DOI 10.37882/2223-2966.2025.05-2.08

МЕТОДИКА ПОВЫШЕНИЯ УСТОЙЧИВОСТИ ОПТИЧЕСКИХ ТРАНСПОРТНЫХ СЕТЕЙ СВЯЗИ В УСЛОВИЯХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВОЗНИКАЮЩИХ НА ФИЗИЧЕСКОМ И КАНАЛЬНОМ УРОВНЯХ

A TECHNIQUE FOR INCREASING THE STABILITY OF OPTICAL TRANSPORT COMMUNICATION NETWORKS IN THE CONTEXT OF INFORMATION SECURITY THREATS ARISING AT THE PHYSICAL AND CHANNEL LEVELS

S. Grishchenko
A. Ivanin

Summary. The article discusses a technique for increasing the stability of special-purpose optical transport communication networks (STS SN) in the context of information security threats. An integrated approach based on the use of machine learning methods and hidden Markov models (SMM) is proposed, which reduces the time required to detect attacks at the physical and channel levels. A model of the network status and attack classification has been developed, as well as an algorithm for taking preventive measures. The results obtained contribute to improving the survivability and reliability of networks within the critical information infrastructure.

Keywords: stability, information security, optical transport networks, neural networks, hidden Markov model, EMVOS, critical information infrastructure.

Грищенко Сергей Сергеевич
Адъюнкт, Военная академия связи им. Маршала Советского Союза С.М. Буденного
sergeogri@yandex.ru
Иванин Андрей Николаевич
к.т.н, докторант, Военная академия связи им. Маршала Советского Союза С.М. Буденного
andreiivanin@gmail.com

Аннотация. В статье рассматривается методика повышения устойчивости функционирования оптических транспортных сетей связи специального назначения (ОТСС СН) в условиях реализации угроз информационной безопасности. Предложен комплексный подход, основанный на применении методов машинного обучения и скрытых марковских моделей (СММ), обеспечивающий сокращение времени обнаружения атак на физическом и канальном уровнях. Разработана модель состояния сети и классификации атак, а также алгоритм принятия превентивных мер. Полученные результаты способствуют повышению живучести и надежности сетей в рамках критической информационной инфраструктуры.

Ключевые слова: устойчивость, информационная безопасность, оптические транспортные сети, нейронные сети, скрытая марковская модель, ЭМВОС, критическая информационная инфраструктура.

Современные оптические транспортные сети связи специального назначения (ОТСС СН) являются основой высоконадежной и высокоскоростной передачи данных. Однако реализация угроз информационной безопасности (ИБ) посредством сетевых и компьютерных атак становится реальным инцидентом, способным нанести ущерб информационным системам за счет нарушения конфиденциальности, целостности и доступности [1], что имеет непосредственное влияние на одно из ключевых требований к ОТСС — устойчивость [2].

В настоящее время множество работ посвящено изучению возможности точного обнаружения и прогнозирования сетевых и компьютерных, добившихся существенных результатов [3].

Однако прямое применение данных методов к ОТСС СН не учитывает особенность ее построения и функционирования, а также плохо интегрируется напрямую с таким показателем как устойчивость:

1. Существующие способы обнаружения сетевых и компьютерных атак, хорошо работают на сетевом уровне и выше ЭМВОС [4], и не затрагивают физический и канальный уровень, это обусловлено принятием факта того, что злоумышленник находится внутри сети связи и для проведения сетевых и компьютерных атак, ему нет необходимости преодолевать первые два уровня. Такой подход разрушает концепцию сетей связи специального назначения функционирующих как часть объектов критической информационной инфраструктуры, а размещения его телекоммуникационного оборудования происходит только в пределах контролируемых зон.
2. Основной целю ИБ сетей связи, является обеспечение устойчивости их функционирования [1], но прямое интегрирование показателя информа-

ционной безопасности в устойчивость, будет вести не только к ужесточению требований к ОТСС СН, но и способствовать снижению общего показатель устойчивости, делая его более пессимистическим.

В контексте современных вызовов информационной безопасности, устойчивость оптических транспортных сетей связи специального назначения (ОТСС СН) становится критически важным аспектом их функционирования. Традиционные методы обеспечения устойчивости, основанные на повышении надежности и живучести сети, не всегда учитывают специфику угроз, возникающих на физическом и канальном уровнях. Это создает уязвимости, которые могут быть использованы злоумышленниками для нарушения конфиденциальности, целостности и доступности передаваемых данных. В связи с этим возникает необходимость разработки новых подходов, которые не только повышают вероятность сохранения работоспособности сети, но и минимизируют время обнаружения и нейтрализации угроз, что особенно важно для сетей, функционирующих в рамках критической информационной инфраструктуры.

Устойчивость функционирования ОТСС СН имеет вероятностный характер и оценивается на основе показателей живучести и надежности. Живучесть выражается как коэффициент оперативной готовности ($K_{о.г.}$), а надежность — коэффициент готовности ($K_г$)

$$K_{о.г.} = P(T)K_г$$
$$K_г = T_O/(T_O + T_в), \quad (1)$$

где $P(T)$ — вероятность сохранения работоспособности в результате внешних дестабилизирующих факторов, T_O — время наработки на отказ, T_B — время восстановления работоспособности.

В данной работе предлагается методика повышения устойчивости ОТСС СН не за счет увеличения вероятности сохранения работоспособности, а путем сокращения времени обнаружения угроз на физическом и канальном уровнях, рисунок 1, и оперативного принятия мер по их предотвращению.

Если вероятность сохранения работоспособности сети постоянна, коэффициент оперативной готовности определяется коэффициентом готовности, который зависит от времени наработки на отказ и времени восстановления.

В свою очередь время восстановления можно определить циклом восстановления:

$$T_в = T_{ОБНР} + T_{УВЕД} + T_{ПРРЕШ} + T_{РЕМ}, \quad (2)$$

где $T_{ОБНР}$ — время обнаружения воздействия, $T_{УВЕД}$ — время уведомления, $T_{ПРРЕШ}$ — время принятия решения, $T_{РЕМ}$ — время на ремонтные работы (принятие мер).

В данной работе предлагается использовать метод повышения устойчивость ОТСС СН не за счет повышения вероятности сохранения работоспособности $P_р(t)$, а за счет сокращения времени обнаружения угроз информационной безопасности на физическом и канальном уровне и принятия упреждающих мер по противодействию им, что позволяет сохранять общий показатель устойчивости сети на требуемом интервале времени.

Разработанная методика, рисунок 2, включает в себя следующие этапы:

1. В процессе функционирования фрагмента ОТСС СН его информационная безопасность определяется как нормальное или нарушение конфиденциальности, целостности и доступности $S = \{S_н, S_к, S_ц, S_д\}$.

В соответствии с требованием руководящих документов ФСТЭК России [5], разрабатывается модель угроз ИБ, включающая перечень актуальных угроз для конкретного фрагмента ОТСС СН. Определяются соответствующие им типы сетевых атак $A = \{A_1, A_2, \ldots A_n\}$.

2. Определение перечня параметров качества функционирования элемента ОТСС СН подлежащих мониторингу ($M_к$) представляющие собой многомерные массивы данных, в которых закодирова-

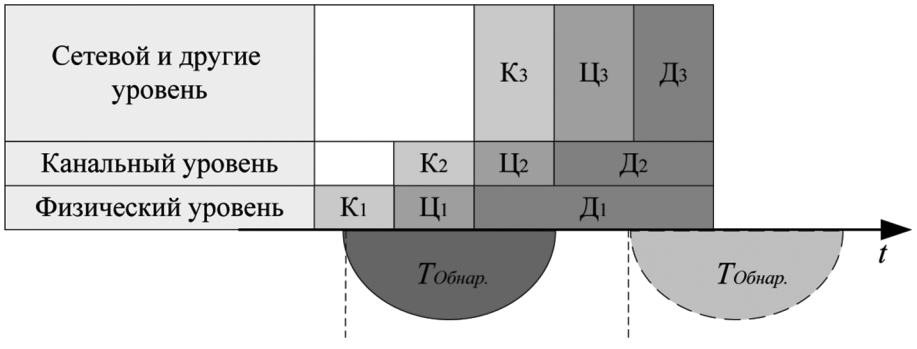

Рис. 1. Взаимосвязь уровней ЭМВОС и состояний ИБ

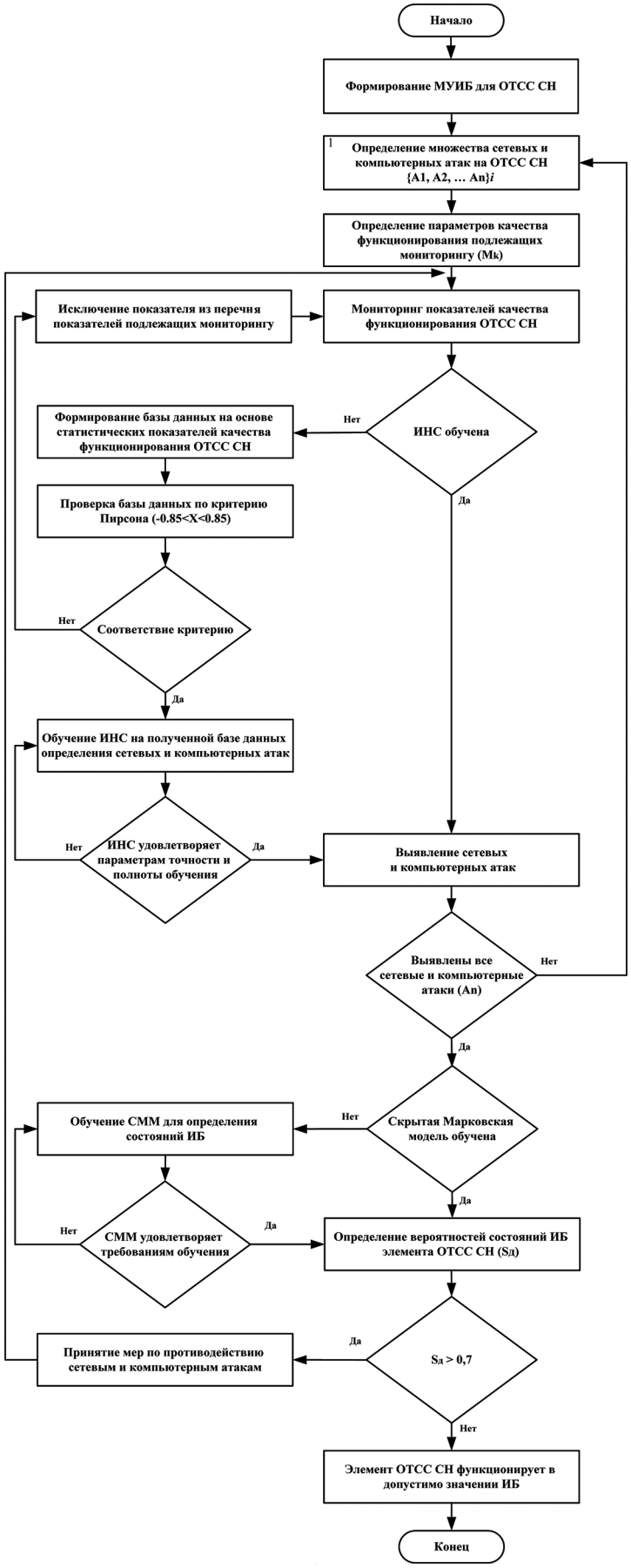

Рис. 2. Алгоритм обнаружения и прогнозирования состояний ИБ

ны значения показателей, влияющих на функционирование элемента ОТСС СН.

В таблице 1 представлен вариант контролируемых параметров способных отображать качество функционирования волоконно-оптических систем передач.

Таблица 1.

Контролируемые параметры оптических линий связи

Параметр	Описание	Параметр	Описание
CD	Хроматическая дисперсия	UBE-FEC	Неисправных ошибок после FEC
DGC	Дифференциальная групповая задержка	BER-POST_FEC	Частота ошибок после FEC
OSNR	Отношение оптический сигнал/шум	OPR	Принятая оптическая мощность
PDL	Потери, зависящие от поляризации	OPT	Переданная оптическая мощность
Q-factor	Q-Фактор	OFT	Оптическая частота на передаче
BE-FEC	Ошибки до FEC	OFR	Оптическая частота на приеме
BER-FEC	Частота ошибок до FEC	LOS	Потери сигнала

3. Формирование базы данных на основе статистических показателей качества функционирования ОТСС СН.

При подготовке обучающей базы данных важно убедиться, что данные не содержат сильной мультиколлинеарности [6] (взаимозависимости между входными переменными), с помощью коэффициента корреляции Пирсона (3) необходимо:

— определить, какие параметры имеют высокую степень корреляции и могут дублировать информацию.

$$K = \frac{\sum_{i=1}^{n}(x_n - \bar{x})(y_n - \bar{y})}{n\sigma_x\sigma_y} = \begin{cases} \leq 1 \\ 0 \\ \geq -1 \end{cases} \quad (3)$$

— сократить размерность данных путем исключения высококоррелированных параметров.

Если значения коэффициента корреляции Пирсона для определенных параметров выходят за пороговые значения $-0.85 \leq K \geq 0.85$, один из этих параметров показателя качества функционирования исключается из обучающей базы данных, так как он избыточен и не влияет на обучение ИНС [7].

Данные контролируемых параметров преобразуются в тензоры ключевых параметров, представляющие собой многомерные массивы данных, в которых закодированы значения показателей, влияющих на функционирование элемента ОТСС СН.

Тензоры позволяют учесть взаимодействие между различными характеристиками и более точно описать состояние системы при сетевых атаках.

4. Для обнаружения сетевых атак, на контролируемых параметрах, используется искусственной нейронной сети (ИНС). В качестве структуры ИНС выбран многослойных персептронов.

Архитектура ИНС обозначается как «5:3:2», что отражает количество нейронов в каждом слое. Для обучения сети применяется алгоритм обратного распространения ошибки, обеспечивающий корректировку весов на основе минимизации функции потерь (4,5).

$$y_j^1 = T_f\left(\sum_i d_i w_{ij}^1\right) \quad (4)$$

$$y_j^2 = T_f\left(\sum_j y_j^1 w_{ki}^2\right) \quad (5)$$

Все слои содержат нейроны, где осуществляется нелинейное преобразование с использованием функции активации . Связи между слоями задаются весами w_{ij}^1 и w_{ki}^2, которые настраиваются в процессе обучения модели. Выходной слой состоит из двух нейронов, обеспечивающих получение итогового результата.

5. После обучения ИНС, необходима проверка полноты (6) и точности (7) обучения ИНС. Данная проверка выполняется с использованием кривой зависимости истинно положительных значений (ИПЗ) от ложноположительных значений (ЛПЗ), вычисляемых по формулам:

$$\begin{cases} \text{ИПЗ} = \dfrac{\text{ИП}}{\text{ИП} + \text{ЛО}} \\ \text{ЛПЗ} = \dfrac{\text{ЛП}}{\text{ЛП} + \text{ИО}} \end{cases}, \quad (6)$$

где ИП — число истинно положительных предсказаний, ЛО — число ложно отрицательных значений, ЛП — число ложно положительных предсказаний, ИО — число истинно отрицательных значений.

На основе этих показателей строится ROC-кривая, позволяющая визуально оценить полноту обученной ИНС на основе обучающих данных.

Точность, как показатель обучения ИНС рассчитывается, как площадь под кривой (AUC) с помощью интегрирования.

$$AUC = \int_0^1 \text{ИПЗ}(\text{ЛПЗ})d(\text{ЛПЗ}) \quad (7)$$

В случае низкого значения точности обучения данные показатели можно улучшить за счет увеличения размерности обучающих данных или же изменение структуры ИНС и ее повторного обучения, пока не будет достигнут желаемый результат.

Обученная и удовлетворяющая требованиям ИНС определяет соответствующие типы сетевых атак $A = \{A_1, A_2, \ldots A_n\}$ в каждый момент времени t и формирует кортеж функционирования элемента ОТСС СН.

6. Обучение СММ для определения состояний ИБ.

Под скрытой марковской моделью понимают статистическую [8] модель, имитирующую работу процесса с неизвестными параметрами, который считается марковским $\lambda = (S, A, \pi)$, где, S — матрица переходов скрытых состояний (s_{ji}), A — матрица зависимости наблюдаемых событий от скрытых (a_{ji}), π — начальные вероятности нахождения в скрытых состояниях (S_n).

В данном случае, в качестве наблюдаемых событиях выступает кортеж по типам сетевых атак, а состояниями СММ выступает ИБ элемента ОТСС СН за определенный интервал времени, рисунок 3.

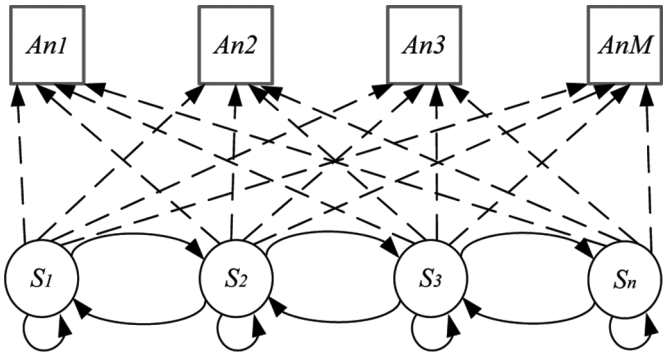

Рис. 3. Структура скрытой Марковской модели

Далее расчета значения переходных вероятностей матрицы S, выполняются итерации алгоритма Баума-Велша [9], прямого распространения ($\alpha_1(i)$).

$$\alpha_1(i) = \pi_i a_{\hat{Y}1i}, \quad (8)$$

$$\alpha_t(i) = (\sum_{j=1}^{4} \alpha_{t-1}(j) \times s_{ji}) \times a_{\hat{Y}_t i}, \quad (9)$$

где S_{ji} — веса случайно-инициализированной квадратной матрицы скрытых состояний S, проводя расчеты для всех значений $t = 1,2,3,\ldots,F$.

По завершению прямого распределения выполняется обратное распространение ($\beta_1(i)$), для чего инициализируют время $t = (F, F\text{-}1,\ldots,1)$, рекурсивно рассчитывается

$$\beta_t(i) = \sum_{j=1}^{4} s_{ij} \times a_{\hat{Y}\,t+1j} \times \beta_{t+1}(j). \quad (10)$$

7. Принятие превентивных мер по поддержанию устойчивости.

На основе вычисленных вероятностей состояний информационной безопасности элементов ОТСС СН принимаются решения о необходимых превентивных мерах для снижения рисков нарушения устойчивости сети. Если вероятность критического состояния (например, нарушение доступности) превышает пороговое значение (0,7), выполняются следующие действия:

- направление линейно-восстановительных групп;
- переход на резервные линии связи;
- переход на резервные оптические волокна;
- переход на другие технологии передачи информации на канальном уровне.

Применение этих мер позволяет оперативно реагировать на угрозы информационной безопасности и поддерживать устойчивость оптических транспортных сетей связи специального назначения.

Вывод

В данной статье предложена методика повышения устойчивости ОТСС СН на основе сокращения времени обнаружения и идентификации атак. Основные достижения:

Разработан алгоритм прогнозирования состояний ИБ с применением ИНС и СММ.

Представлены контролируемые параметры качества работы оптических линий связи.

Определены превентивные меры, позволяющие снизить влияние атак на сеть.

Применение данного подхода позволяет сократить время восстановления сети, повысить ее живучесть и надежность, что критически важно для специального назначения ОТСС СН в условиях современных угроз информационно й безопасности.

ЛИТЕРАТУРА

1. ГОСТ Р 53110–2008. Система обеспечения информационной безопасности сети связи общего пользования. Введен с 18.12.2008, переиздан в мае 2020. М.: Стандартинформ, 2020. 23 с.
2. ГОСТ Р 53111–2008. Устойчивость функционирования сети связи общего пользования. Введен с 18.12.2008, переиздан в мае 2010. М.: Стандартинформ, 2020. 19 с.
3. Алпеев Е.В., Стадник А.Н., Скрыль С.В. Методика прогнозирования компьютерных атак на основе определения весов атрибутов компьютерной атаки с применением метода деревьев решений //. Научные труды КубГТУ. 2021. № 6. С. 82–92.
4. ГОСТ Р 27.102-2021. Надежность объекта. Введен с 01.01.2022. М.: Российский институт стандартизации, 2021. 35 с.
5. ГОСТ Р ИСО/МЭК 7498-1-99. ВОС. Базовая эталонная модель. Часть 1. Базовая модель. — ОКС: 35.100.70. — Действует с 01.01.2000. — 62с.
6. Банк данных угроз безопасности информации. [Электронный ресурс] // ФСТЭК России URL:https://bdu.fstec.ru/threat (дата обращения 25.01.2025)
7. Созыкин А.В. Обзор методов обучения глубоких нейронных сетей //Вестник ЮУрГУ. Вычислительная математика и информатика. — 2017 Т. 6, № 3 — С.28–59.
8. Якунькин, В.Р. Машинное обучение с учителем / В.Р. Якунькин, Е.А. Панин // Оригинальные исследования. — 2022. — Т. 12, № 3. — С. 5–9.
9. Третьяков И.А. Обоснование применения скрытых марковских моделей с функцией плотности распределения наблюдений в АСНИ / И.А. Третьяков // Вестник Донецкого национального университета. Серия Г: Технические науки. — 2023. — № 2. — С. 16–21., Стр. 16
10. Попов А.А., Гультяева Т.А., Уваров В.Е. Распознавание, декодирование и восстановление последовательностей с пропусками, описываемых скрытой марковской моделью с дискретным распределением наблюдений // Системы анализа и обработки данных. 2017. №1 (66). с. 99–119. стр. 102.