УДК 001.891.573
DOI: 10.30987/conferencearticle_5c19e60de0e465.61450093

Б.А. Тургунов, М.М. Халилов
(г. Фергана, Узбекистан, Ферганский филиал Ташкентского университета информационных технологий)

СОВРЕМЕННЫЕ СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИОННОГО СИГНАЛА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В ОПТИЧЕСКИХ СЕТЯХ

Рассмотрены современные способы защиты информационного сигнала от несанкционированного доступа в оптических сетях.

In this work, modern methods of protecting an information signal from unauthorized access in optical networks are considered.

Ключевые слова: информационная безопасность, несанкционированный доступ, защита информации.

Keywords: information security, illegal access, protection of information.

Кроме свойства огромной скорости передачи данных, оптические сети превосходят другие виды сети по возможности обеспечение более высокого степени информационной безопасности. Но придётся признаться, что с усовершенствованием технологии уже появляются все новые способы несанкционированного доступа на волоконно-оптические линии связи (ВОЛС). В связи с этим, в мире совершенствуются методы и средства обеспечения информационной безопасности в ВОЛС, предлагающие противодействия к современным техническим средствам несанкционированного съёма информации. Ниже проанализируем несколько способов, методов и средств обеспечения информационной безопасности в ВОЛС.

Один из известных способов – эта способ защиты информационного сигнала от несанкционированного доступа в волоконно-оптической линии связи путем формирования ограниченных по уровню мощности передаваемых информационных сигналов, ввода их в волоконно-оптическую линию связи, передачи по волоконно-оптической линии связи, приема на другом конце волоконно-оптической линии связи, измерения уровней принятых сигналов, обнаружения подключения к волоконно-оптической линии связи и формирования сигнала тревоги. Недостатком данного способа является высокая вероятность ложной тревоги, обусловленная низкой

точностью контроля затухания информационных сигналов в волоконно-оптической линии связи и нестабильностью их среднего уровня[1].

Следующий способ защиты информационного сигнала от несанкционированного доступа в волоконно-оптической линии связи заключающийся в обнаружении подключения к волоконно-оптической линии связи путем формирования ограниченных по уровню мощности информационного и контрольного оптических сигналов, ввода их в волоконно-оптическую линию связи, приема указанных сигналов, выделения контрольного сигнала и сравнения уровня его мощности с уровнем мощности опорного сигнала, обнаружения подключения к волоконно-оптической линии связи и формирования сигнала управления передачей информации. Недостатком этого способа является низкая эффективность защиты информации от несанкционированного доступа в волоконно-оптической линии связи, так как остается возможность несанкционированного подключения к волоконно-оптической линии связи и вывода из нее передаваемых информационного и контрольного оптических сигналов при высокой скрытности перехвата, особенно когда применяется метод оптического туннелирование съема информации.

Следующий способ защиты информационного сигнала от несанкционированного доступа в волоконно-оптической линии связи заключается в том, что формируют оптический сигнал передачи, состоящий из постоянного оптического излучения и информационного сигнала, передают оптический сигнал по волоконно-оптической линии, принимают, детектируют, усиливают, разделяют информационный сигнал и постоянный уровень, контролируют изменения от внесенных потерь. До передачи в оптический сигнал вводят контрольный сигнал, после приема и детектирования выделяют его, сравнивают амплитуду контрольного сигнала с пороговым уровнем. При снижении амплитуды контрольного сигнала относительно порогового уровня определяют попытку съема информации с волоконно-оптической линии передачи. Недостатком этого способа является так же низкая эффективность защиты информации от несанкционированного доступа в волоконно-оптической линии связи, при высокой скрытности перехвата [2].

Известен также способ защиты информационного сигнала от несанкционированного доступа в волоконно-оптической линии связи, заключающийся в том, что на передающей стороне волоконно-оптической

линии связи формируют исходный информационный сигнал и маскирующий синхросигнал, модулируют подлежащее передаче оптическое излучение, вводят в волоконно-оптическую линию связи передаваемое оптическое излучение, а на приемной стороне волоконно-оптической линии связи выводят из нее принимаемое оптическое излучение. Затем определяют уровень средней мощности принятого оптического излучения, выделяют маскирующий синхросигнал из принятого оптического излучения путем его демодуляции и фильтрации, формируют инверсный маскирующий синхросигнал, синхронизированный с выделенным маскирующим синхросигналом, модулируют инверсным маскирующим синхросигналом дополнительное вспомогательное оптическое излучение, устанавливают уровень средней мощности модулированного дополнительного вспомогательного оптического излучения равным уровню средней мощности принятого оптического излучения, формируют результирующее оптическое излучение путем смешивания принятого оптического излучения и модулированного дополнительного вспомогательного оптического излучения, после чего выделяют информационный сигнал из результирующего оптического излучения путем его демодуляции и фильтрации[3]. Недостатком этого способа является низкое качество принимаемой информации из-за неполной взаимной компенсации маскирующих синхросигналов в составе выделенного информационного сигнала.

Несмотря на существование упомянутых способов обеспечения информационной безопасности в ВОЛС, все еще не имеется ни одного способа, полностью защищающего информацию от нежелательного использования в ВОЛС.

Список литературы

1. *Шубин, В.* Информационная безопасность волоконно-оптических систем, 2015.

2. *M.P. Fok, Z. Wang, Y. Deng, P.R.* Prucnal, Optical layer security in fiber-optic networks, IEEE Trans. Inf. Secur. Forensics 6 (3) (2011) 712–726.

3. *P.R. Prucnal, B. Wu, B.J. Shasti.* “Secure communication in fiber-optic networks”, in: Emerging Trends in ICT Security, Elsevier, 2014.

Материал поступил в редколлегию 11.10.18.