# Угрозы информационной безопасности современных оптических транспортных сетей связи

С. С. Грищенко, А. Н. Иванин, Д. В. Субботин

*Военная академия связи, Санкт-Петербург*

sergeogri@yandex.ru, andreiivanin@gmail.ru, d1sub@yandex.ru

***Аннотация*. Обладая очевидными преимуществами, оптические сети связи повсеместно используются в интересах переноса мультисервисного трафика в интересах разнородных, распределенных систем управления (пользователей). На фоне высокой надежности и помехозащищенности остаются актуальными вопросы обеспечения устойчивости с учетом информационной безопасности физического и канального уровней оптических сетей.**

***Ключевые слова: оптические транспортные сети связи; информационная безопасность; сквозная архитектура защиты.***

## I. Современные оптические транспортные сети связи

С развитием информационных технологий и постоянным увеличением объема передаваемых данных растет значение оптических транспортных сетей связи. Применение волоконно-оптического кабеля обеспечивает высокую пропускную способность, низкую задержку и потерю данных, повышает стойкость к помехам, а также обладает хорошей масштабируемостью за счет возможности объединения большого количества узлов, расположенных на большом расстоянии друг от друга.

Современные оптические транспортные сети связи, как показано на рис. 1*а*,*в* [1], можно разделить на два основных типа: с технологией опто-электронного преобразования и так называемые прозрачные оптические сети. В тоже время использование различных технологий, таких как SDH (Synchronous Digital Hierarchy), PDH (Plesiochronous Digital Hierarchy), ATM (Asynchronous Transfer Mode), Ethernet, OTN (Optical Transport Network) и WDM (Wavelength Division Multiplexing), рис. 1*б*, обеспечивает различные уровни агрегирования и транспортировки данных, что позволяет поддерживать интеграцию различного типа трафика и добиться пропускной способности в сотни и тысячи Гбит/с.

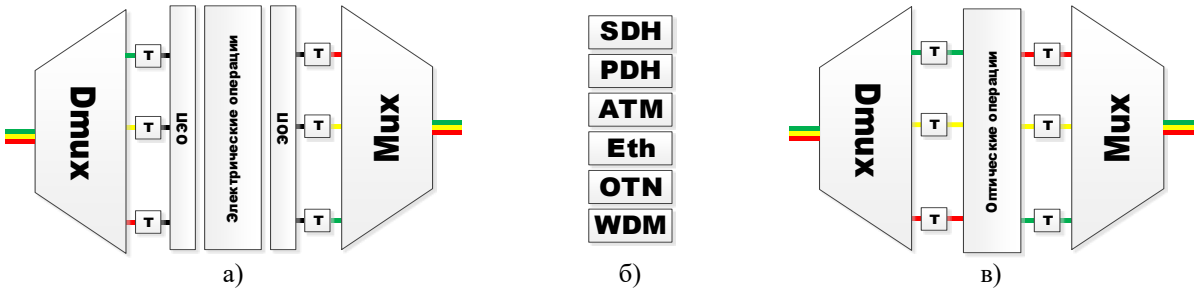
## II. Угрозы информационной безопасности

Оптические транспортные сети связи как объект, агрегирующий в себе большое количество разнородной информации, становится желанной целью злоумышленника для возможного нанесения ущерба, дополнительно усугубляет факт относительно легкой доступности оптических линий связи, прокладываемых за пределами контролируемых зон.

Проводя анализ нормативных документов в области информационной безопасности, в частности банка данных, угроз безопасности информации и уязвимостей [2], содержащий 222 угрозы безопасности информации и 55721 уязвимостей, стоит отметить, что значительная часть из них направлена на идентификацию и классификацию угроз безопасности уровня приложений и мало затрагивают физический и канальный уровни, в том числе оптические транспортные сети связи. Можно предположить, что это связано с отсутствием нормативных документов, что делает исследования в данном направлении актуальным.

Так, в проекции на угрозы информационной безопасности оптические транспортные сети связи можно представить, как сложную сквозную архитектуру [3] на рис. 2, состоящую из уровней:

- инфраструктура – составные элементы оптических транспортных узлов связи (мультиплексоры, усилители, муфты, оптические линии связи, демультиплексоры);
- каналы – STM (Synchronous Transport Module), E (1-4), Ethernet, OTN и другие;
- приложения – протоколы и управления сетью Telnet, SSH (Secure Shell), SNMP (Simple Network Management Protocol), HTTP (Hypertext Transfer Protocol).




а) б) в)

Рис. 1. (а, в) Строение современных оптических сетей связи, б) применяемые технологии

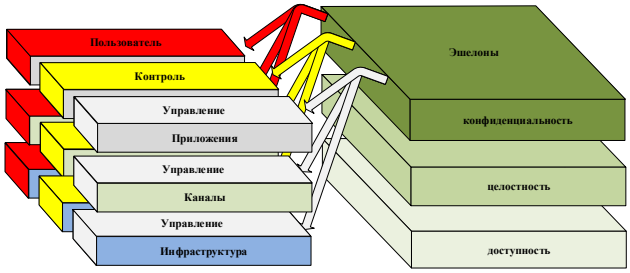



Рис. 2. Сквозная архитектура защиты оптических транспортных сетей

При этом сами уровни разделяются на плоскости управления оптическими транспортными сетями, контроль – мониторинг основных параметров и плоскость конечного пользователя, выраженные через информацию, передаваемую по различным видам услуг связи.

Таким образом, для получения доступа к информации, циркулирующей на уровне приложений, злоумышленнику необходимо провести многоэтапную атаку по преодолению всех эшелонов защиты на каждом уровне, начиная с доступа к оптическому волокну.

Классификация получения несанкционированного доступа к оптическому волокну [4, 5] представлена на рис. 3 и разделена на доступ в точках подключения к телекоммуникационному оборудованию или непосредственно на самой линии связи, при этом доступ к оптическому информационному сигналу возможно осуществить как без нарушения целостности оптического волокна, путем растворения оптических волокон, так и с нарушением, путем монтирования сплиттера для ответвления части оптического сигнала.

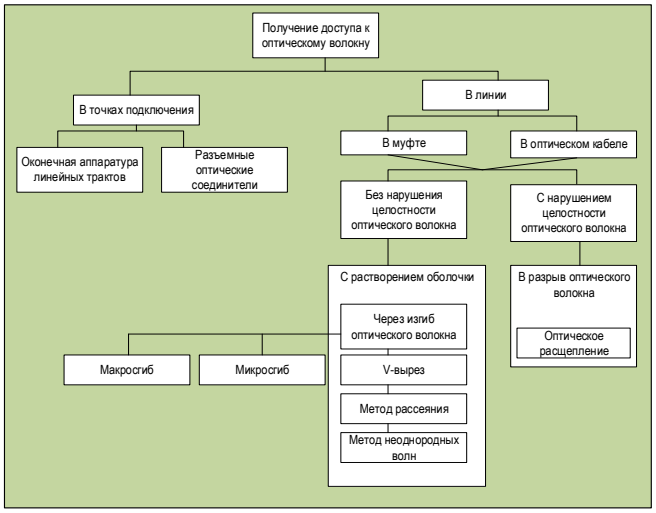



Рис. 3. Несанкционированный доступ к оптическому волокну

При получении доступа к оптическому сигналу злоумышленник, в зависимости от преследуемых целей (нарушение конфиденциальности или доступности канала), может провести различные атаки, используя нелинейные эффекты в оптическом волокне, представленные на рис. 4.

Так, используя эффекты фазовой самомодуляции и кроссмодуляции [6], внося искажения в профиль передаваемого сигнала, можно добиться изменений в оптических каналах, которые могут привести к интермодуляционным искажениям, нарушая доступность канала связи. Кроме того, использование явления четырёхволнового смешения [7] открывает возможности перехвата или подавления сигналов, тем самым нарушая его конфиденциальность.

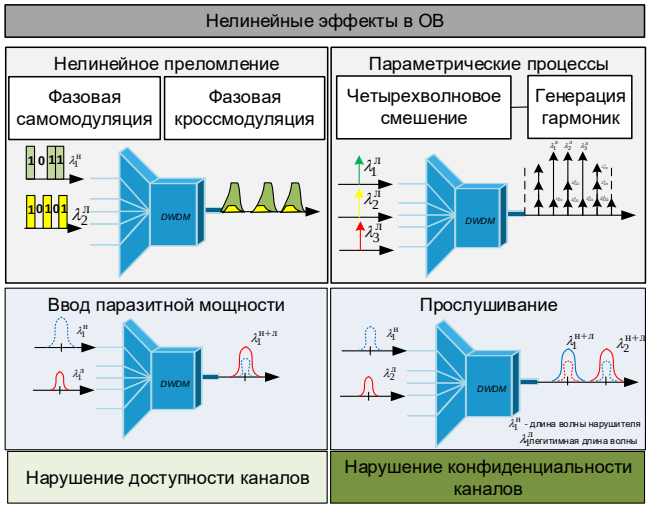



Рис. 4. Связь нелинейных эффектов оптического волокна и проводимых атак на каналы связи

## III. Заключение

В рамках анализа угроз информационной безопасности современных оптических транспортных сетей связи, показана необходимость тщательного изучения возможных атак, осуществляемых на физическом и канальном уровнях. Сложность и высокая стоимость мониторинга оптических параметров в режиме реального времени заставляет учитывать данные угрозы и исследовать пути по формированию механизмов повышения защищенности и устойчивости оптических транспортных сетей связи.

## Список литературы

[1] Jean-Francouis Labourdette. Tellium, opaque and transparent networking // Optical Networks Magazine, 2003.

[2] Банк данных угроз безопасности информации. [Электронный ресурс] // ФСТЭК России URL:https://bdu.fstec.ru/threat (дата обращения 25.03.2024)

[3] К вопросу об идентификации компьютерных атак на транспортную сеть связи специального назначения / А.К. Канаев, А.Н. Иванин, Д.В. Субботин, К.П. Щербак // Региональная информатика и информационная безопасность. Том Выпуск 7. Санкт-Петербург, 2019. С. 44-46.

[4] Spurny V., Munster P., Tomasov A., Horvath T., Skaljo E. Physical Layer Components Security Risks in Optical Fiber Infrastructures // Sensors 2022, 22, 588.

[5] Гришачев В.В. Перехват трафика в оптических сетях: метод оптического туннелирования // Фотоника. Выпуск #8/2020. Москва, 2020. С. 680-695.

[6] Antwiwaa A., Kumar A., Jaiswal A.K. Source based Security Issues in WDM Systems // International Journal of Electrical and Computer Engineering (IJECE). Vol. 7, No. 4, August 2017, pp. 2101~2108.

[7] Anita Antwiwaa, Seth Okyere-Dankwa, Mensah Sitti and Anil Kumar. Four-Wave Mixing Effect and Its Security Implications on a WDM System // 2020 International Journal of Technology and Management Research ISSN 2026. 64802020; 5(4): 1−11.