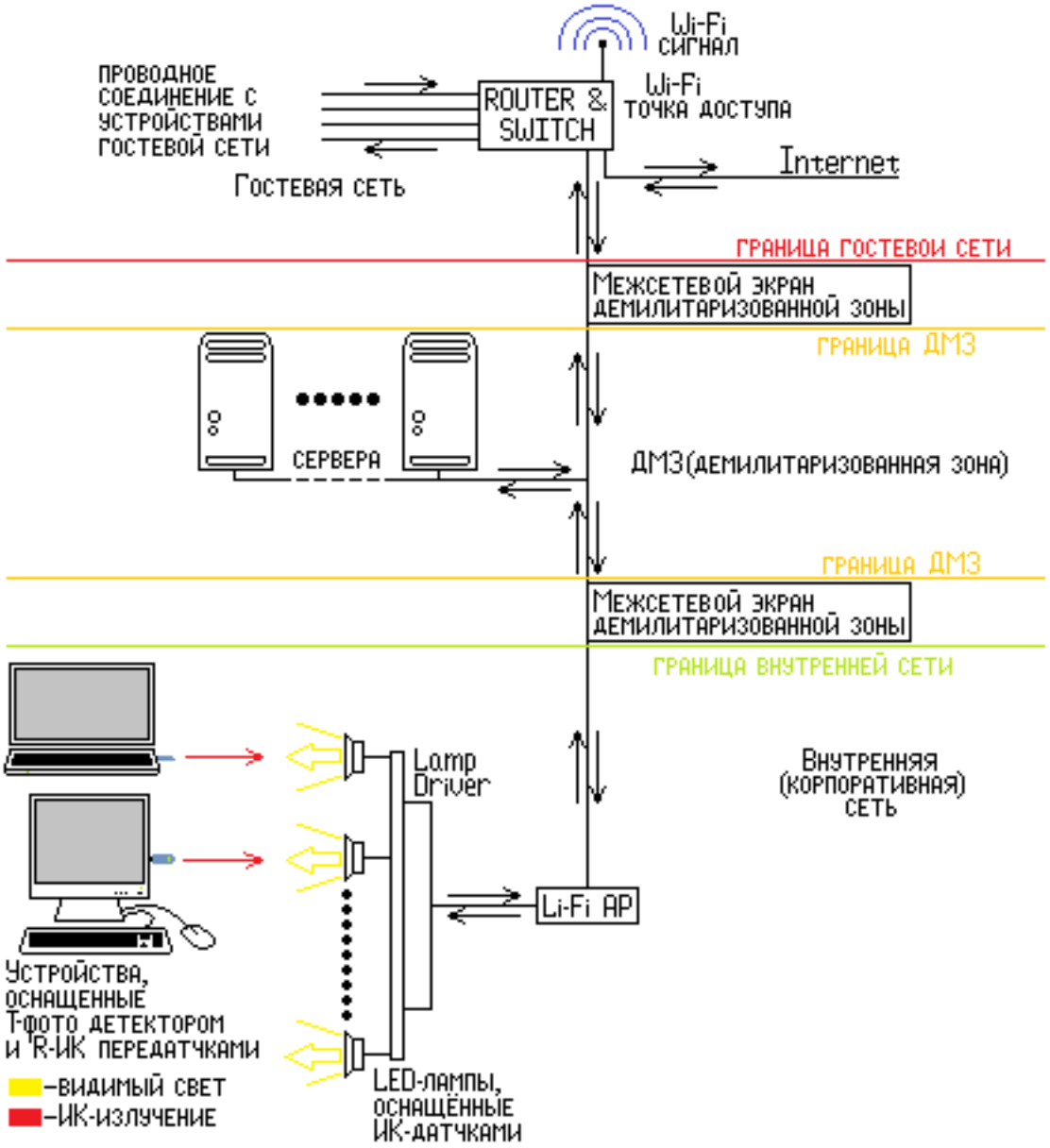

Рисунок 4. Концептуальная модель защищенной беспроводной сети

Гостевой сегмент сети представляет собой одну или совокупность нескольких точек доступа Wi-Fi с возможностью доступа в интернет, как в беспроводном, так и в кабельном формате. Демилитаризованной зоной (ДМЗ) в данном случае является сегмент сети, отделенный межсетевым экраном (МЭ) от интернета и внутренней локальной сети организации, в котором обычно располагаются сервера, которые должны быть доступны из интернета, например, почтовый - Microsoft Outlook. Цель создания ДМЗ – повышение уровня безопасности, который позволит минимизировать ущерб в случае успешной атаки (злоумышленник получит доступ только к оборудованию ДМЗ). Внутренний уровень (локальная сеть организации) будет реализован при помощи описанной ранее высокоскоростной и достаточно защищённой технологии Li-Fi. В данной модели мы использовали комбинацию двух МЭ: один из них контролирует соединения из внешней (гостевой) сети в ДМЗ, второй — из ДМЗ во внутреннюю сеть. Выбор этой конфигурации позволяет значительно повысить уровень безопасности спроектированной сети. Кроме этого на МЭ демилитаризованной зоны существует функция настройки правил фильтрации на уровне приложений, правильно настроив которую можно обеспечить еще более усиленную защиту локальной сети без негативного влияния на производительность внутреннего сегмента. Хотелось бы отметить, что при конструировании реальной системы желательно использовать МЭ различной архитектуры, что уменьшает вероятность существования одинаковой уязвимости.

Заключение.

В ходе работы была рассмотрена технология Li-Fi, ее значительные преимущества: как со стороны скорости, так и со стороны безопасности. Сравнив возможности покрытий Wi-Fi и Li-Fi, подведем итог: технология Li-Fi является наиболее безопасной для использования в качестве беспроводной внутренней сети организации. Проанализировав основные сценарии атак на беспроводные сети и методы их предотвращения, мы предложили собственную концептуальную модель беспроводной сети. При развертывании реальной сети необходимо соблюдать следующие меры безопасности: запрет на использование гостевой сети сотрудниками, режим изоляции пользователей точки доступа, надежные механизмы шифрования, безопасные методы аутентификации с проверкой сертификатов, обновление ПО на сетевом оборудовании и повышение осведомленности сотрудников в вопросах информационной безопасности.

Список литературы:

1. Путь к «сердцу» компании лежит через Wi-Fi – как работают злоумышленники – [Электронный ресурс] – Режим доступа. –URL: https://rb.ru/opinion/korporativnyj-wi-fi/ (дата обращения 01.12.2018).

2. Обзор вариантов организации доступа к сервисам корпоративной сети из Интернет – [Электронный ресурс] – Режим доступа. –URL: https://habr.com/post/302068/ (дата обращения 27.11.2018).

3. PureLiFi - – [Электронный ресурс] – Режим доступа. –URL: https://purelifi.com/technology/ (дата обращения 30.11.2018).