Чеботарев Алексей 015 гр.

Доклад по курсу «Защита Информации»

Защита информации в системах оптического излучения.

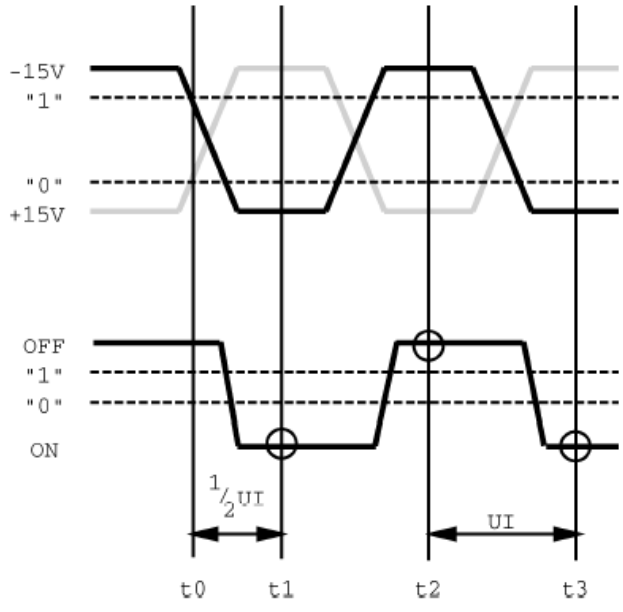
1. Введение

Может ли оптическое излучение от обычных светодиодов влиять на информационную безопасность? Современные средства передачи данных и даже некоторые устройства шифрования данных иногда излучают модулированные оптические сигналы, в которых содержится достаточное количество информации для злоумышленника, что бы восстановить исходные данные, направленные между передатчиком и приемником. Все что ему потребуется – небольшое устройство, расположенное неподалеку от излучения, совершенно незаметное для человека. Светодиод излучает пространственно-оптический сигнал, который можно считать на расстоянии, почти как оптоволокно, только без самого волокна.

2. Оптическое излучение.

Светодиод – надежный, дешевый и наиболее распространенный способ «излучать». Они используются почти во всех электронных устройствах, где необходим легко заметный индикатор. Особенно они себя зарекомендовали в устройствах передачи данных. Светодиоды очень быстры, они быстро изменяют свою яркость при изменении приложенного напряжения (доли наносекунд). Сразу появляется проблема: если светодиод довольно яркий, он может быть легко видим для злоумышленника с достаточно большого расстояния, чтобы стало возможным наблюдать все данные, проходящие через то или иное устройство. Преимущество светодиодов в том, что их можно заметить внутри комнаты, но является ли преимуществом то, что их можно также заметить снаружи - на другой стороне улицы, к примеру?

Рассмотрим идеализированный шифратор EIA/TIA-232E. На рисунке 1 сверху изображена форма последовательного сигнала данных этого устройства. Нижняя форма обозначает график полученный наблюдением (фотодатчиком) за его светодиодом.



Пока время переключения меньше половины t_{UI} светодиод довольно точно отображает сигнал устройства EIA/TIA-232E.

EIA/TIA-232E стандарт (ранее известный как RS-232) определяет последовательный формат битов, использую биполярную кодировку с несуществующим нулевым значением (может быть или только положительно или отрицательное значение). Биты передаются асинхронно с указательными битами «конца» и «начала» в последовательном потоке, для синхронизации между источником и приемником.

Рисунок 1

EIA/TIA-232E использует биполярную кодировку: отрицательное напряжение обозначает логическую «1», а положительное – «0». Во время того, пока данные не передаются, передатчик находится в состоянии «1».

3. Классификация оптического излучения

Удобно разбить оптические излучатели на 3 класса в соответствии с информацией передаваемой через них. Предлагаемая систематика показана в таблице.

Тип	Связанно с:	Уровень риска
Класс I	Состоянием устройства	Низкий
Класс II	Уровнем активности устройства	Средний
Класс III	Содержимым (данные)	Высокий

Классификация следующая:

- Класс I. Индикаторы не модулированные. Излучение источников этого типа постоянное и связанно с данным состоянием устройства или каналом связи. Индикаторы класса I по большей части просто сообщают пользователю о работоспособности или выполнении какого-нибудь поручения. Пример - индикатор работы машины (включено, выключено питание) или включение индикатора зарядки при вставлении аккумулятора в зарядное устройство.
- Класс II. Индикаторы модулированы по времени и показывают уровень активности устройства или канала связи. Индикаторы класса II обеспечивают злоумышленника гораздо большей информацией, чем индикаторы класса I. По сути, передаваемая информация не известна, но факт что что-то передается и приблизительный объем данных – налицо. Пример устройств класса II – индикатор активности на сетевых платах или индикатор на лицевой панели маршрутизатора Cisco.
- Класс III. Модулированные оптические сигналы, которые сильно связаны с передаваемыми данными. Если взаимосвязь достаточно хороша, тогда из анализа полученного излучения, возможно восстановить исходные данные. Пример устройств класса III удивительно обычны: индикаторы «посылаемые данные» и «принятые данные» на модеме.

Устройства класса III могут появляться из-за невнимательности разработчика. Например, с помощью изготавлимаего устройства нет необходимости передавать конфиденциальную информацию. Не понятно где есть такая ситуация, в которой установление индикатора этого класса было бы оправданно, за исключением случая, когда необходимо использовать канал с чрезвычайно низкой пропускной способностью, в котором можно наблюдать каждый переданный бит. В большинстве случаев канал связи имеет большую пропускную способность и человек не способен отследить передачу конкретного бита с помощью глаза. В настоящее время осциллограф более применимый инструмент, нежели индикатор класса III, по которому со стороны можно сказать только что он мигает. Потенциально опасные индикаторы, могут быть переделаны в индикаторы класса II, добавлением специального модулятора, растягивающего импульсы, в результате чего на выходе получается сигнал, связанный с входной последовательностью, но однозначно не дающий достаточной информации для восстановления исходного текста.

4. Обратная сторона устройств.

Оказывается что в некоторых типах шифровальных устройств, в частности автономных шифраторах и модемах уже со встроенными алгоритмами шифрования, могут испускаться оптические сигналы в незашифрованном виде.

На рисунке 2 показан DES шифратор, модель Infolock 2811-11. Infolock 2811 это шифратор, перерабатывающий данные в канале связи финансовых учреждений, в их проводных сетях. На рисунке показана передача пакета данных от терминального оборудования(DTE) – со стороны компьютера, к аппаратуре передачи данных(DCE) –

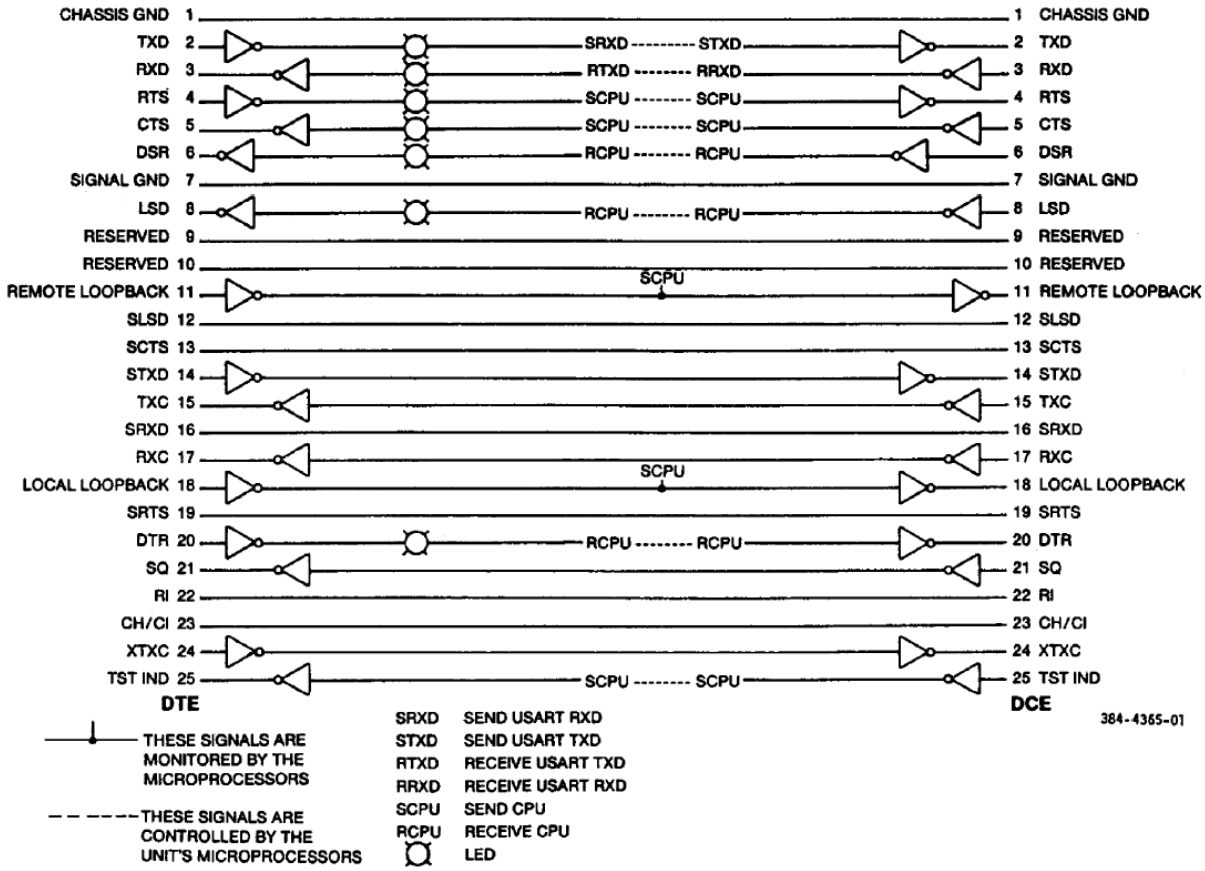


Рисунок 2

сторона, которая подключается к модему. DTE или красная сторона не зашифрована, DCE или черная сторона, зашифрована шифром министерства обороны (Department of Defense). Из схемы ясно, что светодиоды, находящиеся на каналах приема/получения данных находятся на красной стороне шифратора. Это серьезный недостаток разработчиков. Светодиоды отображают все данные, проходящие через устройство в незашифрованном виде.

Теоретически, любое устройство, шифрующее канал связи при использовании светодиодов может потенциально содержать этот недостаток. Модемы со встроенными система шифрования данных так же подвержены этой атаке. Автономные шифраторы, такие как Infolock 2811 защитят информацию на черной стороне, но уязвимы во время передачи информации. В результате получается утечка исходного текста. Что бы определить является ли конкретный шифратор уязвимым или нет, требуется исследование внутренней структуры каждого устройства в отдельности.

Не все источники оптического излучения проявляются естественным образом. Например, сетевая карточка. В ней, как правило, стоит светодиод второго класса. Предположим, что у пользователя системный блок стоит на столе, перед окном. Злоумышленник может находиться через дорогу напротив и читать все данные, проходящие через эту карту. Было проведено масса экспериментов, по обнаружению сигналов от светодиодов на больших расстояниях. Выяснилось, что однозначно могут быть определены данные, считываемые с 20 метрового расстояния. Если учесть, что современная техника быстро развивается, не только оптические датчики, но и обработчики радио-информации, то это расстояние может достигнуть порядка сотни метров.

Существуют вынужденные источники оптического излучения, т.е. такие которые могут быть использованы не по своему прямому назначению. Рассмотрим самую обыкновенную клавиатуру. Обычно она содержит 3 светодиода Caps Lock, Scroll Lock, Num Lock. Интересно то, что эти светодиоды не подключены непосредственно к кнопкам, а управляются программным путем. Т.е. при нажатии на Caps Lock, посылается сигнал в машину. Машина понимает, что нажата эта кнопка и посылает назад на клавиатуру сигнал светодиоду «гори». И он загорается. Скорость передачи информации между компьютером и клавиатурой 10 kb/s. Пропускная способность канала связи сильно превосходит возможности самого быстрого машинописца. По этому этот канал связи зачастую простаивает. И легко можно управляя светодиодами передавать любые данные.

Были проведены эксперименты. Данные передавались на скорости 500 бит/с по одному из светодиодов. Атаке подверглись следующие платформы (на всех она удалась): MS-DOS, Microsoft Windows 3.1, Windows 95, and Windows 98, Windows NT 3.5 and 4.0, and Sun Microsystems Solaris 2.5, 2.5.1, Solaris 7, and Trusted Solaris 2.5 and 2.5.1.

5. Оптоволокно.

Стало ясно, что непосредственная передача оптического сигнала очень не безопасна. До сих пор не удавалось сделать передатчик, который передает только в строго указанном направлении. Всегда есть какое то расхождение пучка, следовательно передаваемый сигнал может быть перехвачен. Поэтому искали путь с помощью которого можно было передавать сигнал со скоростью света, но по «защищенной траектории». Оптимальным решением оказалось оптоволокно, а волоконно-оптические системы передачи информации (ВОСПИ) зарекомендовали себя наилучшим образом.

Не будем останавливаться на преимуществах ВОСПИ, нас интересуют слабые стороны данного способа передачи информации. В оптоволокне утечка информации возможна за счет побочного электромагнитного излучения и наводок (ПЭМИН) как в радиочастотном, так и в оптическом диапазонах.

Рассмотрим простейшую модель ВОСПИ. Чаще всего в качестве излучательных элементов используются полупроводниковые устройства: светодиоды и лазеры. Светодиод имеет широкую диаграмму направленности, поэтому используется в многомодовых оптоволоконных системах с большим диаметром сердцевины. Лазеры в свою очередь, могут создавать более узкий, направленный пучок, с гораздо большей излучаемой мощностью. Зависимость типа излучателя определяется только потребностью канала связи: так светодиод подходит для канала с невысокой пропускной способностью.

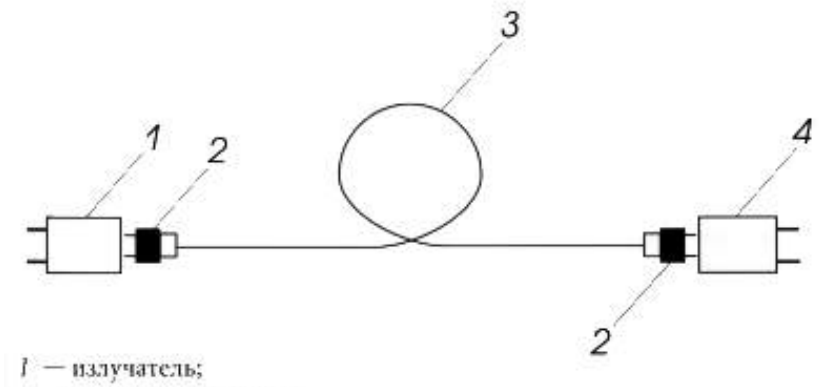


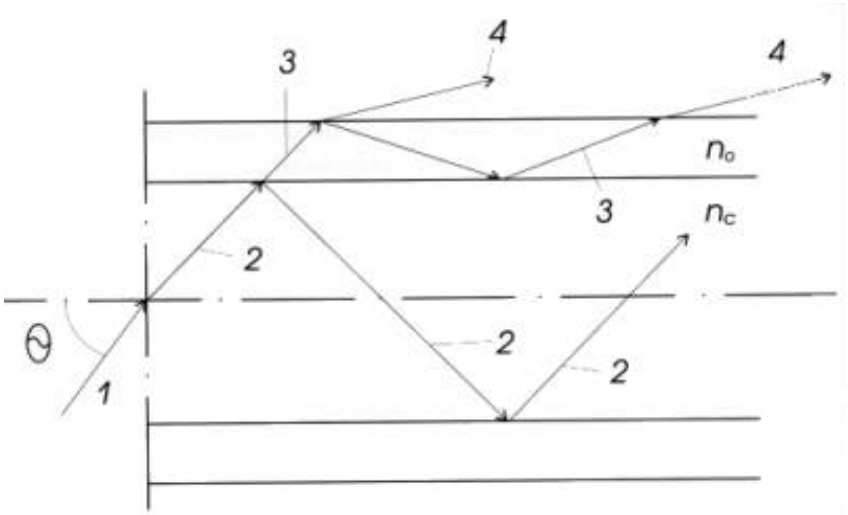
Рисунок 3

Рассмотрим причины, по которым возможно утечка информации:

- Несоответствие геометрических размеров окна (микролинзы) светодиода или лазера и торца (апертуры) волоконного световода.
- «Окна прозрачности» вокруг контактов на подложке, к которым подводится передаваемый информационный сигнал в радиочастотном диапазоне.

Эта утечка возможна как с сигнальной стороны, так и с приемной. Что бы исключить утечку информации, необходимо, чтобы их конструкция с физической точки зрения представляла собой абсолютно черное тело. Помимо утечки из контактирующих звеньев всего канала связи, утечка так же возможна посредством излучения информации самого оптоволокна.

Световоды делятся на многомодовые, маломодовые и одномодовые, кроме того, они бывают со ступенчатым и с градиентным показателем преломления. Рассмотрим структуру передаваемого сигнала через многомодовое волокно со ступенчатым показателем преломления.



Θ — угол ввода оптического сигнала в волокно;

n_c — показатель преломления сердцевины оптического волокна; n_0 — показатель преломления оболочки оптоволокна; 1 - траектория луча (моды), вводимого в волокно; 2 — траектория луча (моды) передаваемого оптического информационного сигнала по сердцевине волокна; 3 — траектория луча (моды), передаваемого по оболочке волокна; 4 — траектория вытекающего луча (моды).

Из рисунка становится ясно, что наиболее опасными с точки зрения утечки информации являются внешние слои волокна. Утечка составляет небольшую величину от величины передаваемого сигнала, но специальные высокочувствительные фотоприемные устройства могут принять передаваемый сигнал. Само по себе внешнее излучение довольно мало и его порой бывает сложно перехватить и обработать на практике. Но при нарушении структуры волокна потери и внешние излучения многократно усиливаются. Под нарушением структуры понимается появление микротрещин, вследствие физического воздействия. Более того, заметно увеличивается излучение в местах изгиба кабеля. При изгибах порядка диаметра сердцевины оптоволокна потери составляют величину сравнимую с самим сигналом. Из вышесказанного становится ясно, что не маловажно при прокладывании и изготовлении оптического волокна надо особое влияние уделять механической защите.

Важно рассматривать не только механические уровни защиты, но и так же параметры передачи данных. При достаточно больших частотах, почти вся энергия концентрируется в средней части световода, а с уменьшением частоты происходит перераспределение поля и уже большая часть энергии переходит во внешний слой. Существует некоторый порог частоты f_0 - «частота отсечки». Чем дальше значение частоты передаваемого сигнала от этой частоты, тем больше энергии «высвечивается» из волокна.

6. Заключение

При построении ВОСПИ для передачи конфиденциальной информации необходимо решить вопросы об условиях эксплуатации, средствах защиты. В качестве защиты можно использовать зашумление в оптическом диапазоне. Т.е. если злоумышленник пытается считать информацию за счет излучения, ему на его фотодатчики подаются специализированные шумовые сигналы значительные усложняющие ему жизнь.

В заключении отметим, что современные устройства обнаружения способны на многое и облегчают задачу взломщиков. Но и системы передачи и защиты информации развиваются в свою очередь, поэтому вопрос перехвата информации будет актуален всегда. Вопрос лишь в том кто будет прогрессировать с большей скоростью.

Литература:

Information Leakage from Optical Emanations
http://applied-math.org/

Безопасность оптоволоконных кабельных систем
http://kiev-security.org.ua/box/6/22.shtml

Защита информации в оптическом диапазоне частот
http://kiev-security.org.ua/box/8/122.shtml

Optical Time-Domain Eavesdropping Risks of CRT Displays
http://www.cl.cam.ac.uk/~mgk25/ieee02-optical.pdf