REDS:

Телекоммуникационные устройства и системы

№4

2024

СОДЕРЖАНИЕ

ДВУХФАКТОРНЫЙ АНАЛИЗ ВЛИЯНИЯ ФЛУКТУАЦИИ ЧАСТОТЫ НА ХАРАКТЕРИСТИКИ ПЕРЕДАЧИ М-КАМ-СИГНАЛОВ

Алферова Ирина Александровна,
Донской Государственный Технический университет, Ростов-на-Дону, Россия

Енгибарян Ирина Алешаевна ,
Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО «Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия

Сафарьян Ольга Александровна,
Донской Государственный Технический университет, г. Ростов-на-Дону, Россия

Юхнов Василий Иванович
Северо-Кавказский филиал ордена Трудового Красного Знамени ФГБОУ ВО «Московский технический университет связи и информатики», г. Ростов-на-Дону, Россия

Аннотация
В статье предлагается анализ влияния долговременной и кратковременной нестабильности частоты на основные характеристики канала передачи цифровых сигналов – отношение сигнал/шум в одном бите информации и вероятность битовой ошибки. Приводится теоретическое обоснование в виде аналитических соотношений, связывающих нестабильность частоты и снижение отношения сигнал/шум. Кроме того, приведены аналитические соотношения, непосредственно связывающие отклонение частоты с вероятностью битовой ошибки. Приведены на примере сигнала 8-QPSK результаты численного моделирования.

Ключевые слова: *М-КАМ-сигналы, стабильность частоты сигнала, вероятность битовой ошибки.*

Современные системы связи, включая и системы радиосвязи, характеризуются практически повсеместным использованием сложных сигналов. Наибольшее применение среди сложных сигналов находят *QAM*-сигналы, достоинством которых являются:

– высокая энергетическая эффективность, следствием которой является повышение скорости передачи информации и снижение вероятности битовой ошибки;

– высокая спектральная эффективность, которая определяет максимальную скорость передачи информации в заданной полосе частот.

Отмеченные требования наиболее полно реализуются, как отмечено выше, при использовании *QAM*-сигналов [1-3].

В современной литературе достаточно полно и подробно рассмотрены вопросы, связанные с влиянием отклонения частоты сигнала на энергетические показатели канала связи [1]. В свою очередь, для *QAM*-сигналов существуют хорошо вычисляемые аналитические соотношения, связывающие отношение сигнал/шум в канале связи с вероятностью битовой ошибки. Однако с практической точки зрения представляет интерес получение зависимостей изменения (увеличения) вероятности битовой ошибки от отклонения частоты от номинального значения. Такие зависимости позволят на этапе разработки аппаратуры канала связи более точно сформулировать требования к данной аппаратуре и оценить характеристики каналов связи с учетом влияния отклонения частоты.

Целью работы является двухфакторный анализ влияния нестабильности частоты на характеристики передачи *QAM*-сигналов.

Запишем в соответствии с результатами работ [2-3] вероятность битовой ошибки:

$$P_{ber} = 2\left(1-\frac{1}{\sqrt{M}}\right)\operatorname{erfc}\left(\sqrt{\frac{3\log_2 M}{2(M-1)}\cdot\frac{E_b}{N_0}}\right), \qquad (1)$$

где E_b – энергия сигнала на один символ; N_0 – спектральная плотность мощности шума; M – количество символов на один бит информации; $\operatorname{erfc}(x) = \frac{1}{\sqrt{2\pi}} \int_x^{+\infty} \exp\left(-t^2/2\right) dt$.

Зависимость отношения энергии бита к спектральной плотности мощности от величины отклонения частоты сигнала может быть приведено к виду

$$\frac{E_b}{N_0} = \sqrt{Q_I^2 + Q_Q^2}, \tag{2}$$

где

$$Q_I = \frac{\int_0^T \left(v_I^{(0)} \cdot \cos\left(\varphi_0 + \Delta\omega \cdot \tau_u + \delta\omega \cdot \tau_u\right) - v_Q^{(0)} \cdot \sin\left(\varphi_0 + \Delta\omega \cdot \tau_u + \delta\omega \cdot \tau_u\right)\right) \cos\varphi_0 \cdot dt}{\int_0^T \zeta_I \cos\varphi_0 \cdot dt}, \tag{3}$$

– для синфазной составляющей

$$Q_Q = \frac{\int_0^T \left(v_Q^{(0)} \cdot \cos\left(\varphi_0 + \Delta\omega \cdot t + \delta\omega \cdot t\right) + v_I^{(0)} \cdot \sin\left(\varphi_0 + \Delta\omega \cdot t + \delta\omega \cdot t\right)\right) \sin\varphi_0 \cdot dt}{\int_0^T \zeta_Q \sin\varphi_0 \cdot dt}. \tag{4}$$

– для квадратурной составляющей.

В приведенных выражениях (3), (4) $v_I^{(0)}$ и $v_Q^{(0)}$ – представляют отсчеты синфазной и квадратурной составляющих принимаемого сигнала; φ_0 – начальная фаза сигнала; $\Delta\omega$ и $\delta\omega$ – соответственно долговременная и кратковременная составляющие нестабильности частоты сигнала; T – длительность импульса; ζ_I и ζ_Q – отсчеты шумового сигнала в синфазном и квадратурном каналах приемного устройства.

Соотношения (1)-(4) позволяют представить вероятность битовой ошибки как функцию отклонения частоты от номинального значения. Данная зависимость имеет вид

$$P_{ber} = 2\left(1 - \frac{1}{\sqrt{M}}\right) \operatorname{erfc}\left(\sqrt{\frac{3\log_2 M}{2(M-1)}} \cdot \sqrt[4]{Q_I^2\left(\Delta\omega, \delta\omega\right) + Q_Q^2\left(\Delta\omega, \delta\omega\right)}\right). \tag{5}$$

Формула (5) является аналитическим выражением, связывающим долговременную и кратковременную нестабильность частоты с вероятностью битовой ошибки.

Будем считать, что корреляционный интеграл имеет вид

$$I_I = \frac{\cos\varphi_0}{\sqrt{2\pi}\sigma} \exp\left(-\frac{\delta\omega^2}{2\sigma^2}\right) \cdot \int_0^T \cos\left(\left(\varphi_0 + \Delta\omega + \delta\omega\right) \cdot t\right) \cdot dt. \tag{6}$$

для синфазной составляющей и

$$I_Q = \frac{\sin\varphi_0}{\sqrt{2\pi}\sigma} \exp\left(-\frac{\delta\omega^2}{2\sigma^2}\right) \cdot \int_0^T \sin\left(\left(\varphi_0 + \Delta\omega + \delta\omega\right) \cdot t\right) \cdot dt. \tag{7}$$

для квадратурной составляющей.

Вычисление интеграла (6) приводит к выражению вида

$$I_I = \frac{\cos\varphi_0}{\sqrt{2\pi}\sigma}\exp\left(-\frac{\delta\omega^2}{2\sigma^2}\right)\cdot\frac{\sin\left((\varphi_0+\Delta\omega+\delta\omega)T\right)}{\varphi_0+\Delta\omega+\delta\omega}. \quad (8)$$

В свою очередь, интеграл (7) для квадратурной составляющей может быть представлен в форме

$$I_Q = \frac{\sin\varphi_0}{\sqrt{2\pi}\sigma}\exp\left(-\frac{\delta\omega^2}{2\sigma^2}\right)\cdot\frac{1-\cos\left((\varphi_0+\Delta\omega+\delta\omega)T\right)}{\varphi_0+\Delta\omega+\delta\omega}. \quad (9)$$

На рисунке 1 приведены нормированные зависимости, показывающие снижение отношения сигнал/шум на выходе корреляционного устройства обработки как функцию долговременной и кратковременной нестабильности частоты. Сплошная горизонтальная линия соответствует отсутствию кратковременной нестабильности частоты при наличии только долговременной составляющей отклонения частоты.

При проведении исследований принято, что долговременная нестабильность частоты составляет 100 Гц. Кратковременная нестабильность частоты изменяется в пределах:

– рисунок 1,*а* от 10 кГц до 50 кГц;
– рисунок 1,*б* от 30 кГц до 150 кГц;
– рисунок 1,*в* от 50 кГц до 250 кГц;
– рисунок 1,*г* от 70 кГц до 210 кГц.

Приведенные на рисунке 1 графики представляют собой количественные зависимости, которые легко могут быть получены на качественном уровне из общефизического анализа. Характерным на приведенных графиках является изменение знака кривизны с увеличением кратковременной нестабильности частоты.

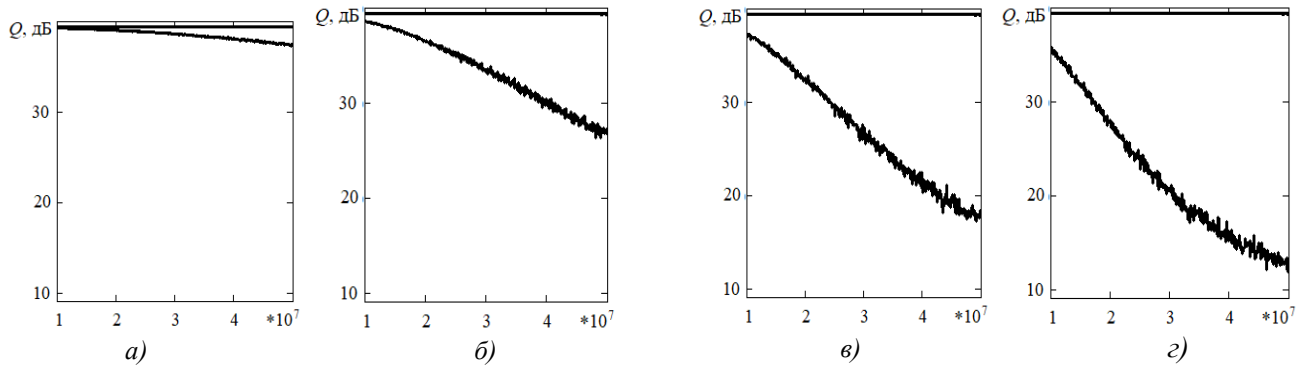


Рис. 1. Зависимость нормированного значения ОСШ как функции относительной нестабильности частоты

Результаты исследований вероятности битовой ошибки как функции кратковременной нестабильности частоты в канале связи для сигнала 8-QPSK приведены на рисунке 2.

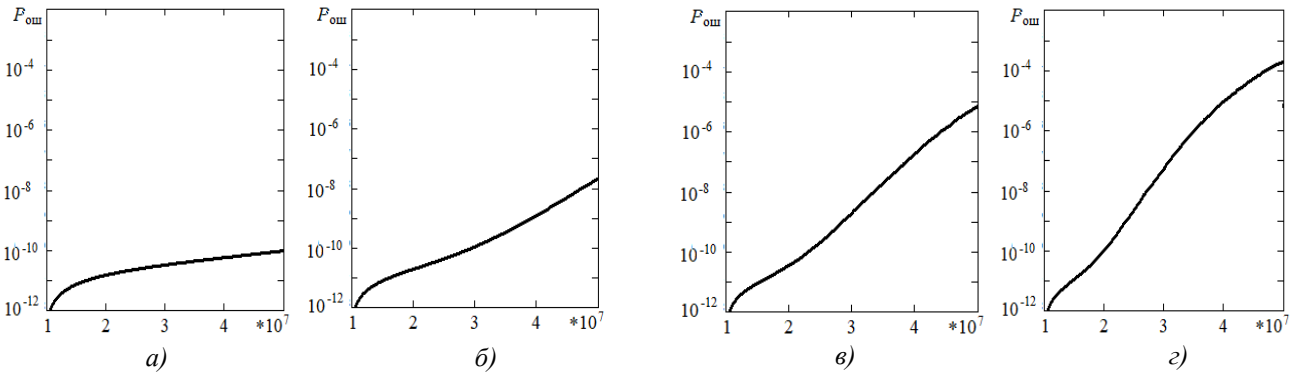


Рис. 2. Зависимость вероятности битовой ошибки для сигнала *M-PSK* как функции кратковременной нестабильности частоты: *а* – *M*=2; *б* – *M*=4; *в* – *M*=8; *г* – *M*=16.

В результате исследований можно сделать выводы:

1. Влияние обеих составляющих нестабильности частоты сигнала, имеющих долговременный и кратковременный характер приводит к снижению отношения сигнал/шум и, как следствие увеличению вероятности битовой ошибки. Полученные зависимости могут быть получены и объяснены на основе ранее известных данных. Однако в такой форме представления данные зависимости являются новыми и позволяют непосредственно связать такие важные характеристики как нестабильность частоты и вероятность битовой ошибки в канале связи.

2. При доминирующем значении кратковременной нестабильности частоты, проявляющейся на интервалах длительностью единицы секунд, величина отклонения частоты принимает случайные значения. Следствием этого является немонотонность зависимостей отношения сигнал/шум и вероятности битовой ошибки в канале связи.

Полученные результаты позволяют обосновать требования к значению долговременной и кратковременной нестабильности частоты в канале связи.

Литература

1. *Safaryan O.A., Pilipenko I.A., Boldyrikhin N.V., Yukhnov V.I.* Multidimensional likelihood function in the problem of estimating time-frequency parameters of signals // Radiation and Scattering of Electromagnetic Waves, RSEMW 2021, Conference Proceedingsб pp. 393-396.

2. *Safaryan O.A., Pilipenko I.A., Saharov I.A.* Features of Frequency Generators Stabilization in Distributed Information-Measuring Systems // Radiation and Scattering of Electromagnetic Waves, RSEMW-2019. Conference Proceedings, pp. 208-211.

3. *Safaryan O.A., Pilipenko I.A.* Prerequisites and Theoretical Foundations of the Statistical Method of Frequency Stabilization in Information and Telecommunication Systems // Electronics. 2022, №11(18), pp 1-9.

ИССЛЕДОВАНИЕ СВОЙСТВ ГЕНЕРАТОРА, УПРАВЛЯЕМОГО НАПРЯЖЕНИЕМ ДЛЯ СИСТЕМ 5G, НА КОМПЛЕМЕНТАРНОЙ ПАРЕ МОП ТРАНЗИСТОРОВ

Логвинов Василий Васильевич
доцент, к.т.н., МТУСИ, Москва, Россия,
adlerbasil@rambler.ru

Верятин Алексей Валерьевич
магистрант МТУСИ, Москва, Россия,
aleksey_veryatin@mail.ru

Аннотация

В статье представлены результаты исследования характеристик автогенератора, реализованного по схеме емкостной трехточки на комплементарной паре МОП транзисторов для частотного диапазона FR1 стандарта 5G. Анализ свойств автогенератора проводилось в среде MicroCap с использованием принципиальной схемы Колпитца, реализованной с использованием технологии 0,35 мкм. Свойства автогенератора исследовались в частотной и временной области (в режиме возникновения колебаний и в стационарном режиме), оценивались его энергетические характеристики, их изменение под действием внешних условий. Величина спектральной плотности мощности шума на выходе устройства составила значения, не превышающие –176,9 дБВ/Гц, при незначительном влиянии изменения температуры окружающей среды. Оценивалась возможность изменения частоты генерации при использовании варикапа как элемента колебательного контура для режима ГУН. Исследовались свойства автогенератора под внешним гармоническим воздействием для определения пределов полосы синхронизации, как потенциального синхронного усилителя в СВЧ диапазоне частот.

Ключевые слова: *однотактный автогенератор, фазовой шум, схема Колпитца, ГУН, комплементарная пара, полоса захвата, полоса удержания.*

Введение

Автогенератор является неотъемлемой частью любого устройства, осуществляющего прием и передачу сигналов. Он может функционировать как опорный генератор (ОГ), который генерирует стабильный гармонический сигнал, либо как генератор с регулировкой частоты через напряжение (ГУН). Опорный генератор используется в частотных синтезаторах для создания ряда фиксированных частот с заранее заданным шагом, зависящим от конструкции синтезатора. Частота ГУНа регулируется подаваемым напряжением от цифрового блока, что позволяет согласовать частоту получаемого сигнала с частотой, генерируемой синтезатором, в приемных устройствах прямого преобразования или при выбранной промежуточной частоте в супергетеродинных приемниках.

Современные разработки приемников с архитектурой прямого преобразования акцентируют внимание на необходимости применения ГУНов, которые обеспечивают стабильность частоты генерации. Кроме того, конструкция таких генераторов должна быть компактной, энергоэффективной и предусматривать возможности интеграции.

Для проведения анализа характеристик автогенератора была выбрана схема Колпитца с емкостной трехточкой. В качестве активных элементов использована комплементарная пара кремниевых МОП-транзисторов, которые отличаются отличными шумовыми характеристиками, упрощенной конструкцией благодаря использованию технологии ионной имплантации, а также возможностью создания устройств на единой подложке.

Анализ схемы автогенератора

В качестве автономной системы используется однотактный автогенератор, генерирующий квазипериодические колебания, выполненный по схеме Колпитца на базе комплементарной пары МОП-транзисторов. Этот генератор функционирует от источника питания с пониженным напряжением (примерно

3 В) и минимальным набором компонентов. Схема Колпитца представляет собой один из вариантов электронных генераторов, где частота автоколебаний определяется комбинацией индуктивности и двух конденсаторов. В данной реализации (см. рис. 1) используется делитель напряжения в колебательном контуре, состоящем из двух конденсаторов, соединенных таким образом, что обеспечивается положительная обратная связь. Ключевыми преимуществами такой схемы являются минимизация количества компонентов и предотвращение прохождения высокочастотных сигналов через источник питания.

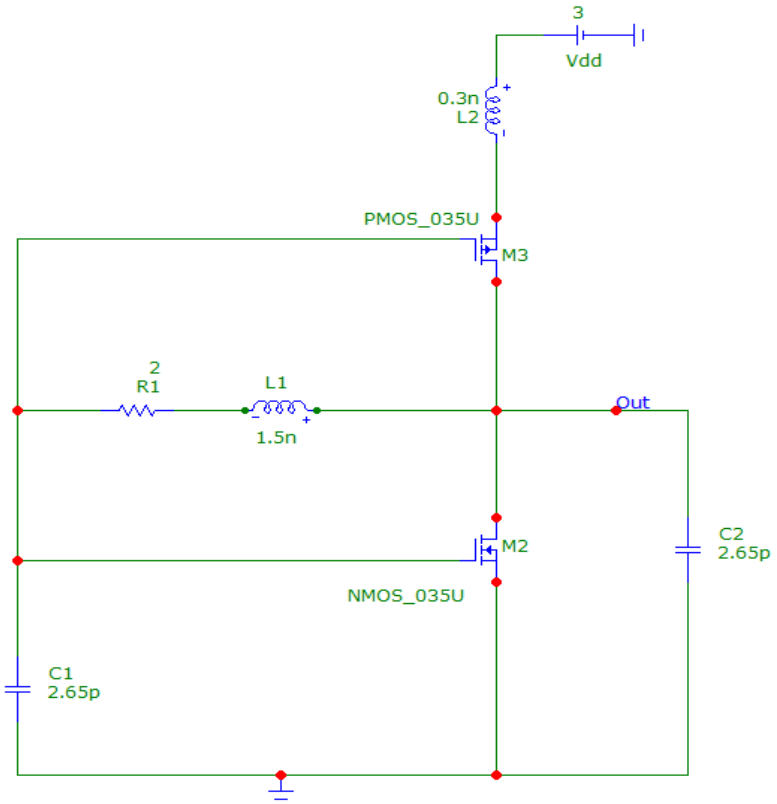


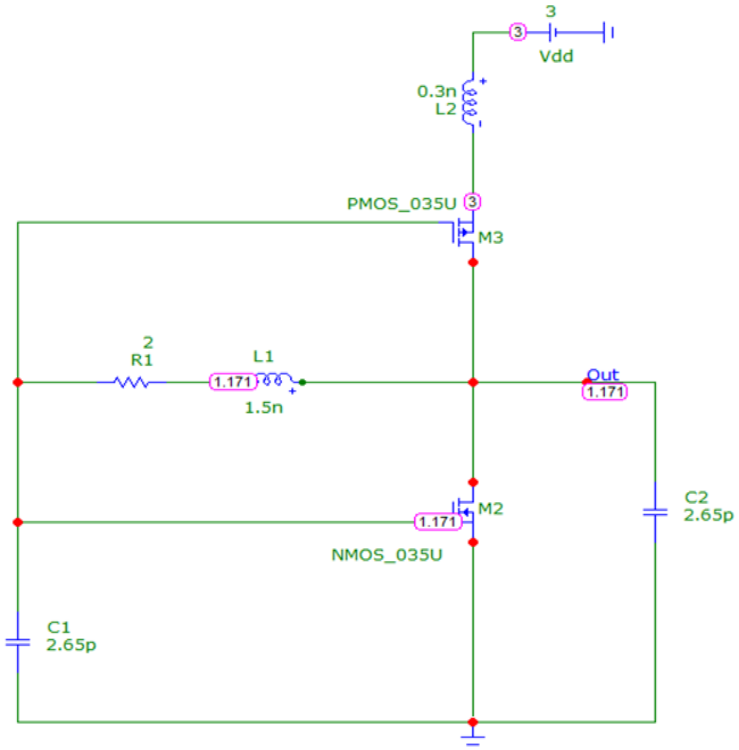
Рис. 1. Схема однотактного автогенератора на комплементарной паре МОП-транзисторов

Параметры PSPICE моделей nМОП и pМОП транзисторов с длиной канала 0.35мкм, используемые в программе моделирования MicroCap 12, представлены ниже.

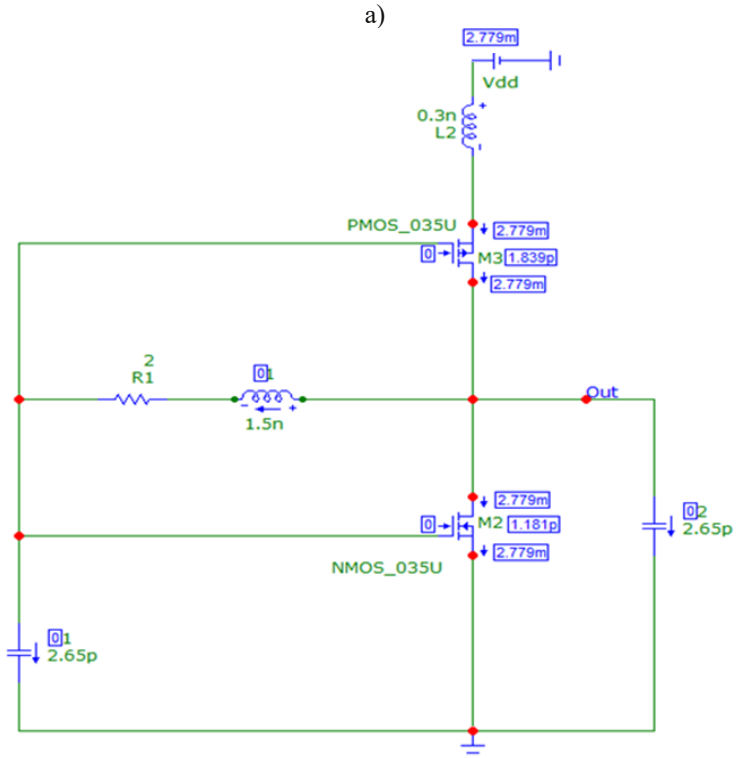
```
.MODEL NMOS_035u NMOS (LEVEL=8 A0=2.208 AF=1.4 AGS=249E-3 B0=-17.6E-9 CAPMOD=2
+ CDSC=0 CDSCD=84.48E-6 CF=0 CGBO=110E-12 CGDL=135E-12 CGDO=112E-12
+ CGSL=135E-12 CGSO=112E-12 CIT=1E-3 CJ=930E-6 CJSW=280E-12 CLC=1E-15 DLC=29E-9
+ DROUT=500E-3 DSUB=500E-3 DVT0=22.27 DVT1=1.051 DVT1W=0 DVT2=3.393E-3
+ DWC=26.76E-9 ETA0=30.85E-3 ETAB=-39.5E-3 JS=20E-6 K1=604.4E-3 K2=2.945E-3
+ K3=-1.72 K3B=632.5E-3 KETA=-621E-6 KF=2.810000E-027 KT1=-330E-3 L=0.35E-6
+ LINT=-16.7E-9 MJ=310E-3 MJSW=190E-3 NCH=2.310000E+017 NFACTOR=111.9E-3
+ NLX=191.8E-9 PB=690E-3 PBSW=690E-3 PCLM=683.1E-3 PDIBLC1=107.6E-3
+ PDIBLC2=1.453E-3 PDIBLCB=258.3E-3 PSCBE1=275.6E6 PSCBE2=9.654E-6 RDSW=604.3
+ RSH=82 TOX=3.5E-9 UA=1E-12 UA1=0 UB=0.001723E-15 UB1=0 UC=57.56E-12 UC1=0
+ UTE=-1.8 VERSION=3.1 VOFF=-57.2E-3 VSAT=117.8E3 VTH0=465.5E-3 W=24E-6
+ W0=118.4E-9 WINT=26.76E-9 XJ=300E-9 XPART=1);
.MODEL PMOS_035U PMOS (LEVEL=8 A0=.4716551 A1=.3417965 A2=0.83 AGS=0.12
+ AT=33000 CDSC=8.937517E-04 CDSCB=1.45e-4 CDSCD=1.04e-4 CIT=-1.015667E-03
+ DROUT=.3222404 DSUB=.23222404 DVT0=1.903801 DVT0W=0.232 DVT1=.5333922
+ DVT1W=4.5e6 DVT2=-.1862677 DVT2W=-0.0023 ETA0=6.024776E-02 ETAB=-4.64593E-03
+ K1=.8362093 K2=-8.606622E-02 K3=1.82 K3B=-0.24 KETA=-1.871516E-03 KT1=-0.25
+ KT2=-0.032 L=0.35E-6 LINT=6.23e-8 NCH=3.533024E+17 NFACTOR=1.54389
+ NLX=1.28e-8 PCLM=.989 PDIBLC1=2.07418E-02 PDIBLC2=1.33813E-3 PRT=64.5
+ PRWB=-0.323 PRWG=-0.001 PSCBE1=118000 PSCBE2=1E-09 RDSW=460 TNOM=27.0
```

+ TOX=9E-09 U0=138.7609 UA=1.39995E-09 UA1=4.312e-9 UB=1.e-19 UB1=6.65e-19
+ UC=-2.73e-11 UC1=0 VOFF=-.074182 VSAT=103503.2 VTH0=-.6732829 W=24E-6
+ W0=2.1e-6 WINT=1.22e-7 XJ=1.00000E-07).

На первом этапе моделирования анализа схемы однотактного автогенератора определяется режим работы МОП транзисторов по постоянному току при стандартной температуре (T=27°C), где ток составляет 2,8 мА при питании от источника ЭДС величиной +3 В (см. рис. 2).



а)



б)

Рис. 2. Результаты моделирования схемы однотактного автогенератора по постоянному току: а) напряжения в узлах; б) тока в ветвях схемы генератора

Исследование характеристик однотактного автогенератора было проведено как во временной, так и в частотной областях с использованием моделирования в среде Microcap. На рисунке 3 представлены формы напряжений на конденсаторах C1 и C2, а также ток через индуктивность L1 с потерями RL. Результаты показывают, что колебания начинают возникать и стремятся к гармоническому виду в установившемся режиме (см. рис. 3) при заданных начальных условиях моделирования.

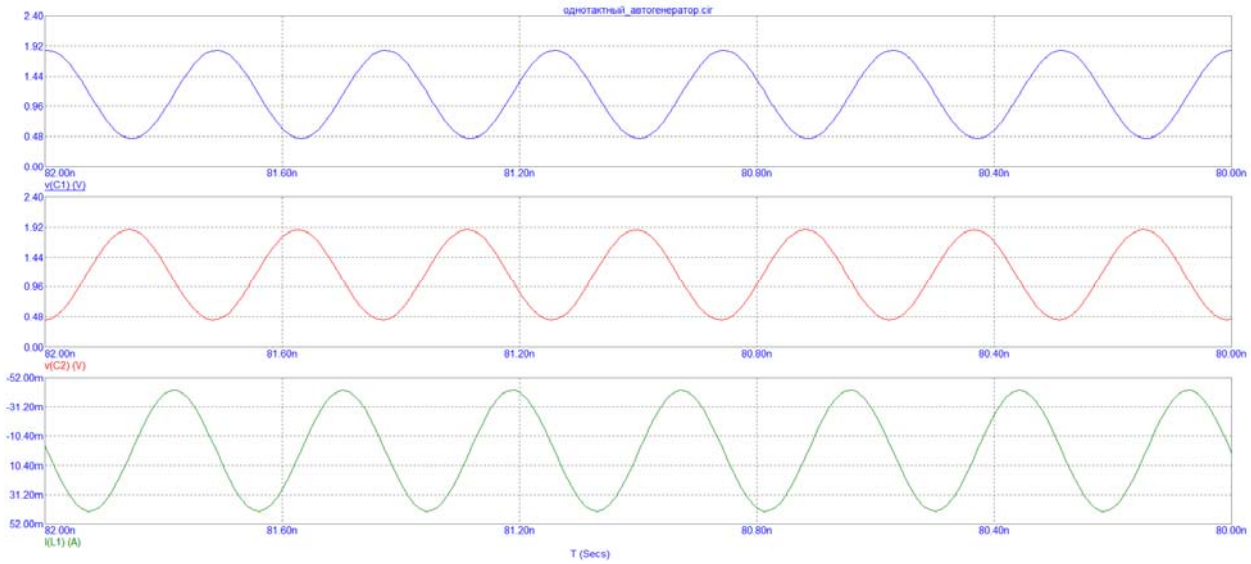


Рис. 3. Форма напряжения на конденсаторах v(C1) и v(C2) и тока через индуктивность I(L1) для стационарного режима автогенератора (на временном отрезке от 80 нс до 82 нс)

Выходное напряжение снимается с конденсатора C2 и имеет амплитуду Uвых = 0,72 В на частоте f0 = 3,509 ГГц.

При этом спектр выходного сигнала автогенератора, полученный с использованием процедуры преобразования сигнала (FFT) для установившегося режима, показывает ярко выраженную составляющую на частоте генерации с минимальным уровнем паразитных составляющих (см. рис. 4). Результаты анализа демонстрируют, что генерируемые колебания обладают достаточно чистым спектром и амплитудой первой гармоники благодаря высокой фильтрующей способности эквивалентного колебательного контура.

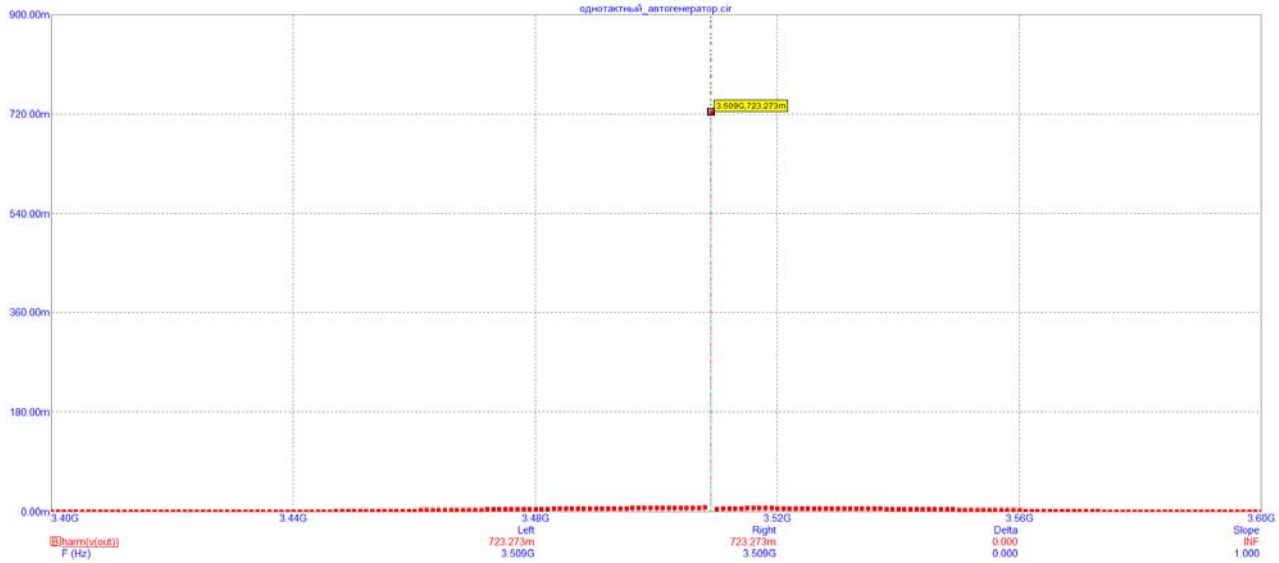


Рис. 4. Спектр сигнала автогенератора на комплементарной паре МОП транзисторов (установившемся режиме)

Таким образом, в установившемся состоянии автоколебательная система на комплементарной паре МОП транзисторов, выполненная по схеме Колпитца, генерирует напряжение на частоте 3,509 ГГц, близкое к гармоническому.

Был проведён анализ стабильности ключевых параметров автогенератора без применения дополнительных методов стабилизации, таких как поддержание стабильности напряжения источника питания, введение отрицательной обратной связи и прочее. Для заданных стандартных условий (T=27°C) и генерируемой частоты fвых 3.509 ГГц был исследован эффект изменения температуры окружающей среды в диапазоне от -20°C до +50°C на частоту и амплитуду выходного сигнала (см. табл. 1).

Таблица 1

Значения частоты генерации и амплитуды выходного сигнала от температуры окружающей среды

T(°C)	-20	-10	0	10	20	27	30	40	50
fвых(ГГц)	3.50891	3.50904	3.50912	3.50921	3.50932	3.5094	3.50943	3.50955	3.50967
*U*вых(В)	0.628	0.644	0.710	0.744	0.744	0.723	0.709	0.636	0.518

Результаты анализа, представленные на рисунке 5, демонстрируют зависимость частоты от температуры окружающей среды. Было отмечено, что частота генерируемого сигнала изменяется лишь незначительно при изменении температуры среды.

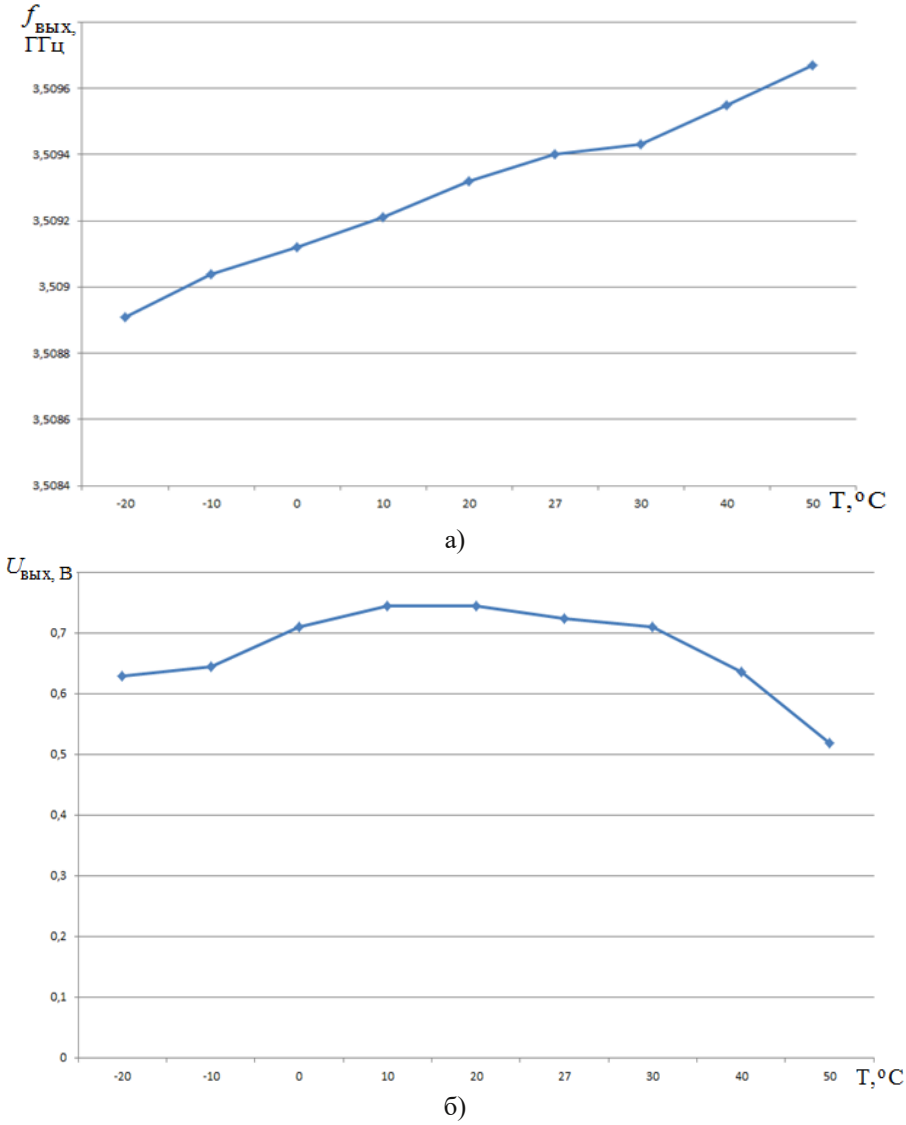


Рис. 5. Свойства выходного сигнала при различных температурах: а) частота; б) амплитуда

Амплитуда выходного сигнала изменяется в зависимости от температуры. При повышении температуры окружающей среды относительно нормальных условий происходит значительное уменьшение амплитуды генерируемых колебаний, в то время как при её понижении амплитуда также уменьшается. В пределах диапазона температур, близких к нормальной (T = 10-30°C), амплитуда выходного сигнала остаётся стабильной.

Анализ шумовых показателей автогенератора

Хотя гетеродин или генератор, регулируемый напряжением (ГУН), формально не являются частью радиотракта приёмника, их шумовые характеристики могут значительно повлиять на точность частоты преобразуемого сигнала. Более того, они оказывают значительное воздействие на общий коэффициент шума преобразующего устройства, что следует учитывать при проектировании системы.

Из известных источников шума, присущих БТ, основными являются: тепловые шумы, шумы токораспределения, дробовые шумы, рекомбинационные шумы, мерцательные (фликкер) шумы.

Наибольшее влияние на шумовые характеристики МОП транзисторов оказывают тепловые шумы, что связано с особенностями их работы и применяемыми технологиями производства.

Для анализа шумовых свойств устройств используется коэффициент шума, который отражает ухудшение отношения мощности полезного сигнала к мощности шума на выходе устройства по сравнению с аналогичным отношением на его входе. Также важным параметром является спектральная плотность шумов, которая показывает, как распределяется мощность шума в пределах рабочей полосы частот.

Анализ шумовых характеристик синхронных усилителей и генераторов в среде MicroCap выполняется с использованием параметров PSPICE моделей для МОП транзисторов восьмого уровня (BSIM3), которые учитывают тепловые, дробовые и фликкер-шумы. Расчёт спектральной плотности шума на выходе однотактного автогенератора осуществляется с использованием принципиальной схемы, представленной на рисунке 6.

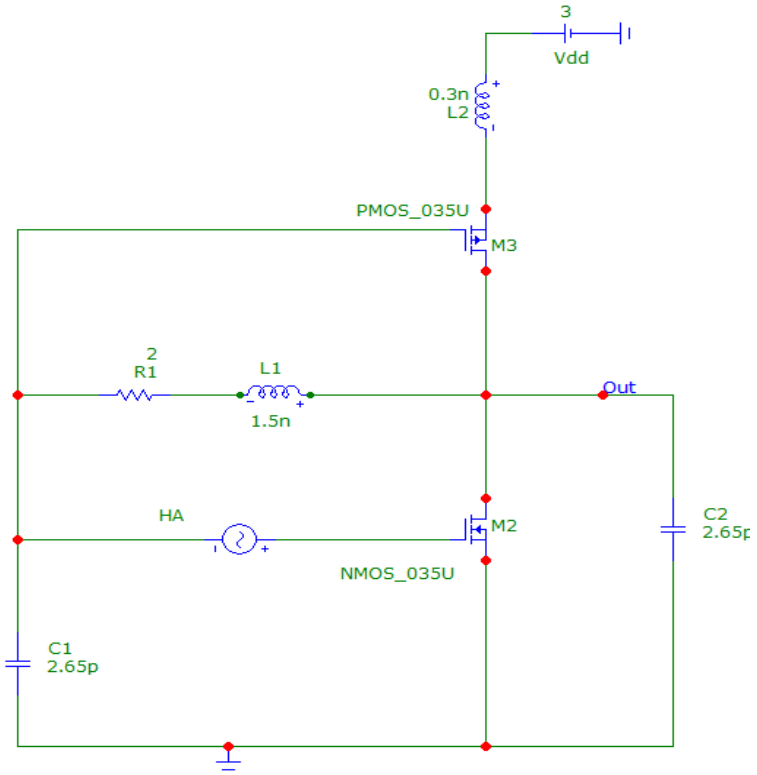


Рис. 6. Схема однотактного автогенератора, применяемая для расчета спектральной плотности шума на выходе

Анализ осуществляется с использованием дополнительного источника гармонического напряжения (HA), который указывает на узел схемы (INOISE), относительно которого выполняются расчёты шумовых характеристик генератора. Для измерения спектральной плотности мощности выходного шума применяется спектральная плотность квадрата напряжения между выходными узлами схемы (Out),

которые указаны в поле Noise Output. Условия анализа, а также точки ввода и вывода, обозначены на рисунке 7.

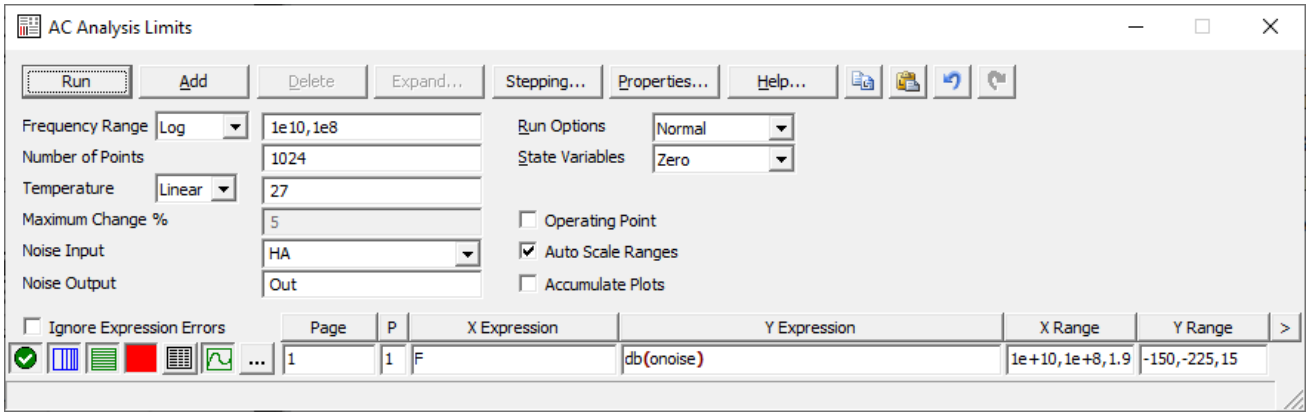


Рис. 7. Подменю условий анализа шумовых показателей однотактного автогенератора

Если рассматривать автогенератор как усилитель с положительной обратной связью, можно оценить спектральную плотность мощности шума на его выходе, выделяя две составляющие: одну, создаваемую автогенератором (АЭ), и другую, возникающую от пассивной избирательной цепи ПОС. При этом предполагается независимость источников шума, присутствующих в модели транзистора, воздействующих на его вход.

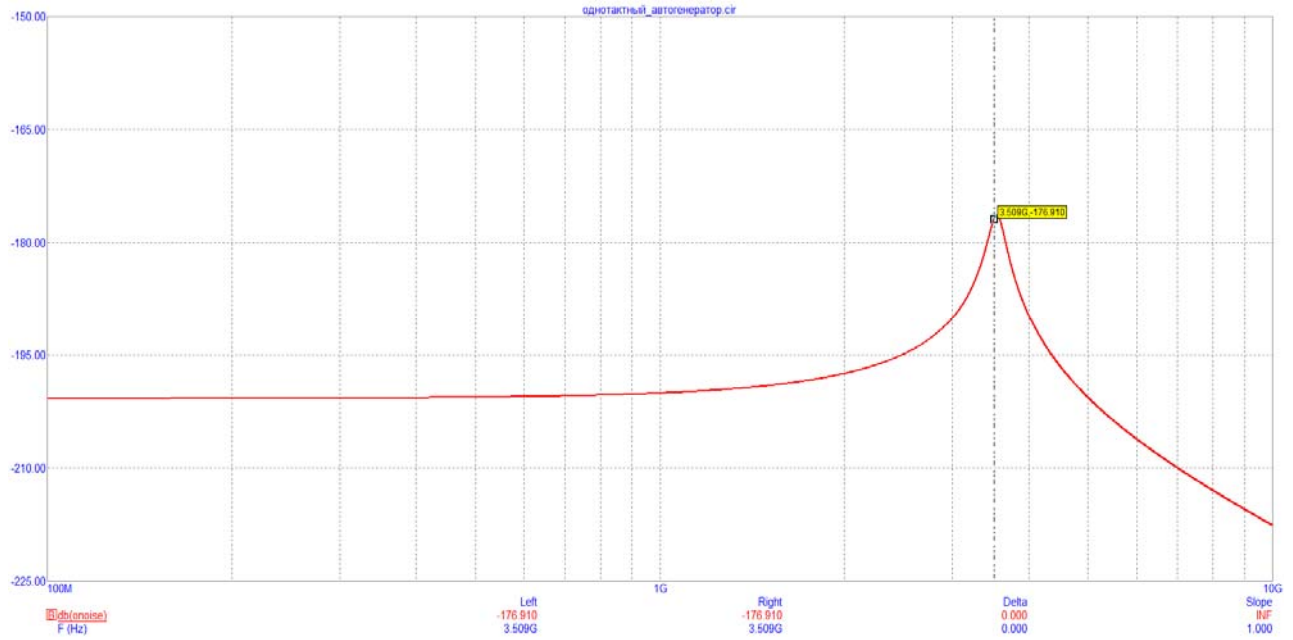


Рис. 8. Спектральная плотность фазовых шумов на входе и выходе однотактного автогенератора

Анализ шумовых характеристик автогенератора и синхронного усилителя, основанного на его конструкции, проводится с использованием модели МОП транзисторов восьмого уровня, представленной в PSPICE. Эта модель включает компоненты, которые позволяют учитывать тепловые шумы, возникающие от резисторов, а также дробовые и фликкер-шумы, являющиеся наиболее значимыми компонентами итогового шума, пересчитанного на вход синхронного усилителя.

На рисунке 9 приведены вычисленные кривые спектральной плотности мощности шумов в рабочем диапазоне частот для различных значений температуры внешней среды (табл. 2).

Таблица 2

Зависимость спектральной плотности шумов однотактного автогенератора на рабочей частоте от температуры

T(°C)	-20	-10	0	10	20	27	30	40	50
$S(f_0)$[дБВ/Гц]	-177.649	-177.481	-177.319	-177.163	-177.012	-176.91	-176.867	-176.726	-176.589

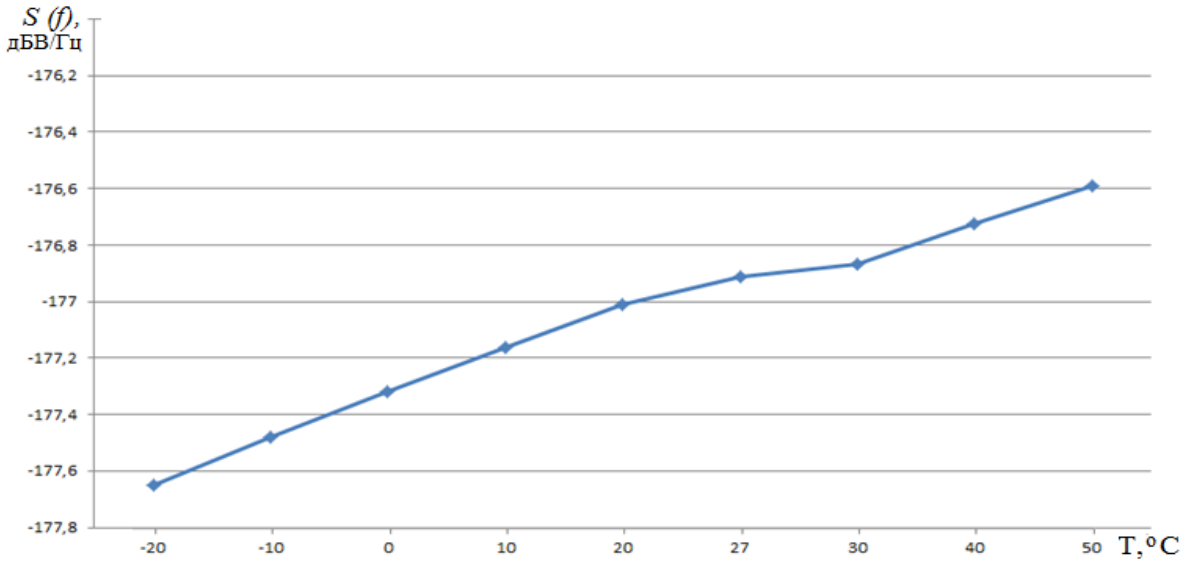


Рис. 9. Зависимость спектральной плотности шумов однотактного автогенератора от температуры

Управление частотой сигнала в однотактном автогенераторе изменением емкости варикапа

Для обеспечения возможности изменения частоты в широком диапазоне используется блок с переключаемыми конденсаторами. Для точной настройки частоты генерации применяются варикапы, на которые подаётся управляющее напряжение от выхода сглаживающего фильтра, интегрированного в систему ФАПЧ, которая функционирует в составе частотного синтезатора.

Для исследования зависимости частоты генерации однотактного автогенератора на комплементарных МОП транзисторах от величины напряжения была использована принципиальная схема, представлена на рисунке 10.

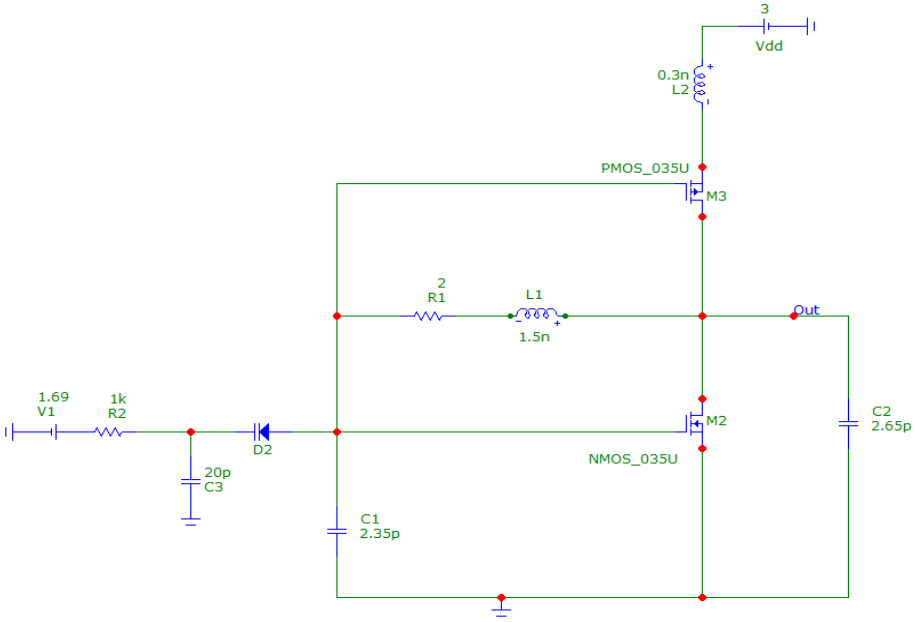


Рис. 10. Схема управления частотой генерации изменением емкости варикапа

В результате проведённого моделирования была получена таблица 3, а также её визуальное представление на рисунке 11, где отображена зависимость частоты генерации от напряжения смещения в виде кривой.

Таблица 3

Зависимость частоты генерации автогенератора от напряжения V1

Частота генерации $f_{вых}$	3.368	3.413	3.453	3.488	3.521	3.548	3.564	3.590	3.605
Напряжения V1, В	1.5	1.55	1.6	1.65	1.7	1.75	1.8	1.85	1.9

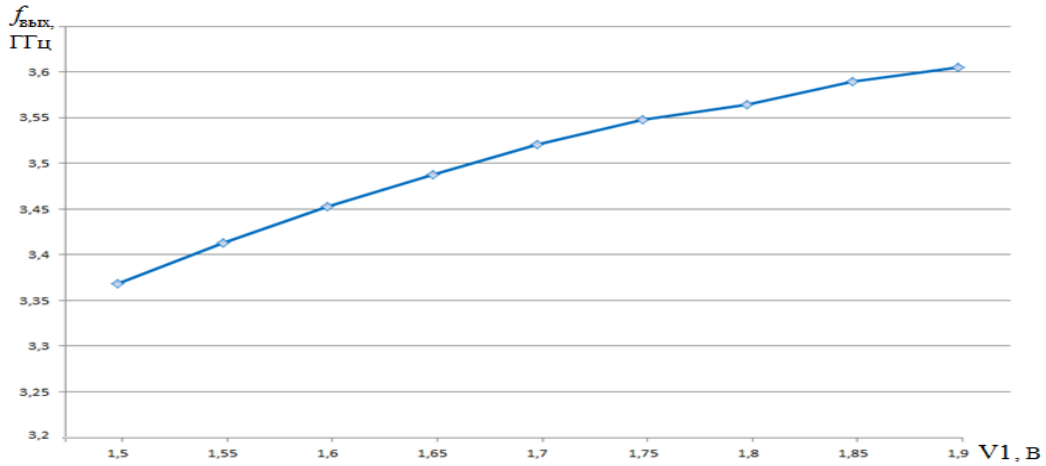


Рис. 11. Кривая зависимости частоты генерации от управляющего напряжения на варикапе V1

Для проведения анализа свойств использовалась схема автогенератора (рисунок 1) с напряжением питания, установленным на уровне Vdd = 3 В. В схеме, представленной на рисунке 6, pМОП транзистор М3 играет роль динамической нагрузки для nМОП транзистора М2, а дроссель L_0 выполняет функции фильтра источника питания. Внешний сигнал поступает от высокостабильного источника тока I_1, например, кварцевого генератора, генерирующего СВЧ-колебания с частотой $f_{вх}$.

Для моделирования работы автогенератора использовалась математическая модель источника внешнего воздействия, описываемая следующим выражением:

$$i_{вх}(t) = I_{вх}\sin(\omega_{вх}t) = I_{вх}\sin(2\pi f_{вх}t)$$

В ходе моделирования была выбрана малая амплитуда внешнего сигнала, равная I_вх=0,2 мА . На рисунке 12 представлена электрическая принципиальная схема исследуемого автогенератора.

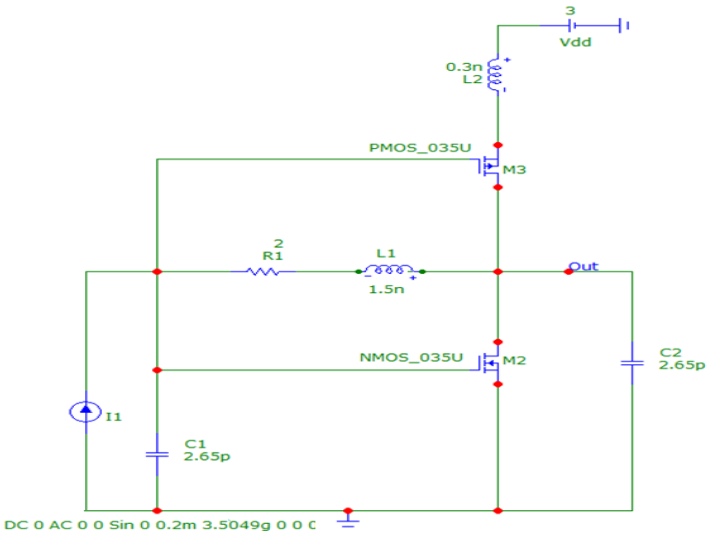


Рис.12. Схема однотактного синхронного усилителя на комплементарной паре МОП-транзисторов

Когда частота внешнего гармонического воздействия приблизительно совпадает с частотой автоколебаний генератора ($f_{вх}$ = 3,509 ГГц) , а амплитуда тока внешнего источника составляет ($I_{вх}$ = 0,2 мА) происходит захват автоколебаний под воздействием внешнего сигнала. Этот процесс подробно проиллюстрирован на рисунке 13.

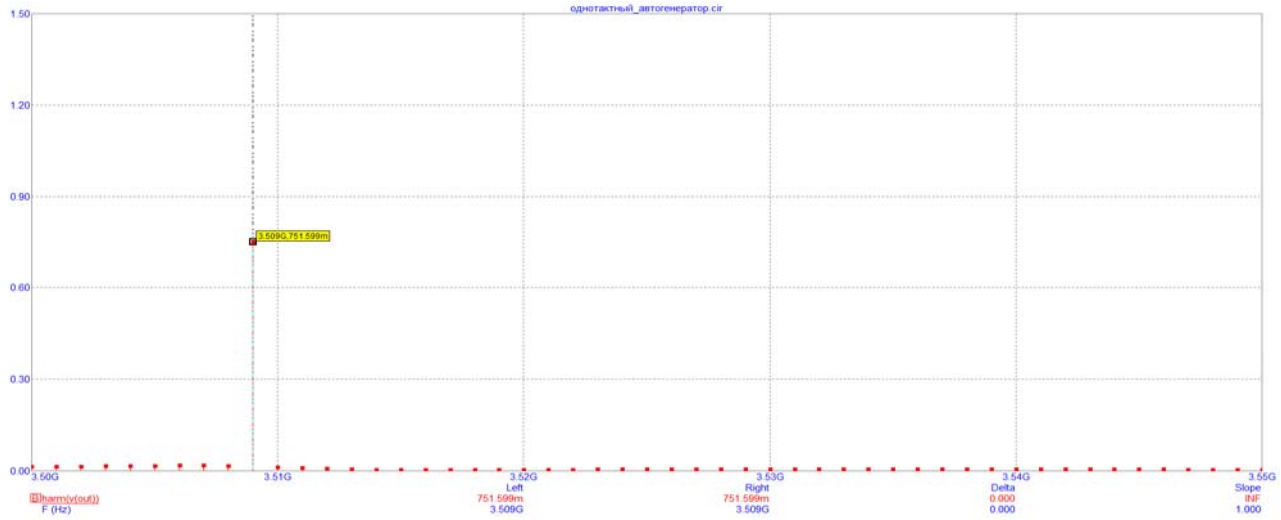
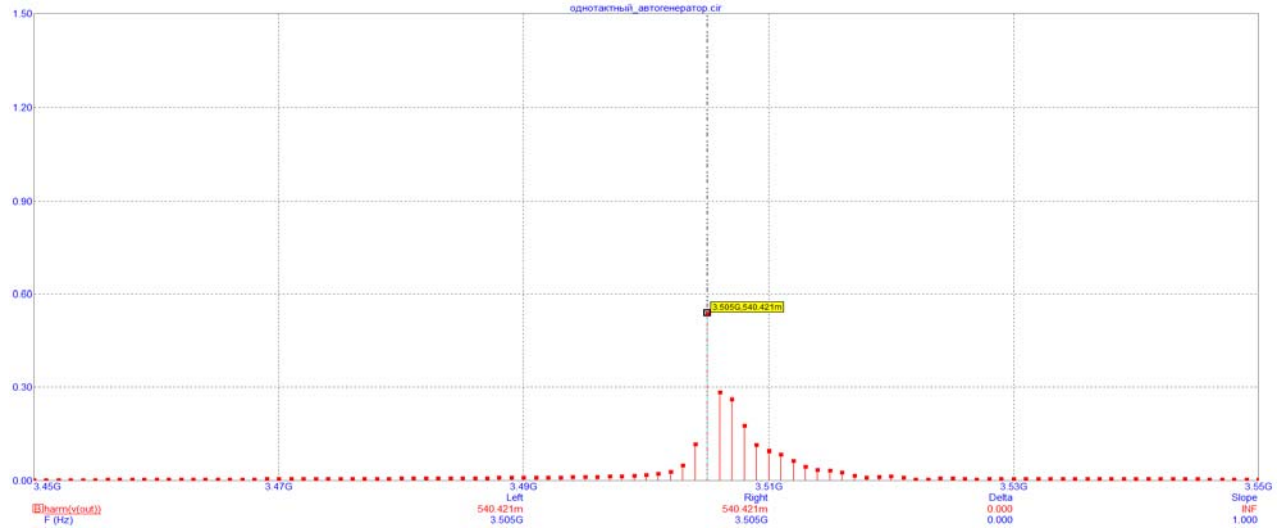


Рис. 13. Спектр сигнала на выходе СУ с $U_{вых}$ = 0,75В (f_0= 3,509 ГГц)

Анализ свойств синхронного усилителя во временной области показывает, что колебания на его выходе являются гармоническими. Это подтверждается тем, что в спектре выходного сигнала присутствует только одна частота, совпадающая с частотой внешнего воздействия, а шумовые компоненты отсутствуют. Таким образом, можно утверждать, что существует режим синхронизации между колебаниями автогенератора и внешнего источника.

Ключевыми характеристиками работы синхронного усилителя являются ширина полосы захвата (pull-in range) и полосы удержания (hold-in range). В режиме удержания частоты автогенератора и выходного сигнала полностью совпадают, а любые незначительные изменения параметров выходного сигнала, влияющих на его частоту, эффективно компенсируются работой синхронного усилителя. Режим захвата представляет собой переходный процесс, в ходе которого система изменяет своё состояние от биений, вызванных различием частот, к устойчивому режиму удержания.

При изменении частоты входного сигнала, начиная с $f_{вх}$ = 3.5048 ГГц, можно наблюдать «рассыпание» спектра, связанное с появлением множества комбинационных составляющих в спектре выходного сигнала. Однако при достижении частоты $f_{вх} = f_{зн}$ = 3.5049 ГГц спектр вновь становится монохромным, сохраняя особенности, характерные для биений между собственными автоколебаниями системы и внешним гармоническим воздействием (рис. 14б).

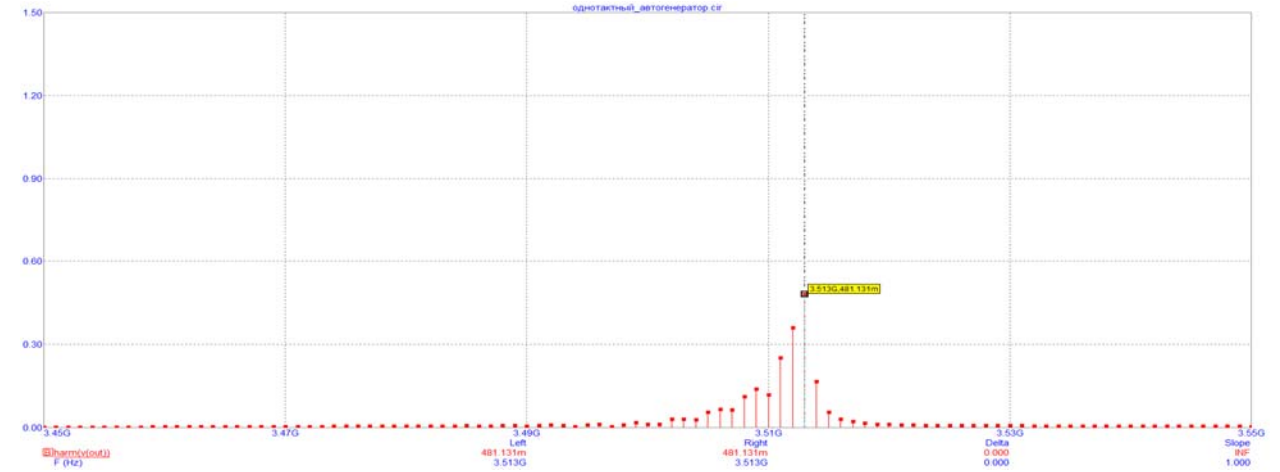


а)

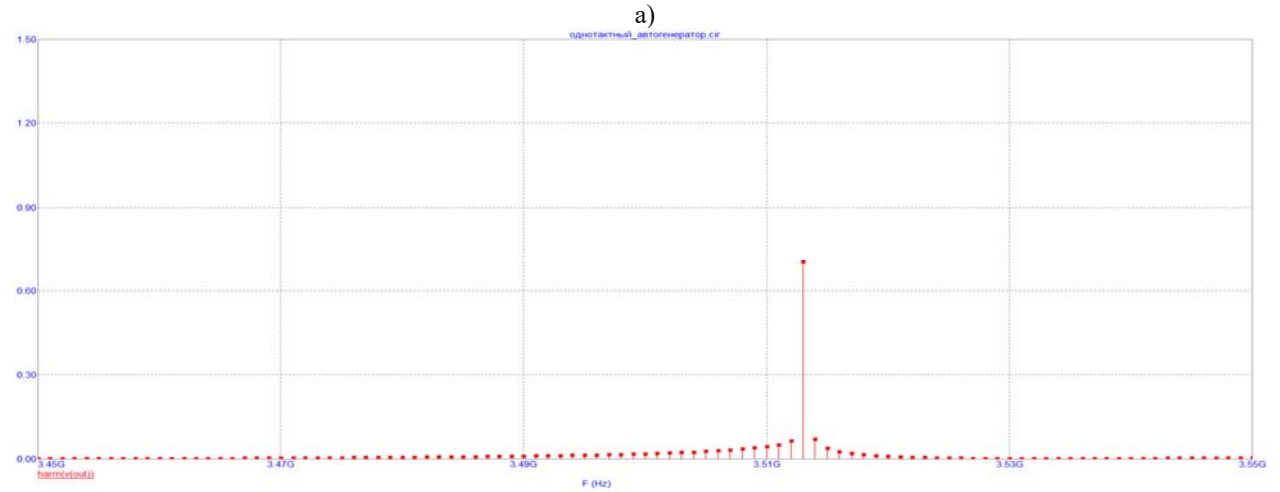
б)

Рис. 14. Спектр выходного сигнала входном воздействии на частотах:
а) $f_{вх} = 3{,}5048$ ГГц б) $f_{вх} = 3{,}5049$ ГГц;

Похожий процесс наблюдается при постепенном снижении частоты входного сигнала. Начальная с частоты $f_{вх} = 3{,}5132$ ГГц, а по мере уменьшения достигается значение, при котором частота внешнего воздействия становится равной частоте автоколебаний системы, то есть fвх = fзв = 3,5131 ГГц. Этот момент соответствует верхней частоте захвата.



а)



б)

Рис. 15. Спектр выходного сигнала при: а) $f_{вх} = 3.5132$ ГГц; б) $f_{вх} = 3.5131$ ГГц

На основании проведённых расчётов была определена полоса захвата, вычисляемая как $П_з = f_{зв} - f_{зн}$ = 3,5131 – 3,5049 = 0,0082 ГГц или 8.2 МГц.

Аналогичным образом определяется и полоса удержания. Для этого сначала находят нижнюю частоту удержания $f_{ун}$, постепенно снижая частоту входного сигнала с уровня автогенерации $f_0 = 3{,}509$ МГц, до момента появления многочастотного спектра выходного сигнала. В данном случае $f_{вх} = f_{ун} = 3{,}5048$ ГГц – это нижная частота удержания. Затем, увеличивая частоту входного сигнала от f_0 , находят верхнюю частоту удержания $f_{ув} = 3{,}5132$ ГГц. Таким образом, полоса удержания составляет $П_у = f_{зв} - f_{зн}$ = 3,5132 – 3,5049 = 0,0083 ГГц или 8.3 МГц.

При увеличении амплитуды внешнего сигнала до $I_{вх} = 0.25$ мА, и частоте внешнего воздействия, близкой к частоте автогенератора $f_{вх} = 3.509$ ГГц амплитуда выходного сигнала возрастает до 0,76 В. В этом случае полоса захвата и удержания составляют $П_з = f_{зв} - f_{зн}$=3.5142-3.5039=10.3 МГц $П_у = f_{ув} - f_{ун}$=3.5143-3.5038=10.5 МГц.

При еще большей амплитуде внешнего сигнала $I_{вх} = 0.3$ мА, и частоте внешнего воздействия, аналогичной частоте автогенератора $f_{вх} = 3.509$ ГГц амплитуда выходного сигнала увеличивается до 0.77 В. В этом случае полоса захвата составляет $П_з = f_{зв} - f_{зн}$=3.5152-3.5029=12.3 МГц, а полоса удержания равна $П_у = f_{ув} - f_{ун}$=3.5153-3.5028=12.5 МГц.

Моделирование проводилось для различных значений частот и амплитуд внешнего воздействия. На рисунке 16 представлены графики, отражающие зависимость частоты выходного сигнала синхронного усилителя от частоты гармонического воздействия для разных амплитуд синхронизирующего (усиливаемого) сигнала.

.

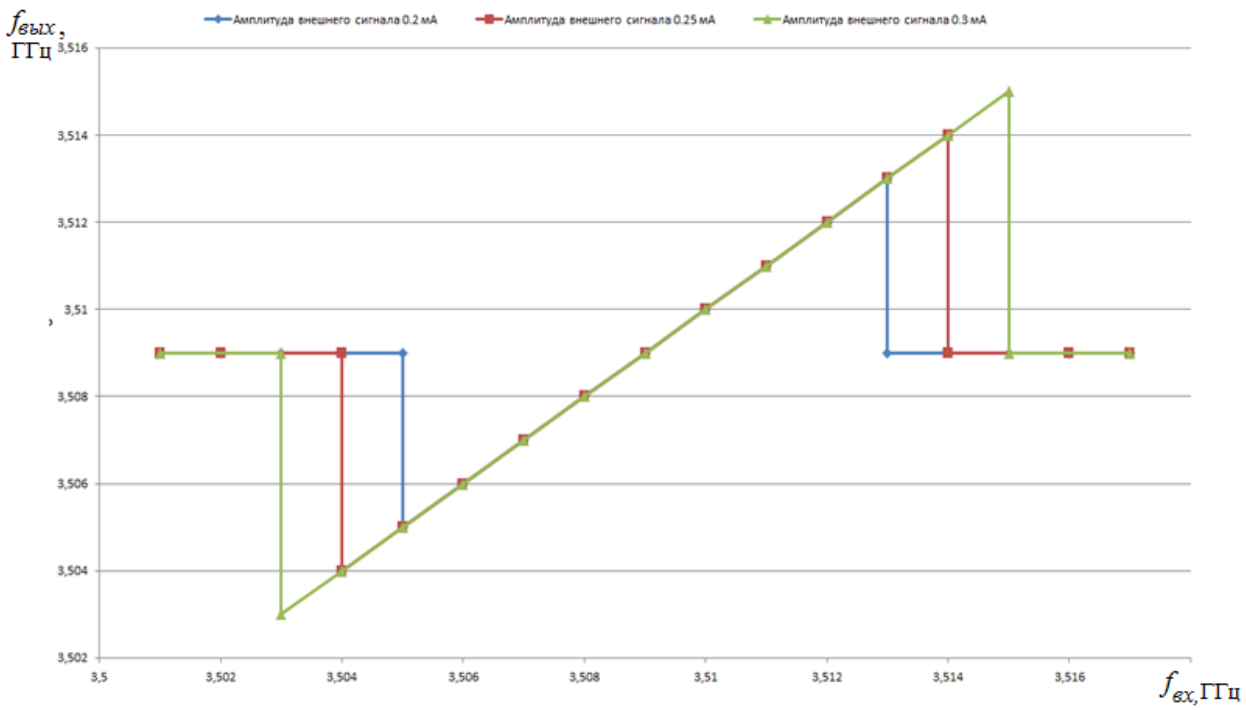


Рис. 16. Зависимость частоты выходного сигнала от частоты внешнего действия для различных значений амплитуды входного воздействия

Когда частота внешнего сигнала приближается к частоте автоколебаний и становится с ней идентичной, в спектре выходного сигнала остаётся только одна частота. В случае, если частота внешнего воздействия значительно отклоняется от частоты автоколебаний, временной сигнал приобретает форму биений, возникающих из-за наложения гармонических колебаний, близких по частоте. При этом спектр выходного сигнала отражает наличие комбинационных частот.

Заключение

В этой статье разработана и проанализирована математическая модель электрической схемы синхронного усилителя, основанная на восьмом уровне модели МОП-транзистора. Проведённые исследования позволяют сделать следующие выводы:

– Выходной сигнал практически не изменяет свою частоту при колебаниях температуры окружающей среды, что подтверждает её слабую зависимость от этого параметра.

– Автоколебательная система формирует колебания с частотой $f_0 = 3{,}509$ ГГц и амплитудой 0,72 В;

– Под воздействием внешнего гармонического сигнала система генерирует выходные колебания исключительно в синхронном режиме. В этом режиме частота автогенератора синхронизируется с частотой внешнего сигнала $f_{вх}$;

– Сохранение синхронного режима возможно лишь в пределах определённой полосы частотного расстройки между генератором и внешним сигналом. Ширина полос захвата и удержания определяется величиной входной амплитуды. Например, при Iвх = 0.2 мА ширина полосы захвата составляет Пз= 8.2 МГц, а удержания Пу = 8.3 МГц. При увеличении входной амплитуды до Iвх = 0.25 мА параметры увеличиваются до Пз=10.3 МГц и Пу =10.5 МГц соответственно, а при Iвх = 0.3 мА – до Пз=12.3 МГц и Пу =12.5 МГц, что соответствует требованиям стандарта 5G. Полоса удержания обычно превышает полосу захвата. Это объясняется тем, что колебания в контуре обеспечивают повышенную динамическую крутизну по первой гармонике активного элемента, тогда как в режиме захвата она ниже. Для модели синхронного усилителя это различие вызвано нелинейным поведением реактивных компонентов МОП-транзистора. Вне указанных полос система либо не генерирует колебаний, либо функционирует в асинхронном режиме.

– Были исследованы и представлены характеристики спектральной плотности мощности шума.

Синхронный усилитель обладает широкими возможностями применения в радиотехнических системах и устройствах. Он может использоваться для стабилизации частоты в СВЧ-генераторах, усиления промежуточной частоты в приёмной аппаратуре, а также в выходных каскадах передающих устройств (усилителей мощности). Помимо этого, устройство пригодно для синхронизации процессов преобразования, приёма и обработки сигналов, синтеза сложных форм сигналов и других специализированных задач.

Литература

1. *Осинов Г.В., Половинкин А.В.,* Синхронизация внешним периодическим воздействием: учебное пособие. Нижний Новгород: ННГУ им. Н.И. Лобачевского, 2005. 78 с.

2. *Фомин Н.Н., Андреев В.С., Воробейчиков Э.С., Логвинов В.В. и др.* Радиотехнические устройства СВЧ на синхронизированных генераторах / Под ред. Н. Н. Фомина. М.: Радио и связь, 1991. 191с.

3. *Logvinov V.V., Anh P.T.* Controlled Microwave Auto generator on a Complementary Pair of MOSFET Transistors // 2022 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO), Arkhangelsk, Russian Federation, 2022.

4. *Фан Т.А., Логвинов В.В.* Управляемый СВЧ автогенератор на комплементарной паре МОП-транзисторов // Телекоммуникации и информационные технологии. 2022. Т. 9, № 2. С. 166-173.

5. *Амелина М.А., Амелин С.А.* Программа схемотехнического моделирования Micro-Cap. Версии 9, 10: учеб. Пособие – СПб.: Лань, 2014. 632 с.

6. *Иванова И.* Основы разработки СВЧ усилителей. Россия: ЛитРес, 2022.

7. *Фан Т.А., Логвинов В.В.* Исследование свойств синхронного СВЧ усилителя, выполненного на комплементарной паре МОП транзисторов // Телекоммуникации и информационные технологии. 2023. Т. 10. № 1. С. 196-205.

8. *Гоноровский И.С.* Радиотехнические цепи и сигналы. М.: СР, 1971. 671 с.

9. *Тихвинский В.О., Терентьев С.В., Коваль В.А.* Сети мобильной связи 5G: технологии, архитектура и услуги М.: Издательский дом Медиа Паблишер, 2019. 376 с.

РАЗРАБОТКА АВТОМАТИЗИРОВАННЫХ СРЕДСТВ ТЕСТИРОВАНИЯ СИСТЕМЫ УПРАВЛЕНИЯ КОММУТАЦИОННЫМ ОБОРУДОВАНИЕМ

Кудряшова Анастасия Юрьевна
доцент кафедры ОТС МТУСИ, к.т.н., н.с., Москва, Россия;
доцент кафедры 402 МАИ, к.т.н., Москва, Россия
a.i.kudriashova@mtuci.ru

Хорошун Владимир Владимирович
магистрант кафедры 402 МАИ, Москва, Россия
horoshun12345@gmail.com

Аннотация
Статья посвящена разработке автоматизированных средств тестирования, способных проводить проверку работы системы управления коммутационного оборудования. Рассмотрен подход к автоматизации тестирования, предложена архитектура автоматизированного комплекса, проведена оценка его преимуществ. Разработанное решение включает реализацию программного обеспечения, тестирование и отладку. Продемонстрированы преимущества автоматизированного тестирования по сравнению с ручным. Основной результат - сокращение времени тестирования и повышение точности.

***Ключевые слова**: автоматизация тестирования, система управления коммутационного оборудования, тестирование сетевых устройств.*

Проблема автоматизации тестирования систем управления коммутационным оборудованием в настоящее время остается актуальной. Существуют различные подходы тестирования, подробно описанные в литературе [1]. Однако ситуация усложняется, когда необходимо тестировать не только программное обеспечение, но и само оборудование с использованием программных средств. Эта задача менее формализована, особенно в случае нестандартного или неунифицированного оборудования. Тем не менее, если оборудование имеет в какой-то мере стандартный интерфейс, задачу автоматизации тестирования системы управления можно решить.

В нашем случае происходило тестирование системы управления маршрутизирующего коммутатора третьего уровня, функционирующего под операционной системой Linux. Для оценки тестирования, необходима оценка качества работы и получение численных характеристик, характеризующих количеств удачных и неудачных команд, а также затраты времени и количество прогонов теста.

Был разработан автоматизированный комплекс для тестирования системы управления коммутатора, основной его задачей является проверка успешного выполнения команд, заявленных производителем. Комплекс включает простейшие скриптовые языки tcl и bash и генератор отчетов на html. Описана архитектура разработанного комплекса и его работы.

Вначале исследования рассматриваются современные методы автоматизации тестирования. К основным подходам относятся использование скриптовых языков, применение инструментов генерации и анализа трафика, интеграция автоматизированных тестов с системами непрерывной интеграции и развертывания (CI/CD), автоматизация с помощью систем управления конфигурациями, а также использование облачных сервисов для проведения тестирования. В рамках данного исследования для автоматизации тестирования были выбраны скриптовые языки TCL и Bash, что обусловлено рядом ключевых факторов [2-5].

1. Широкие возможности для автоматизации:

- Язык TCL (Tool Command Language) и оболочка Bash предоставляют мощные средства для создания скриптов, которые позволяют управлять сетевыми устройствами, выполнять команды, проверять ответы и анализировать результаты. Эти языки широко используются в области тестирования сетевого оборудования и телекоммуникаций.

2. Совместимость с сетевыми устройствами:

- Оба языка поддерживают работу с командным интерфейсом (CLI) устройства, что делает их удобными для автоматизации тестирования и управления сетевыми устройствами. Это обеспечивает простоту интеграции и выполнения тестов на оборудовании.

Удобство разработки и использования:

- Простота синтаксиса и мощные возможности для обработки текста делают TCL и Bash идеальными инструментами для написания скриптов автоматизации. Эти языки не требуют глубоких знаний программирования, что облегчает их использование разработчиками и тестировщиками.

3. Низкая стоимость внедрения и эксплуатации:

- Оба языка являются бесплатными и открытыми, что исключает необходимость приобретения лицензий, снижая затраты на внедрение и эксплуатацию системы автоматизации.

Далее была разработана архитектура автоматизированного комплекса:

- Интерфейс пользователя (UI): обеспечивает взаимодействие пользователя с системой, предоставляя удобный доступ к функциям для создания, настройки и запуска тестов, а также для мониторинга и анализа результатов тестирования.
- Модуль управления тестами: отвечает за планирование, координацию и контроль выполнения тестов. Он принимает запросы от UI, инициирует запуск тестов, отслеживает их выполнение и обрабатывает результаты.
- Тестовые скрипты: Программные сценарии, содержащие набор команд и инструкций для проведения тестов. Тестовые скрипты на TCL и Bash включают команды для взаимодействия с устройствами, генерации трафика и анализа результатов.
- Система сбора и анализа данных: отвечает за сбор, хранение и анализ результатов тестирования. Включает базу данных для хранения данных, аналитические модули и средства визуализации для представления результатов.
- Система отчетности: генерирует отчеты по результатам тестирования, автоматически создавая отчеты с информацией о выполненных тестах, результатах и выявленных проблемах, предоставляя возможность просмотра и анализа через UI.

Была разработана модель будущего тестового комплекса [3].

Рис. 1. модель архитектуры автоматизированного комплекса

Также была разработана структурная схема с функциональными и информационными связями, а также таблицы с описанием элементов, связей и функций.

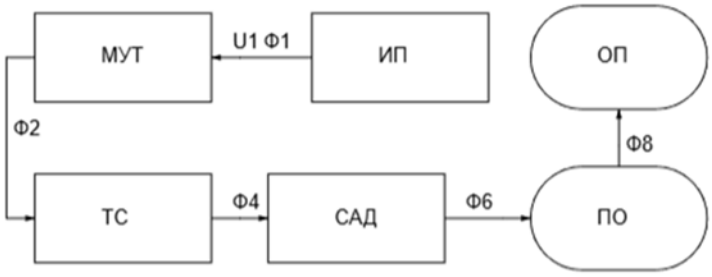


Рис. 2. структурная схема архитектуры с функциональными и информационными связями

Таблица 1

Модель внешней среды системы автоматизированного тестирования

Модель внешней среды системы автоматизированного тестирования	
Элементы среды	Коммуникативные связи
Подсистема интерфейса пользователя (ИП)	U1 Ф1 – Оператор системы (ОП) получает доступ к системе управления тестами.
Подсистема отчетности (ПО)	Y Ф8 – Оператор системы (ОП) получает отчет о результатах тестирования.

Таблица 2

Состав и функции элементов системы автоматизированного тестирования

Состав и функции элементов системы автоматизированного тестирования	
Элементы	Функции
Подсистема интерфейса пользователя (ИП)	Ф1: передает команды оператору системы для выполнения тестов.
Модуль управления тестами (МУТ)	Ф2: обрабатывает команды и направляет их в подсистему тестовых сценариев.
Подсистема тестовых сценариев (ТС)	Ф3: выполняет тестовые сценарии (TCL, Python, Bash). Ф4: передает результаты тестов в подсистему сбора и анализа данных.
Подсистема сбора и анализа данных (САД)	Ф5: обрабатывает результаты тестов. Ф6: передает данные в подсистему отчетности.
Подсистема отчетности (ПО)	Ф7: генерирует и визуализирует отчеты.

После разработки автоматизированного комплекса рассмотрим работу основных сценариев блок схемы. Блок-схема автоматизированных TCL и Bash скриптов представляет собой визуальное представление последовательности действий, которые выполняются в скриптах.

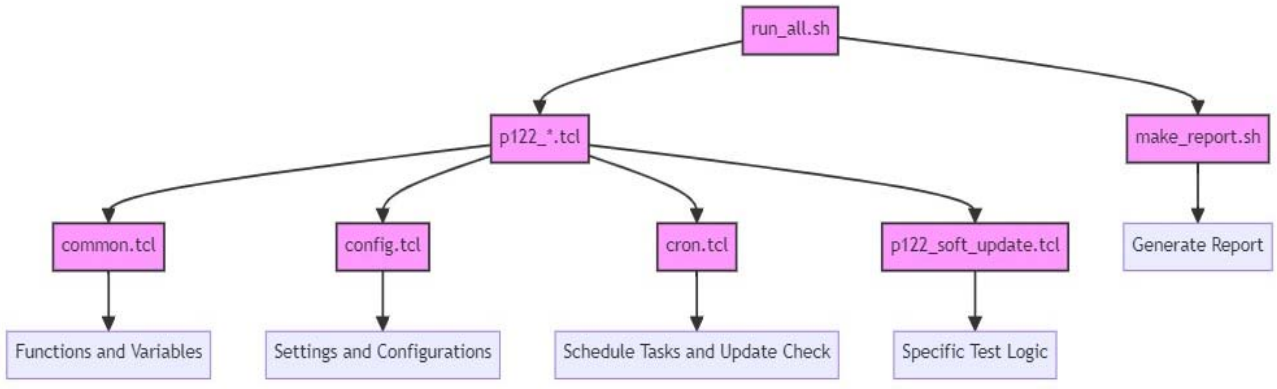


Рис. 3. Блок схема автоматизированных тестовых скриптов

Скрипт common.tcl служит для автоматизации взаимодействия с устройством через Telnet. Он включает функции для входа и выхода из системы, перезагрузки устройства, настройки IP-адреса, и ведения логов. Кроме того, скрипт предоставляет инструменты для генерации случайных данных, что может быть полезно для тестирования. Таким образом, этот скрипт помогает администрировать устройство, автоматизировать рутинные задачи и вести журнал действий, что упрощает мониторинг и отладку [4].

Скрипт config.tcl содержит настройки и параметры, необходимые для работы скриптов автоматизации управления коммутатором. Этот файл содержит все необходимые параметры для настройки соединения с коммутатором по Telnet и FTP, а также для управления проектными файлами на FTP-сервере. Давайте рассмотрим каждую установленную переменную [5].

Скрипт cron.tcl представляет собой скрипт, который используется для автоматизации регулярного тестирования проекта и отправки отчетности на FTP-сервер.

Скрипт p122_soft_update.tcl автоматизирует процесс обновления программного обеспечения на устройстве, начиная с настройки Telnet [6] и FTP-соединений для загрузки обновления. После установления соединения с FTP-сервером скрипт загружает файл с обновлением и выполняет команду установки нового ПО на устройстве.

Скрипты p122_*.tcl для проверки команд и всех сценарием коммутатора начинают с указания пути к интерпретатору expect и импорта общих функций из файла common.tcl [14]. Затем устанавливается telnet-соединение с устройством, осуществляется вход с помощью функции login, и отправляются команды для получения системной информации. Для разных параметров, таких как имя системы, местоположение, контактные данные и другие, генерируются случайные значения, а также устанавливаются текущие дата и время. Полученные данные проверяются с использованием регулярных выражений, и в случае несоответствия записывается ошибка в журнал. В завершение выполняется выход из telnet-сессии с помощью функции logout. Принцип работы остаётся одинаковым для всех скриптов, с изменениями в параметрах и тестируемых командах.

Скрипт make_report.sh: Этот скрипт предназначен для создания отчета о результатах тестирования в формате HTML на основе лог-файлов, содержащих результаты выполнения скриптов тестирования. Отчет содержит подробную информацию о результатах тестирования, включая успешно пройденные тесты и выявленные ошибки или несоответствия.

Скрипт run_all.sh: Данный скрипт предназначен для последовательного запуска всех скриптов проверки команд коммутатора и создания отчета о результатах в формате HTML.

Далее проведем тестирование автоматизированного комплекса используя скрипт run_all.sh, запустим не все тестовые сценарии, а будем тестировать по одному для проверки корректности написанных скриптов. Тщательно отслеживаем вывод каждого теста и удостоверяемся, что результаты соответствуют ожиданиям. Пример результатов проверки сценария p122_user.tcl:

File user.log

get login prompt	OK
send login/password	OK
help user	OK
show users all	OK
show user-login-config	OK
user set-login-config lock-user	OK
show locked-users	OK
user set-login-config no-lock	OK
user thflgyosvh admin	OK
user password thflgyosvh	OK
show users admin	OK
no user thflgyosvh	OK
logout	OK

Success: 13, Failed: 0

Рис. 4. Результаты отчёта html на примере сценария user

Выполнение тестов: Каждый тест проверяет определенные аспекты работы коммутатора, такие как маршрутизация, фильтрация, обработка данных, безопасность и другие функции. Во время выполнения тестов используются заранее определенные наборы команд для взаимодействия с коммутатором через протокол Telnet. Тесты проверяют корректность ответов коммутатора на эти команды и сравнивают их с ожидаемыми результатами.

Каждый тест генерирует log файл, содержащий результаты его выполнения. Эти логи сохраняются в директории logs для последующего анализа. После завершения всех тестов скрипт make_report.sh создает отчет в формате HTML на основе собранных логов. Отчет предоставляет сводную информацию о выполненных тестах, обнаруженных ошибках и их распределении по категориям.

После создания отчета происходит его анализ для выявления проблемных мест и ошибок, обнаруженных в ходе тестирования. Итог тестирования позволяет выявить и классифицировать возможные проблемы, такие как ошибки в работе функций коммутатора, несоответствие ожидаемым результатам и другие неполадки. Из рисунка 5 следует, что тестирование прошло успешно, поэтому отладка и дополнительное тестирование не требуются.

TOTAL - Success: 402, Failed: 0

Рис. 5. Результаты тестирования, количество успешных и неуспешных команд

Эти результаты демонстрируют пользу автоматизации тестирования [7-13] для одного программного обеспечения (ПО) коммутатора. Однако, учитывая постоянное обновление ПО, возможные изменения в командах или добавление новых, важно оценить, как будут работать автоматизированные тесты для других версий ПО [15-19].

Из рисунка 6 видно, что тесты успешно выполняются и для других версий ПО коммутатора. Однако стоит отметить, что имеются неудачные тесты, поэтому для новых версий ПО требуется проведение отладки и дополнительного тестирования автоматизированных средств.

TOTAL - Success: 387, Failed: 18

Рис. 6. Результаты тестирования, количество успешных и неуспешных команд для другого ПО коммутатора

Чтобы полностью осознать преимущества автоматизированного тестирования, построим график, отражающий затраченное время на ручное тестирование по стандартной методике, а также на автоматизированное тестирование на примере 10 прогонов нового программного обеспечения, с учетом отладки и повторного тестирования. По рисунку 7 можно увидеть, что с учетом отладки и дополнительного тестирования автоматизированных средств, с увеличением числа тестовых прогонов, выгода от автоматизации тестирования становится более заметной.

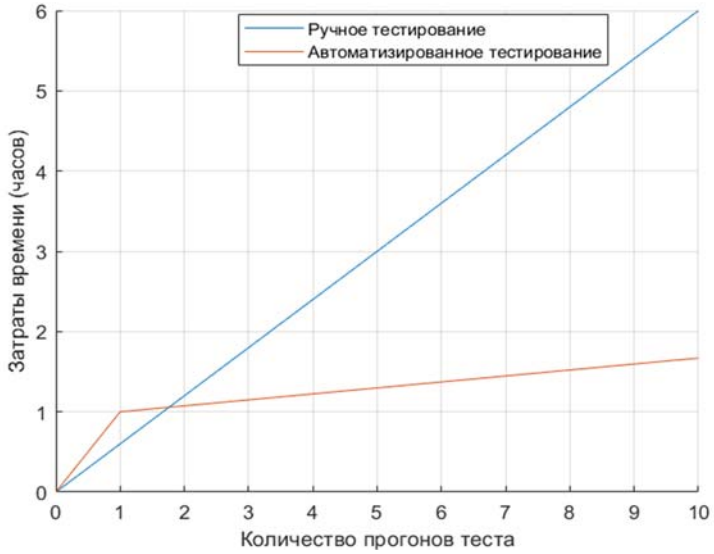


Рис. 7. Затраты времени на тестирование ПО коммутатора

Заключение

Данная статья посвящена разработке автоматизированных средств тестирования для системы управления коммутационным оборудованием. В исследовательской части был выбран подход к автоматизации тестирования, определена архитектура тестового комплекса и проведена оценка его эффективности. Результаты исследования показали, что автоматизированное тестирование обладает рядом преимуществ перед ручным, таких как сокращение времени на выполнение тестов и повышение точности результатов. В практической части был разработан сам автоматизированный комплекс, включающий создание программного обеспечения, проведение тестирования и отладки системы. Также был представлен перечень языков, таких как TCL и Bash, которые могут использоваться для тестирования, а также приведены блок-схемы, иллюстрирующие логику работы тестовых скриптов.

В статье на примере реальных тестовых сценариев продемонстрирована работа системы, включая генерацию отчетов и анализ результатов. Полученные данные подтвердили высокую эффективность автоматизации, а также выявили области, требующие дальнейшей доработки и оптимизации для обеспечения совместимости с различными версиями программного обеспечения.

Перспективы статьи включают дальнейшее расширение функциональности тестового комплекса, в том числе через интеграцию с системами непрерывной интеграции (CI/CD), что позволит оперативно выявлять ошибки на ранних стадиях разработки. Также планируется внедрение адаптивных механизмов для автоматического обновления тестов с учетом изменений в программном обеспечении коммутатора.

Литература

1. *Roy Osherove*. The Art of Unit Testing with Examples in .NET Manning-2009, 320 p.
2. *Брент Б. Уэлш, Кен Джонс, Джеффри Хоббс*. Практическое программирование на Tcl и Tk. 4-е изд. М.: Издательский дом Вильямс, 2003. 1123 с.
3. *Москвин П.В*. Азбука TCL. 2-е изд. М.: Горячая линия – Телеком, 2012. 216 с.
4. *Алексей Петровский*. Командный язык программирования TCL (Tool Command Language). М.: Майор, 2001. 192 с.
5. *Ousterhout J., K. Ken Jones*. Tcl and the Tk Toolkit. 2-е изд. Boston: Addison-Wesley Professional, 2009. 808 с.
6. Electronic Frontier Foundation. SSH Port Forwarding and Tunneling // SSH URL: www.ssh.com.
7. IEEE Communications Society. Automated Network Testing: Challenges and Solutions. IEEE Communications Magazine, том 59, выпуск 7, 2021. С. 42-48.
8. *Johnson R., Smith A*. Network Automation with Bash and Tcl. Journal of Network Engineering, том 15, выпуск 2, 2020. С. 33-45.
9. Maggiano David. CGI Programming with Tcl. Boston: Addison-Wesley, 1999. 576 с.
10. *Foster-Johnson Eric, Welch John C., Anderson Micah*. Beginning Shell Scripting. Hoboken, New Jersey: John Wiley &Sons, April 2005. 530 с.
11. *Foster-Johnson Eric, Welch John C., Anderson Micah*. Beginning Shell Scripting. Hoboken, New Jersey: John Wiley &Sons, April 2005. 530 с.
12. *Zimmer J. Adrian.* Tcl/Tk for Programmers: With Solved Exercises that Work with Unix and Windows. Hoboken, New Jersey: IEEE Computer Society, distributed by John Wiley and Sons, 1998. 564 с.
13. *Калмук А*. Автоматизация измерений с помощью программных средств Expect-Tcl на примере тестирования АТСП. URL: https://oops.math.spbu.ru/SE/diploma/2014/s/KalmukAlexander_Slides.pdf.
14. Автоматизация измерений с помощью программных средств Expect-Tcl на примере тестирования АТСП. URL: https://cyberleninka.ru/article/n/avtomatizatsiya-izmereniy-s-pomoschyu-programmnyh-sredstv-expect-tcl-na-primere-testirovaniya-atsp.
15. *Олифер В.Г., Олифер Н.А.* Компьютерные сети: принципы, технологии, протоколы: учебник для вузов: стандарт третьего поколения, 5-е изд., Питер Пресс, 2024. 1008 с.
16. *Wang Y.* Network Monitoring and Performance Optimization of Large-scale Distributed System Based on Big Data Algorithm // 2024 Asia-Pacific Conference on Software Engineering, Social Network Analysis and Intelligent Computing (SSAIC), New Delhi, India, 2024, pp. 281-287.
17. *Давыдов А.Е., Смирнов П.И., Парамонов А.И.* Проектирование телекоммуникационных систем и сетей. Раздел Коммутируемые сети связи. Расчет параметров сетей связи и анализ трафика. СПб: Университет ИТМО, 2016. 47 с.
18. *Locke H.L., Kai Ting Keshia Y., Ken Yu J.C., Yao Chua H*. QEX: Automated Testing Observability and QA Developer Experience Framework // 2023 IEEE Conference on Software Testing, Verification and Validation (ICST), Dublin, Ireland, 2023, pp. 454-460.
19. *Zhang D*. et al. HyperTester: High-Performance Network Testing Driven by Programmable Switches // IEEE/ACM Transactions on Networking, vol. 29, no. 05, pp. 2005-2018, Oct. 2021.

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ ИСПОЛЬЗОВАНИЯ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ВЫЯВЛЕНИЯ УГРОЗ В POWERSHELL-СКРИПТАХ

Василевский Павел Антонович
аспирант, МТУСИ, Москва, Россия
vasilevskiy.pavel@bk.ru

Аннотация
PowerShell широко используется как обычными системными администраторами, так и злоумышленниками для выполнения сложных задач управления и атак. Разнообразные обфускации и сложности анализа делают выявление вредоносных скриптов важной задачей кибербезопасности. В данной статье проводится обзор современных методов выявления вредоносных PowerShell-скриптов с применением машинного обучения. В заключительной части работы предложен новый подход на основе глубокой нейросети, которая использует архитектуру рекуррентных сетей с развёрнутыми слоями. Проведённые эксперименты показывают, что предложенная модель демонстрирует высокую точность и надёжность при классификации обфусцированных и сложных скриптов.

Ключевые слова: *PowerShell, вредоносные скрипты, глубокое обучение, машинное обучение, нейронные сети, информационная безопасность, выявление угроз, обфускация*

Введение

PowerShell, мощный инструмент автоматизации и управления, давно зарекомендовал себя как незаменимый инструмент для системных администраторов и разработчиков. Однако его гибкость и возможности часто используются злоумышленниками для проведения сложных атак, включая внедрение вредоносного кода, загрузку удаленных payload-ов и уклонение от антивирусных систем. Благодаря поддержке .NET Framework, PowerShell предоставляет обширный доступ к операционной системе, что делает его популярным выбором для целевых атак (APT) и других видов киберугроз [1]

Одной из главных сложностей выявления вредоносных PowerShell-скриптов является их обфускация. Программы, такие как Invoke-Obfuscation, позволяют злоумышленникам маскировать код с использованием изменения регистров, кодировки Base64 и динамической генерации команд [2,3]. Это значительно усложняет детекцию даже с применением современных систем защиты.

Ранние исследования предлагали использование классических методов машинного обучения, таких как Random Forest и логистическая регрессия, для классификации PowerShell-скриптов. В работе Хендлера представлены подходы, использующие текстовые признаки для построения простых моделей классификации [1]. В другом исследовании авторы применили конволюционную нейронную сеть (CNN), что улучшило точность детекции за счёт анализа текстовых данных на уровне символов [2]. Современные угрозы, однако, требуют более гибких решений. Например, использование гибридных моделей, включающих комбинацию анализа на уровне токенов, абстрактного синтаксического дерева (AST) и семантической обработки, продемонстрировало высокую эффективностьх [2]. Данные методы обеспечивают надежные результаты даже при работе с длинными скриптами и сложными обфускациями, что делает их важной составляющей современных систем защиты информации.

В данной статье будут рассмотрены существующие подходы к выявлению вредоносных PowerShell-скриптов, а также разработано собственное решение, основанное на глубоких нейронных сетях.

Существующие методы детекции вредоносных PowerShell-скриптов

В последние годы активно развивается применение методов машинного и глубокого обучения для детекции вредоносных PowerShell-скриптов. Различные исследования демонстрируют успехи в этой области, предлагая новые подходы к обработке текстовых данных, семантическому анализу и работе с обфусцированными командами.

В исследовании [4] были рассмотрены архитектуры сверточных нейронных сетей (CNN) и рекуррентных нейронных сетей (RNN), включая GRU, LSTM и Bi-LSTM. В качестве признаков для

классификации использовались такие характеристики, как наличие шелл-кода, информационная энтропия, длина строк, использование URL/IP-адресов и специфические имена переменных. Для обучения применялся датасет, содержащий 3102 вредоносных и 2000 легитимных PowerShell-файлов.

Результаты экспериментов показали, что модель Bi-LSTM достигла точности 98,50% на тестовой выборке, модель GRU обеспечила точность 96,79%, а LSTM – 91,42%. Время обработки инцидента варьировалось от 4 до 10 секунд в зависимости от модели. По итогам анализа предлагается использовать модель Bi-LSTM для выявления ложноположительных инцидентов кибербезопасности благодаря её показателям точности и характеристикам обработки данных

В другом исследовании [5] основное внимание уделяется применению модели Word2vec для преобразования токенов PowerShell в числовые векторные представления, что позволяет эффективно анализировать семантические и синтаксические отношения между командами. Векторные представления используют предварительно обученные embeddings, которые дополняются character-level embedding. Это позволяет учитывать как общий контекст, так и характерные признаки команд.

Экспериментальные результаты демонстрируют, что предложенная глубокая нейросеть, объединяющая архитектуры CNN и LSTM-RNN (рис. 1) [5], превосходит традиционные методы машинного обучения. Она обеспечивает увеличение покрытия угроз на 22 процента при фиксированном уровне ложноположительных срабатываний (0,1%). Модель успешно интегрирована в Microsoft Defender ATP, где она применяется к масштабным потокам PowerShell-скриптов через AMSI-интерфейс.

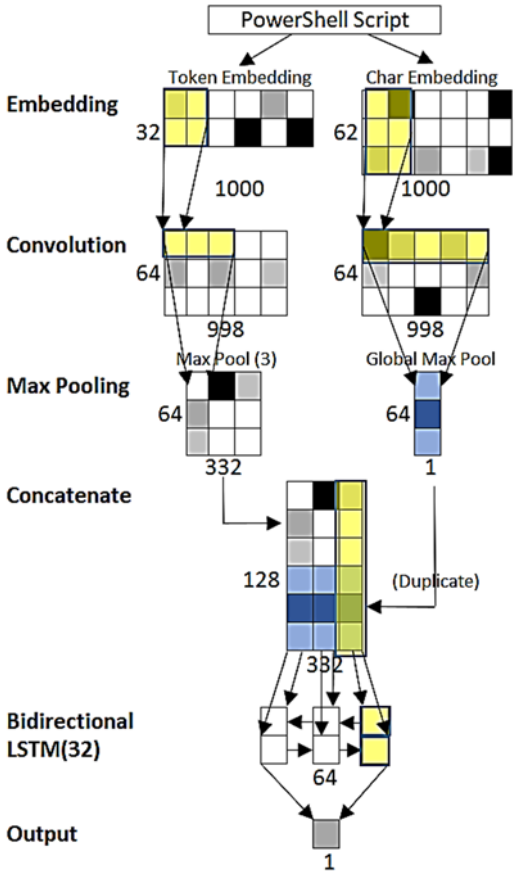


Рис. 1. Глубокая нейросеть, объединяющая архитектуры CNN и LSTM-RNN

Другое исследование [6] фокусируется на создании универсального подхода к обнаружению подозрительной активности PowerShell. Основное внимание уделяется поведению вредоносных скриптов, таких как ViperSoftX, и их способности оставаться незамеченными традиционными антивирусными средствами. Авторы предлагают метод детекции, основанный на мониторинге времени выполнения процессов PowerShell.

Используя инструмент EventSentry, предлагается настраивать фильтры для генерации предупреждений при превышении определённого времени выполнения PowerShell-скриптов (например, более 10 минут). Такой подход позволяет выявлять потенциально вредоносные скрипты, которые работают

непрерывно и скрыто. Указанный метод позволяет обнаруживать опасные сценарии, такие как ViperSoftX, где PowerShell используется для загрузки вредоносного кода из обфусцированных реестров или удалённых DNS TXT записей.

В исследовании [1] несколько подходов, включая традиционные методы обработки естественного языка (NLP), а также глубокие нейронные сети, такие как сверточные сети (CNN) и рекуррентные сети (RNN). Основное внимание уделяется анализу обфускационных техник и их влиянию на точность детекции.

Результаты экспериментов показывают, что ансамбль моделей, объединяющий NLP и CNN, дает наилучшую производительность, позволяя обнаруживать команды, которые ускользают от отдельных детекторов. Использованный датасет включал более 66,000 команд PowerShell, из которых около 6,000 были вредоносными. Наилучшие показатели достигались при использовании гибридного подхода, что демонстрирует потенциал таких методов для реальной практики кибербезопасности. Иллюстрация архитектуры сконструированной нейронной сети CNN приведена на рисунке 2 [1].

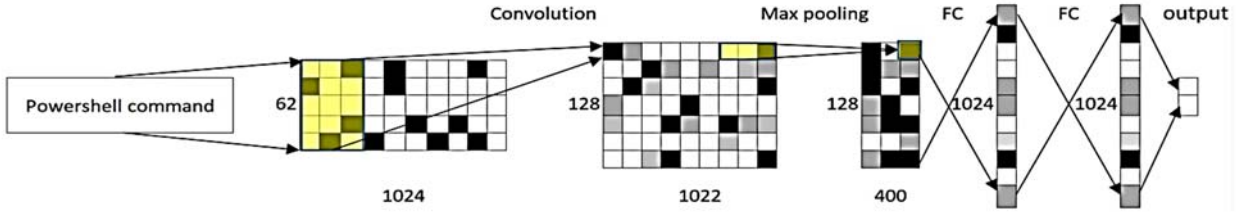


Рис. 2. Архитектуры нейронной сети CNN

Исследование [2] посвящено разработке модели обнаружения вредоносных PowerShell-скриптов на основе гибридных признаков. Исследование анализирует различия между вредоносными и легитимными PowerShell-скриптами на уровнях текстовых характеристик, функций, токенов и узлов абстрактного синтаксического дерева (AST). Для классификации используется алгоритм Random Forest, а семантические признаки извлекаются методом векторизации текста FastText.

В ходе экспериментов использовались наборы данных, включающие 4202 вредоносных и 4316 легитимных PowerShell-скриптов. Модель достигла точности 97,76% на смешанных скриптах, где вредоносный код был намеренно внедрён в легитимные скрипты, и 98,93% на оригинальных скриптах. В сравнении с существующими подходами, такими как 4-CNN и Token-Char-W2V, предложенная модель показала более высокую устойчивость к обфусцированным и длинным скриптам. Архитектура модели нейронной сети на основе гибридных функций представлена на рисунке 3 [2].

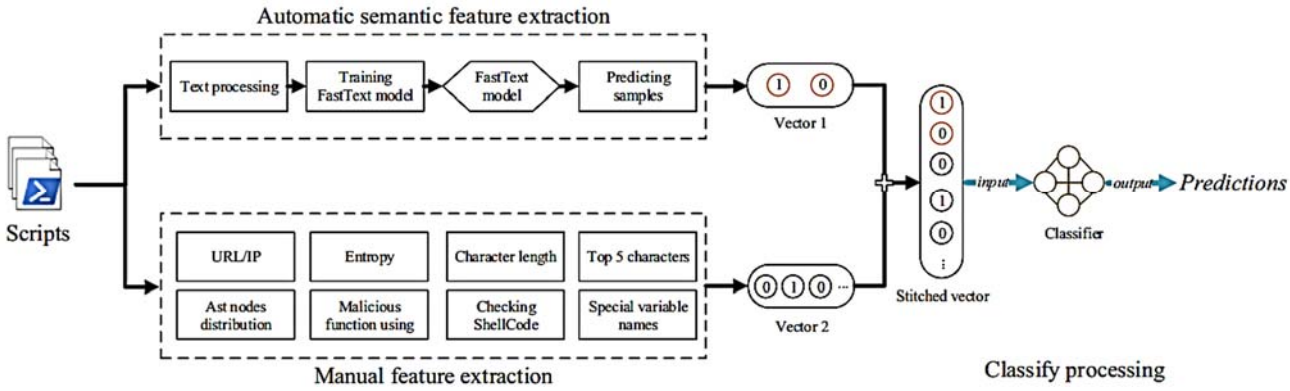


Рис. 3. Архитектура модели нейронной сети на основе гибридных функций

Реализация системы выявления вредоносных PowerShell-скриптов с использованием нейронных сетей

В рамках работы была разработана модель глубокого обучения для выявления вредоносных PowerShell-скриптов. Основной целью было создать инструмент, который может эффективно различать вредоносные и легитимные скрипты, несмотря на сложности, такие как обфускация кода и внедрение вредоносных фрагментов в легитимные скрипты.

Для обучения и тестирования модели был использован набор данных [7], включающий:

- 4202 вредоносных скрипта (категория malicious_pure), содержащих фрагменты из известных утилит, таких как PowerSploit и Empire.
- 4316 легитимных скриптов (категория powershell_benign_dataset), взятых из открытых репозиториев PowerShell.

Для уменьшения дисбаланса между категориями и более точной оценки модели было добавлено разделение на обучающую (80%) и тестовую (20%) выборки. Данные предварительно очищались от лишних символов, заменялись базовые строки Base64 и IP-адреса на соответствующие токены (base64_string, external_ip, internal_ip).

Для решения задачи классификации была выбрана архитектура нейронной сети, оптимизированная для обработки текстовых данных, а именно (рис. 4):

- Слой векторизации текста (TextVectorization): преобразует текстовые строки в последовательности из 2000 токенов с использованием словаря из 90 000 наиболее часто встречающихся элементов.
- Слой встраивания (Embedding): позволяет преобразовать токены в плотные векторные представления размерностью 16, что помогает улавливать их семантические связи.
- Два сверточных слоя (Conv1D): с 64 и 128 фильтрами извлекают локальные признаки из последовательностей, анализируя их структуру.
- Слой глобального усреднения (GlobalAveragePooling1D): уменьшает размерность признаков, сохраняя их основные характеристики.
- Полносвязный слой (Dense): с 128 нейронами для интерпретации извлеченных признаков.
- Выходной слой: с двумя нейронами и активацией softmax, возвращающий вероятности принадлежности к классам "вредоносный" и «легитимный».

Layer (type)	Output Shape	Param #
input_layer (InputLayer)	(None, 1)	0
text_vectorization (TextVectorization)	(None, 2000)	0
embedding (Embedding)	(None, 2000, 16)	1,440,000
conv1d (Conv1D)	(None, 2000, 64)	5,184
conv1d_1 (Conv1D)	(None, 2000, 128)	24,704
global_average_pooling1d (GlobalAveragePooling1D)	(None, 128)	0
dropout (Dropout)	(None, 128)	0
dense (Dense)	(None, 128)	16,512
dense_1 (Dense)	(None, 2)	258

Total params: 1,486,658 (5.67 MB)
Trainable params: 1,486,658 (5.67 MB)
Non-trainable params: 0 (0.00 B)

Рис. 4. Архитектура модели разработанной нейронной сети

Модель была обучена на 13 эпохах с использованием скорости обучения 0.0001 и размером пакета 16. Итоговые результаты обучения:

- Accuracy: 90,3%
- Recall: 89,8%
- Precision): 91,2%
- F1-мера: 90,5%.

Заключение

В данной статье проведен анализ существующих методов выявления вредоносных PowerShell-скриптов с использованием технологий машинного и глубокого обучения. Рассмотренные подходы, включая использование нейронных сетей различной архитектуры (CNN, RNN, LSTM), гибридных методов обработки данных и анализа семантики команд, продемонстрировали значительные успехи в повышении точности и эффективности детекции обфусцированных скриптов.

Разработанная в рамках исследования модель, основанная на глубокой нейронной сети, сочетает передовые подходы векторизации текста и архитектур нейросетей, что позволяет эффективно выявлять вредоносные PowerShell-скрипты даже при сложной обфускации и внедрении вредоносных фрагментов в легитимные сценарии. Проведенные эксперименты подтвердили высокую точность и надежность предложенного решения, которое достигает 90,3% точности классификации.

Таким образом, разработанная модель демонстрирует высокую точность и надежность в выявлении вредоносных PowerShell-скриптов, что делает её эффективным инструментом для противодействия современным угрозам.

Литература

1. *Hendler D., Kels S., Rubin A*. Proceedings of the 2018 on Asia Conference on Computer and Communications Security – ASIACCS-2018: Detecting Malicious PowerShell Commands using Deep Neural Networks // ASIACCS. 2018, pp. 187-197.

2. *Fang Y., Zhou X., Huang C*. Deep Learning for Cyber Security Applications: A Comprehensive Survey // Neurocomputing. No. 448. 2021, pp. 30-39.

3. Using the Power of Deep Learning for Cyber Security (Part 2) – Must-Read for All Data Scientists / [Электронный ресурс] // analyticsvidhya: [сайт]. URL: https://www.analyticsvidhya.com/blog/2019/05/using-power-deep-learning-cyber-security-2/ (дата обращения: 20.11.2024).

4. *Исхаков А.А., Махмутова А.З., Аникин И.В*. Выявление ложноположительных инцидентов кибербезопасности на основе искусственных нейронных сетей // ИВД. 2024. №8 (116). URL: https://cyberleninka.ru/article/n/vyyavlenie-lozhnopolozhitelnyh-intsidentov-kiberbezopasnosti-na-osnove-iskusstvennyh-neyronnyh-setey (дата обращения: 19.11.2024).

5. *Shay K., Rubin A.* Deep learning rises: New methods for detecting malicious PowerShell // Microsoft: [сайт]. URL: https://www.microsoft.com/en-us/security/blog/2019/09/03/deep-learning-rises-new-methods-for-detecting-malicious-powershell/ (дата обращения: 19.11.2024).

6. *Bruno J*. Predict the Future! A universal approach to detecting malicious PowerShell activity // Medium: [сайт]. URL: https://medium.com/@jvmbruno/predict-the-future-a-universal-approach-to-detecting-malicious-powershell-activity-640f9d08a719 (дата обращения: 20.11.2024).

7. mpsd / GitHub: [сайт]. URL: https://github.com/das-lab/mpsd (дата обращения: 20.11.2024).

РАЗРАБОТКА КАБЕЛЬНОЙ ЧАСТИ ВЧ-ТРАКТА ТЕЛЕКОМАНДНОЙ СИСТЕМЫ

Кудряшова Анастасия Юрьевна
доцент кафедры ОТС МТУСИ, к.т.н., н.с., Москва, Россия;
доцент кафедры 402 МАИ, к.т.н., Москва, Россия
a.i.kudriashova@mtuci.ru

Макеев Алексей Михайлович
специалист кафедры 402 МАИ, Москва, Россия,
makeichik2000@mail.ru

Аннотация
Работа посвящена исследованию и выбору кабельной сети ВЧ-тракта телекомандной системы, расчёту потерь в ВЧ-тракте от приемо-передающего устройства до усилителя мощности, исходя из значения мощности на выходе приемо-передающего устройства получить значение мощности на входе усилителя мощности.

***Ключевые слова**: телекомандная система, кабельная сеть, спутниковая связь.*

Разработка кабельной части ВЧ-тракта ТКС

1. Необходимо рассчитать потери в ВЧ-тракте от ППУ до УМ, исходя из значения мощности на выходе ППУ получить значение мощности на входе УМ.

Исходные данные:

– мощность сигнала на выходе ТКС;

– характеристики ППУ (мощность сигнала на выходе);

– характеристики сумматора разветвителя (затухание сигнала);

– элементная база (типы кабелей, их характеристики: затухание, материал для радиационной защиты, гибкость, вес, экран; разъёмы на кабели)

2. На рисунке 1 изображена схема ВЧ-тракта ТКС на ней изображены: ППУ-S (приёмо-передающее устройство), $СР_{ОК}$ и $СР_{ЗК}$ (сумматор разветвитель), ТУМ1 и ТУМ2 (твердотельный усилитель мощности), фильтр.

ППУ-S (приёмо-передающее устройство) предназначен для приема радиосигнала в S-диапазоне частот ($F_{ЗК}$ – запросный канал), а также для формирования радиосигнала в данном диапазоне ($F_{ОК}$ – ответный канал).

Сформированный радиосигнал поступает на вход ТУМ1 и ТУМ2 через сумматор разветвитель $СР_{ОК}$. Данная схема позволяет осуществить ненагруженное резервирование ответного канала.

Длины кабелей выбраны исходя из требований по компоновке космического аппарата (КА).

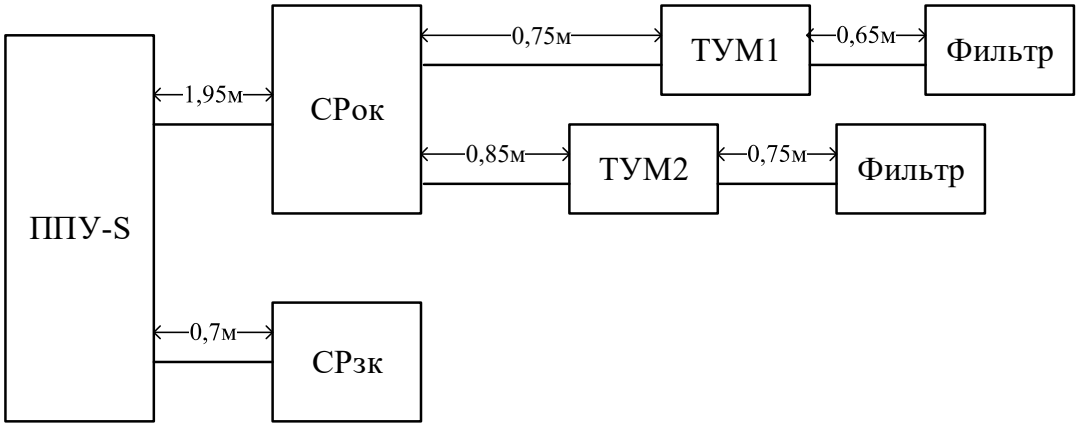


Рис. 1. ВЧ-тракт ТКС

3. Для разработки кабельной части ВЧ-тракта необходимо учитывать следующие факторы:

• Затухание – это потери энергии, проходящей через среду передачи, между источником и приёмником. Затухание должно обеспечивать необходимый диапазон мощности на входе ТУМ;

• Материал должен обеспечивать стойкость к внешним воздействующим факторам в особенности стойкость к радиационным воздействиям;

• Для удобства сборки космического аппарата и надёжности кабель должен быть гибким;

• Кабель должен обладать минимально возможной массой;

• Кабель должен входить в состав перечня электронной компонентной базы, разрешенной для применения при разработке, модернизации, производстве и эксплуатации вооружения, военной и специальной техники;

• Рабочая температура для кабеля должна включать диапазон от - 10°С до +50 °С.

4. Характеристики модулей ТКС, необходимые для расчёта ВЧ-тракта, приведены в таблице 1.

Таблица 1

Характеристики ТКС, необходимые для расчёта ВЧ-тракта

	Выходная мощность, дБм	Потери, дБм	Входная мощность, дБм
ППУ-S	10-15	0,3 (выходной разъём)	-
СР	-	6 (разъёмы +СР)	-
ТУМ	-	0,3 (входной разъём)	0-5,1

Частота ответной радиолинии (линия «Космос-Земля») ТКС составляет 2 ГГЦ.

5. Анализ перечня ЭКБ 17-2022.

Проанализировав перечень ЭКБ «Часть 17 Кабели, провода и шнуры электрические» по характеристикам, приведенным в п.3 были выбраны следующие кабели:

Таблица 2

Основные характеристики выбранных кабелей

Наименование кабеля	Обозначение документа на поставку	Испытательное напряжение, кВ	Коэффициент затухания, дБ/м, не более (при частоте, ГГц)	Диапазон рабочих температур, °С	Масса, кг/км
РК50-4-420С	ФЖТК.358800.089ТУ	5	0,35 (при 1 ГГц) 1,01 (при 10 ГГц)	от -60 до +165	85
РК50-2-22	ГОСТ ВД 11326.74-79	2,2	2 (при 3 ГГц)	от -60 до +200	25,1
РК50-2-42-С	ДКЮГ.358800.030ТУ	4	0,4 (при 1 ГГц) 1,2 (при 10 ГГц)	от -60 до +165	42

Основными материалами, использующихся в качестве изоляции кабелей являются ПЭТФ, ПЭ и ПТФЭ [1-2]. Важным параметром является устойчивость к воздействию ионизирующего излучения. Эти материалы обладают различными характеристиками радиационной стойкости, которые зависят от типа и структуры полимеров.

ПЭТФ (полиэтилентерефталат) обладает высокой радиационной стойкостью благодаря своей плотной структуре и отсутствию двойных связей в молекулах. Он сохраняет свои механические, электрические и оптические свойства даже при воздействии высоких доз радиации.

Полиэтилен (ПЭ) при воздействии ультрафиолетового излучения начинает разрушаться, что не позволяет использовать данный материал в качестве изоляции кабелей в космической технике, подверженной ионизирующему излучению.

ПТФЭ (политетрафторэтилен) имеет самую высокую радиационную стойкость среди рассматриваемых материалов. Его молекулы содержат большое количество атомов фтора, которые образуют плотную оболочку вокруг углеродного ядра, обеспечивая защиту от воздействия радиации. В связи с этим ПТФЭ является предпочтительным материалом, в качестве изоляции кабелей в космической технике.

6. Расчёт потерь в тракте, массы и затухания кабелей при рабочей частоте бортовой аппаратуры.

Проанализировав документацию на поставку изделий [3-5], были выявлены характеристики затуханий кабелей на определенных частотах, указанных в таблице 2.

Данные характеристики не позволяют определить затухание кабелей бортовой аппаратуры при его рабочей частоте [6-8]. Требуется расчёт затухания выбранных кабелей при частоте равной 2 ГГц.

Учитывая, что характеристика затухания кабеля РК50-2-22 указана при 3 ГГц, что близко к необходимому значению частоты, то рассчитаем данную характеристику, исходя из соображения равного отношения затухания (при близкой к 3 ГГц частоте) к рабочей частоте.

$$k = \frac{\beta_{\text{при 3 ГГц}}}{f} = \frac{2}{3} = 0{,}667\ ,$$

где k – отношение затухания к рабочей частоте, f – рабочая частота.

$$k = \frac{\beta_{\text{при 2 ГГц}}}{f} = 0{,}667\ ,$$

$$\beta_{\text{при 2 ГГц}} = 0{,}667 \cdot 2 = 1{,}334$$

Для кабелей РК50-4-420С и РК50-2-42-С даны две точки, отображающие зависимость затухания кабеля указана при определённой частоте. Это позволяет более точно высчитать затухание кабеля исходя из линейной зависимости затухания от частоты [9-11].

На рисунке 2 изображено изменение затухания относительно рабочей частоты.

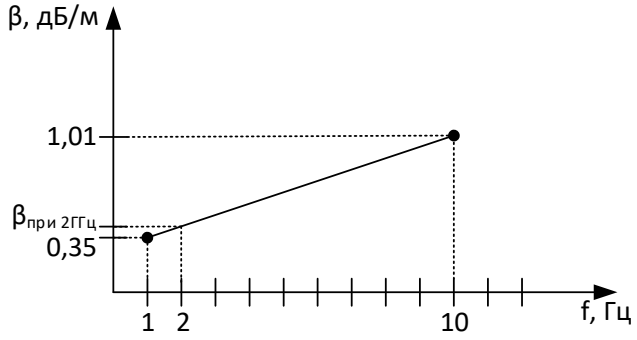


Рис. 2. Зависимость затухания от частоты для кабеля РК50-4-420С

Для вычисления $\beta_{\text{при 2 ГГц}}$ необходимо определить изменения затухания в зависимости от изменения частоты следующим образом:

$$\Delta\ = \frac{1{,}01 - 0{,}35}{10 - 1} = 0{,}073$$

$\beta_{\text{при 2 ГГц}}$ рассчитывается по следующей формуле:

$$\beta_{\text{при 2 ГГц}} = 0{,}35\ +\ \Delta \cdot (2 - 1) = 0{,}42\ \text{дБ/м}$$

Аналогичным образом рассчитаем для РК50-2-42-С:

$$\Delta\ = \frac{1{,}2 - 0{,}4}{10 - 1} = 0{,}089$$

$\beta_{\text{при 2 ГГц}}$ рассчитывается по следующей формуле:

$$\beta_{\text{при 2 ГГц}} = 0{,}4\ +\ \Delta \cdot (2 - 1) = 0{,}489\ \text{дБ/м}$$

Потери на кабеле рассчитываются умножением затухания на длины кабелей.

Масса кабеля высчитывается по следующей формуле:

$$m \cdot L$$

l рассчитывается исходя из рисунка 1, m дано в таблице 2.

Масса кабеля РК50-2-22: $25{,}1 \cdot 0{,}0028 = 0{,}07$ кг.

Масса кабеля РК50-4-420С: $85 \cdot 0{,}0028 = 0{,}238$ кг.

Масса кабеля РК50-2-42-С: $42 \cdot 0{,}0028 = 0{,}118$ кг.

Потери в тракте высчитываются суммированием потерь на выходном разъёме ППУ-S, входном разъёме ТУМ, суммарные потери СР и потери в кабелях.

7. Итоговые значения массы и потерь кабелей, а также потери в тракте указаны в таблице 3.

Под необходимые условия подошёл кабель РК50-2-22, так как он соответствует входной мощности ТУМ и его масса меньше всех остальных, что является одним из важных критериев при проектировании кабельной сети.

Таблица 3

Итоговые значения массы, потерь кабелей и потери в тракте

Кабель	Гибкость	Затухание при 3 ГГц, дБ/м		Затухание при 2 ГГц, дБ/м	Суммарная длина кабелей от ППУ до СР и от СР до ТУМ	Потери в тракте, дБ	Минимальная выходная мощность ППУ, дБм	Максимальная выходная мощность ППУ, дБм	Входная мощность УМ, дБм	Входная мощность УМ, мВт	Масса на 1 км	Масса для нашей длины, кг
РК50-2-22	Гибкий	2		1,33	2,8	10,024	10	15	-0,024	0,994489	25,1	0,07028
									4,976	3,14485		
		Затухание при 1 ГГц, дБ/м	Затухание при 10 ГГц, дБ/м	Затухание при 2 ГГц, дБ/м		7,476						
РК50-4-420С	Гибкий	0,35	1,01	0,42					2,524	1,788134	85	0,238
									7,524	5,654575		
		Затухание при 1 ГГц, дБ/м	Затухание при 10 ГГц, дБ/м	Затухание при 2 ГГц, дБ/м		7,6692						
РК50-2-42-С	Гибкий	0,4	1,2	0,489					2,3308	1,71033	42	0,118
									7,3308	5,408539		

Литература

1. Спутниковые системы связи: Учебное пособие для вузов / Под ред. *А. М. Сомова*. М.: Горячая линия – Телеком, 2012. 244 с.

2. *Макаренко С.И.* Описательная модель системы спутниковой связи Инмарсат // Системы управления, связи и безопасности. 2018. № 4. С. 64-91.

3. ФЖТК.358800.089ТУ.

4. ГОСТ ВД 11326.74-79.

5. ДКЮГ.358800.030ТУ.

6. *Харченко К.П.* УКВ антенны. М. ДОСААФ, 1969. 112 с.

7. *Виноградов А.Ю., Кабетов Р.В., Сомов А.М.* Устройства СВЧ и малогабаритные антенны: Учебное пособие / Под ред. А.М. Сомова. М.: Горячая линия – Телеком, 2012. 440 с.

8. *Лаврецкий Е.И., Чернышов В.С.* Расчет двузеркальной антенны по методу физической оптики с учетом многократных переотражений // Журнал радиоэлектроники. 2022. № 1. DOI 10.30898/1684-1719.2022.1.5.

9. *Сомов А.М., Старостин В.В., Кабетов Р.В.* Антенно-фидерные устройства: Учебное пособие / Под ред. А.М. Сомова. М.: Горячая линия – Телеком, 2011. 404 с.

10. *Петушков С.В*. Адаптивное устройство предыскажающей линеаризации для бортовых радиопередающих устройств // Наукоемкие технологии в космических исследованиях Земли. 2020. Т. 12. № 6. С. 11-17.

11. *Михайлов В.Ф., Мажник И.В.* Влияние неоднородной теплозащиты на характеристики излучения антенны космического аппарата // Наукоемкие технологии в космических исследованиях Земли. 2023. Т. 15. № 3. С. 4-10.

ОБЗОР ВОЗМОЖНОСТИ ОПРЕДЕЛЕНИЯ СКРЫТОГО ПОДКЛЮЧЕНИЯ НА ОСНОВЕ TLS РУКОПОЖАТИЯ

Романов Станислав Викторович
Московский технический университет связи и информатики, Москва, Россия,
stas.romanov-stas@yandex.ru

Аннотация
Определение фактов скрытия сетевого трафика является затруднительным для современных средств классификации сетевого трафика. Проблему решает анализ поведенческих характеристик сетевых потоков для определения факта шифрования и туннелирования. ***Цель исследования*** *- проанализировать возможность определения скрытого подключения на основе поведенческих характеристик скрываемых подключений. По результатам исследования обнаружена возможность определения фактов использование скрытия туннелирования трафика на основе сравнения поведенческих признаков сетевых потоков зашифрованных подключений с признаками TLS рукопожатия. Основным признаком является ряд размеров пакетов, передаваемых между конечным устройством и удаленным ресурсом, выступающим в качестве посредника. Собранные данные возможно отформатировать в датасет, на основе которого возможно дальнейшее исследование автоматизированного определения фактов скрытия использования туннелирования. Существующие реализации обфускации трафика в базовой конфигурации не меняют поведенческие характеристики, которые выражаются в скрываемых подключениях. Следовательно, с развитием данных реализаций скоро появится необходимость в поиске других признаков зашифрованного сетевого трафика, отражающих использования туннелирования.*

Ключевые слова: *информационная безопасность, протокол TLS, туннелирование трафика, цифровой отпечаток.*

Введение

Обеспечение информационной безопасности в системе предполагает защиту каналов связи [1]. Методы защиты включают использование шифрующих методов туннелирования для сокрытия содержимого передаваемой информации от третьих лиц [2-3].

Согласно законодательству Российской Федерации, а также Приказу Роскомнадзора, нелицензированное использование протоколов шифрования является незаконным и блокируется Техническими Средствами Противодействия Угрозам (ТСПУ) [4].

Однако выявление фактов использования протоколов шифрования среди общего потока сетевого обмена сообщениями представляет собой сложную задачу, обусловленную недостаточным уровнем развития методологии обнаружения такого трафика [5]. Данная задача усложняется с совершенствованием обфускации зашифрованного трафика под легитимные сообщения [6].

Таким образом актуализируется необходимость оперативного определения зашифрованного трафика в высоконагруженных сетях.

Методы определения неправомерного доступа

Системы управления сетевым трафиком, в том числе ТСПУ, основаны на методах анализа статических признаков для принятия решений о блокировке соединений [7-8]. Среди этих признаков выделяются:

- IP-адрес – определение и блокировка просты в реализации, однако возможно блокирование доступа к разрешенным ресурсам;
- Поля запросов HTTP – определение и блокировка требуют считывание полей HTTP, однако в настоящее время протокол HTTP без TLS почти вытеснен более защищенными протоколами;
- Доменные имена – определение и блокировка требуют считывания и подмены запросов и ответов Domain Name Service (DNS);
- TLS – определение и блокировка требуют считывания полей TLS SNI при их наличии, либо полей сертификата сервиса;

- Протоколы – определение и блокировка требуют считывания определяющих статических байтов, характерным стандартным протоколом шифрования и туннелирования, включая OpenVPN, Wireguard и IPSec [9-10].

Описанные выше характеристики позволяют определять прямой трафик к удаленным ресурсам, а также определять подключения, использующие не сокрытые протоколы шифрования [11]. Они позволяют блокировать высоко нагружающие протоколы вида BitTorrent, а также открытые протоколы туннелирования [12]. Однако, современные протоколы обхода блокировок используют обфускацию под TLS трафик обозревателей сети Интернет для сокрытия факта использования методов туннелирования [13].

Методы обхода блокировки доступа

В целях обхода запретов доступа к определённым удалённым ресурсам пользователи применяют различные инструменты шифрования и обфускации сетевого трафика [14]. Данные средства включают в себя:

- GoodbyeDPI – утилита для модификации передаваемых пакетов путем фрагментации и модификации TCP-пакетов, что позволяет запутывать ТСПУ и других систем, использующих Deep Packet Inspection (DPI) для определения и классификации сетевого трафика;
- AmneziaWG – протокол, используемый решением Amnezia, подменяющий стандартные определяемые байты протокола WireGuard;
- V2Ray, а также XRay – Набор протоколов и решений, а также графических интерфейсов, предоставляющих реализацию и конфигурацию протоколов VMESS, VLESS и XTLS;
- Sing-box – клиент-серверное решение, предоставляет развертывание конфигурируемых соединений, используя протоколы Trojan, Hysteria 2, Naive и другие варианты прокси-соединений.

Стоит отметить, что русские и западные решения предлагают незначительные изменения в существующих протоколах шифрования и туннелирования, в то время как китайские методы полностью скрывают трафик [15], предоставляя его как обычное TLS-подключение интернет-обозревателя. Также реализованы варианты частичного шифрования, скрывающие только часть пакетов, а также шифруя метаданные, используемые для определения сторон передачи информации [16-17].

Полная инкапсуляция позволяет спрятать содержимое передаваемых сообщений, что является более защищённым, но и более затратным методом обфускации сетевого трафика по сравнение с изменения метаданных пакетов. Например, фрагментация TCP-пакетов, предлагаемая GoodbyeDPI, будет менее эффективной с увеличением производительности ТСПУ, а методы модификации пакетов, в силу соблюдения лимитов толерантности HTTP/1.1, используемые данной утилитой, ограничены [7].

Однако, обнаружение обфусцированных под трафик TLS сетевых соединений требует новых методов классификации зашифрованного трафика, основанных на устойчивых поведенческих информационных признаков данных подключений.

Цель работы – определить возможность применения методов машинного обучения на базе анализа сетевого трафика, сокрытого методами шифрования под TLS трафик интерактивных приложений.

Обнаружение методов обфускации сетевого трафика

Во время туннелирования сетевого трафика в случаях использования прокси-протоколов выполняется инкапсуляция пользовательского трафика в протокол TLS или другой пользовательский протокол, использующий шифрование содержимого. Примерами такой инфраструктуры являются TLS-over-TLS и TLS-over-Unknown.

Инкапсулированный трафик TLS является достаточно уникальным в применении среди всего сетевого трафика и обнаруживается в случаях туннелирования. Протокол TLS можно определить с помощью поведенческих характеристик, выявляемых во время установления соединения:

- Размер сообщений ClientHello составляет до 1 килобайта и имеет стандартный формат, в то время как ServerHello имеет размер в несколько килобайт и большую вариативность;
- Алгоритм рукопожатия выполняется строго по порядку, что позволяет определить признаки соединения без необходимости фильтровать сообщения;

- Процесс рукопожатия происходит независимо от инкапсуляции сетевого трафика, что сохраняет поведенческие характеристики независимо от применяемого протокола обфусцирования [18];
- Применение TLS и инициализация рукопожатия зависит от конечной точки подключения,в связи с чем его определение является независимым от применяемого протокола обфусцирования [19].

Вследствие данных характеристик возможно идентифицировать наличие инкапсуляции TLS в конкретных соединениях на основе стандартных поведенческих признаков рукопожатия TLS. На рисунке 1 представлена передача сообщений внутри протокола обфускации на базе TLS over TLS, где красным цветом отмечены сообщения, которые являются зашифрованными, но всегда следуют закономерности в порядке и формате [20].

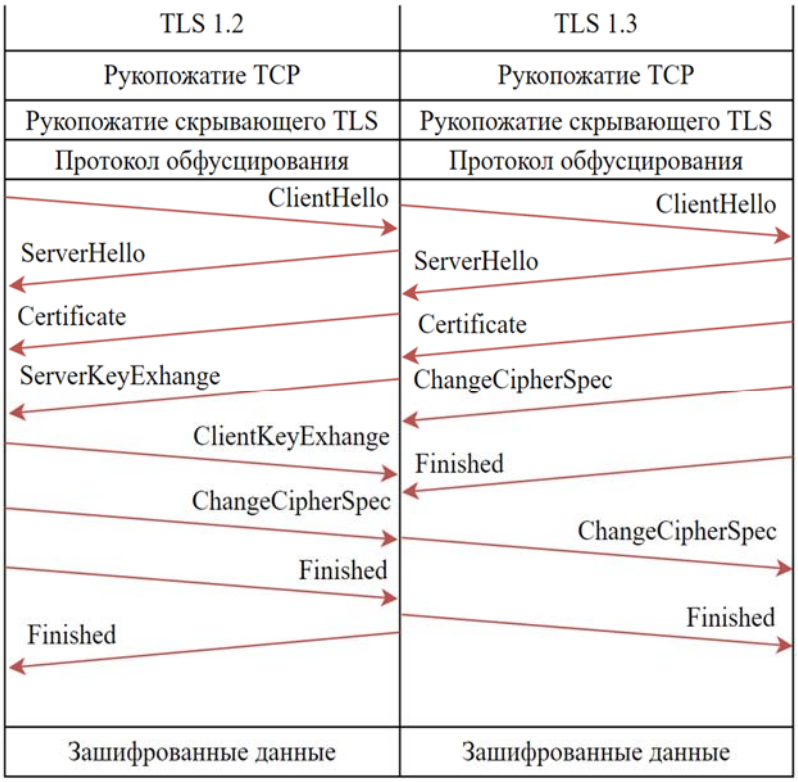


Рис. 1. Рукопожатие TLS в потоке TLS over TLS

Таким образом, определение обфусцированного сетевого соединения заключается в выполнении следующего алгоритма:

1. Определение зашифрованного соединения;
2. Считывание поведенческих признаков обнаруженного соединения;
3. Сверка поведенческих признаков соединения с признаками алгоритма рукопожатия TLS;
4. Определение соединения как обфусцированное при совпадении значений признаков.

Этот алгоритм можно представить как бинарную классификацию, где принятие решения об определении зашифрованного соединения зависит от дистанции значений признаков обнаруженного соединения от значений стандартного TLS-рукопожатия.

Важно отметить, что при классификации необходимо снизить ошибку второго рода, которая обозначается классификацией прямого TLS подключения как сетевого трафика, содержащего туннелирование. Данная ошибка может привести к блокировке разрешенных, а также критических соединений [21].

В свою очередь, относительно частое использование протоколов обфусцирования для соединения с прокси-сервером создаёт огромное число соединений, содержащих TLS-рукопожатие. Следственно, при анализе допускается высокий процент ошибки первого рода.

Сбор данных

Для анализа необходимо собрать тестовые данные. Для сбора данных сетевого потока была использована модель, схематично отраженная на рисунке 2. Зеленым цветом отмечены потоки данных, содержащие прямые подключения к удаленным серверам, красным – потоки данных протоколов обфусцирования, а синим – прямые потоки данных вторичных устройств наблюдаемой сети.

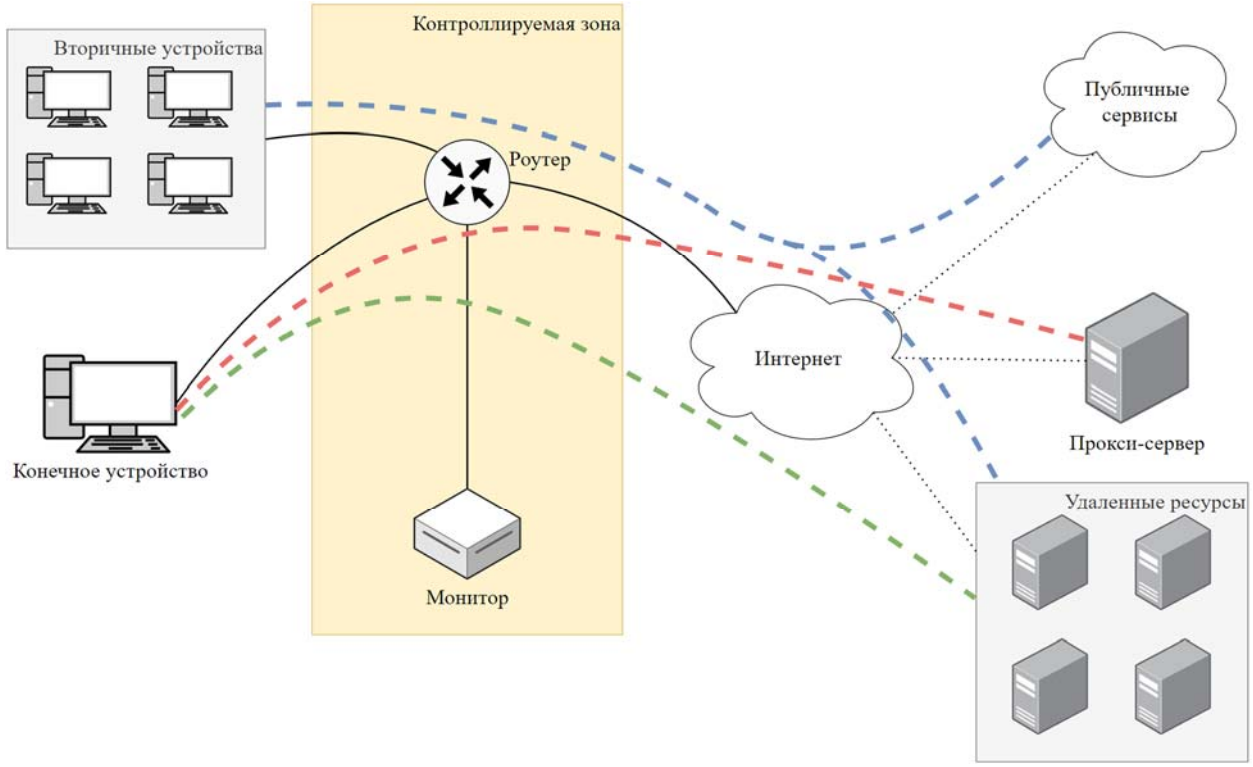


Рис. 2. Логическая схема сбора датасета

Каждый из удаленных ресурсов, отраженных на схеме, содержит два одинаковых сервера с разными доменные именами. Пользовательское устройство и прокси-сервер используют утилиту sing-box, сконфигурированную на использование VLESS over TLS. Вторичные устройства подключаются к публичным сервисам сети Интернет, а также к удаленным ресурсам гарантированно без конфигурации прокси-протоколов. Монитор собирает данные о сетевых потоках, проходящих по маршрутизатору. Все подключения автоматизированы при помощи Selenium. По завершению тестирования монитор сохраняет информацию в файл в формате .pcapng.

Анализ сетевого трафика

Полученные данные были отфильтрованы, сохранив только релевантные TCP соединения между конечным устройством и удаленными ресурсами. Второй этап фильтрации отфильтровал данные по периодам времени, оставляя только 3 секунды с момента инициализации каждого подключения.

На основе анализа трафика без использования решения sing-box были получены средние значения поведенческих характеристик рукопожатия TLS. Следующим шагом были определены пакеты TLS рукопожатия в соединениях к прокси-серверу. Поиск пакетов инициализации выполнялся по следующему алгоритму:

- Определения начала соединения;
- Фильтрация пакетов инициализации внешнего TLS подключения;
- Агрегация пакетов, имеющих максимальный размер и идущих подряд;
- Определение ряда пакетов, каждый из которых весит больше, чем аналогичный в контексте прямого подключения, на 10%;

- Сверка определенных пакетов с расшифрованным на конечных устройствах для проверки корректности классификации сетевого потока.

При успешном определении из ряда пакетов выделяются следующие характеристики: размер пакетов, количество пакетов в алгоритме инициализации, соотношение количества принимаемых и отправляемых пакетов. Средние показатели трафика отражены на таблице 1.

Таблица 1

Результаты анализа сетевого трафика

Метрика	Прямое подключение	Прокси-подключение
Средний размер сообщения ClientHello, байт	642,4	712,3
Средний размер сообщения ServerHello, байт	2674,7	4103,1
Среднее количество пакетов, шт	4,2	6,7
Соотношение отправляемых и получаемых пакетов	1,34	1,39
Определенные инициализации TLS, %	100	85

Результаты анализа показывают, что определение зашифрованного TLS рукопожатия на основе поведенческих признаков рукопожатия TLS подключения является более чем возможным. Из всех признаков более выраженными являются размер сообщений, а также количество передаваемых пакетов. К сожалению, соотношение передаваемых пакетов не является достаточно выраженной метрикой для использования в качестве метрики автоматизированного определения.

Заключение

Результаты проведенного эксперимента свидетельствуют о перспективности применения методов машинного обучения для выявления обфусцированного трафика. Классификация на основе поведенческих отпечатков обфусцированного сетевого трафика позволяет определять факт скрытия туннелирования подключений.

Однако для дальнейшего совершенствования данных методов необходимо провести дополнительные исследования, направленные на выявление иных закономерностей, характерных для применения методов обфускации, а также на разработку более устойчивых к методам, изменяющим поведенческие характеристики сетевого потока.

В связи с постоянным развитием методов и решений обхода блокировки доступа, логично предположить, что требуется поиск новых признаков сетевого трафика, позволяющих определять факт скрытия сетевых подключений, независящих от поведенческих характеристик передачи пакетов.

Литература

1. *Кривоносова Н.В*. Моделирование вирусных войн как инструмент защиты сетевого ресурса телекоммуникационных систем // Актуальные вопросы развития систем и сетей связи : Сборник материалов Всероссийской научно-технической конференции, Ставрополь, 10-20 ноября 2023 г. Ставрополь: Северо-Кавказский федеральный университет, 2023. С. 216-218. EDN SZKHHN.

2. *Когос К.Г.* Математическая модель скрытого канала в сетях пакетной передачи данных // Информационная безопасность : Сборник докладов Всероссийской Школы молодых ученых, Новосибирск, 14-18 ноября 2022 г. Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2022. С. 10-18. DOI:10.55648/978-5-91434-080-0-2022-10-18. EDN LEDCPG.

3. *Xue D.* et al. TSPU: Russia's decentralized censorship system // Proceedings of the 22nd ACM Internet Measurement Conference. 2022. С. 179-194. https://dl.acm.org/doi/pdf/10.1145/3517745.3561461

4. *Гусев А.С., Мартынова И.С., Казак И.Б.* Действие норм цифрового права в пространстве // Аграрное и земельное право. 2024. № 3(231). С. 74-75. DOI:10.47643/1815-1329_2024_3_74. EDN OPQTOO.

5. *Лавриенко А.Д., Каштанов В.В., Алферов Ю.В.* Применение методов машинного обучения для определения вредоносного трафика в шифрованном сетевом трафике // Информационная безопасность и защита персональных данных. Проблемы и пути их решения : сборник материалов и докладов XVI межрегиональная научно-практическая конференция, Брянск, 29 апреля 2024 г. Брянск: Брянский государственный технический университет, 2024. С. 143-146. EDN TBVSRR.

6. *Fenske E., Johnson A*. Security notions for fully encrypted protocols // Free and Open Communications on the Internet. 2023. Vol. 1, pp. 24-29 https://petsymposium.org/foci/2023/foci-2023-0004.pdf (Дата обращения 01.11.2024).

7. *Ишкуватов С.М., Бегаев А.Н., Комаров И.И., Левко И.В*. Метод обнаружения фактов обхода блокировок ресурсов сети Интернет // Вопросы кибербезопасности. 2024. № 3(61). С. 76-84. DOI:10.21681/2311-3456-2024-3-76-84. EDN YQZJHU.

8. *Гурьев Н.А., Старун И.Г., Югансон А.Н*. Признаки использования VPN соединения // Сборник трудов IX Конгресса молодых ученых, Санкт-Петербург, 15-18 апреля 2020 г. Том 1. Университет ИТМО, Санкт-Петербург: федеральное государственное автономное образовательное учреждение высшего образования "Национальный исследовательский университет ИТМО", 2021. С. 134-136. EDN DHEPGN.

9. *Гетьман А.И., Маркин Ю.В., Евстропов Е.Ф., Обыденков Д.О.* Обзор задач и методов их решения в области классификации сетевого трафика // Труды Института системного программирования РАН. 2017. Т. 29, № 3. С. 117-150. DOI:10.15514/ISPRAS-2017-29(3)-8. EDN YUFLVX.

10. *Гетьман А.И., Иконникова М.К*. Обзор методов классификации сетевого трафика с использованием машинного обучения // Труды Института системного программирования РАН. 2020. Т. 32, № 6. С. 137-154. DOI:10.15514/ISPRAS-2020-32(6)-11. EDN QYCRVZ.

11. *Яблоков Д.С*. Традиционные методы классификации сетевого трафика // Тенденции развития науки и образования. 2024. № 114-9. С. 166-169. DOI 10.18411/trnio-10-2024-417. EDN FMCWBO.

12. *Dong Sh., Xia Yu*. Network traffic identification in packet sampling environment // Digital Communications and Networks. 2023. Vol. 9, No. 4, pp. 957-970. DOI:10.1016/j.dcan.2022.02.003. EDN NOIUFU.

13. *Тятюков Р.Л., Шкаев Р.Е., Калинин Д.А*. и др. Исследование безопасности VPN на VLESS с XTLS-reality // Математика и математическое моделирование : Сборник материалов XVIII Всероссийской молодёжной научно-инновационной школы, Саров, 10-12 апреля 2024 г. Саров: ООО "Интерконтакт", 2024. С. 368-369. EDN LTMYMH.

14. *Stadler R., Steger L*. Survey on the Chinese Governments Censorship Mechanisms // Network 65. 2023. URL: https://www.net.in.tum.de/fileadmin/TUM/NET/NET-2023-06-1/NET-2023-06-1_12.pdf (Дата обращения 08.11.2024)

15. *Alice Bob, Carol Beznazwy J., Houmansadr A.* How China detects and blocks Shadowsocks // Proceedings of the ACM Internet Measurement Conference. 2020. URL: https://gfw.report/publications/imc20/data /paper/shadowsocks.pdf (дата обращения 01.11.2024).

16. *Frolov S., Wustrow E*. HTTPT: A Probe-Resistant Proxy // 10th USENIX Workshop on Free and Open Communications on the Internet (FOCI 20). 2020. https://www.usenix.org/system/files/foci20-paper-frolov.pdf (дата обращения 08.11.2024).

17. *Satija S., Chatterjee R.* BlindTLS: Circumventing TLS-based HTTPS censorship // Proceedings of the ACM SIGCOMM 2021 Workshop on Free and Open Communications on the Internet. 2021. С. 43-49. https://dl.acm.org/doi/abs/10.1145/3473604.3474564

18. *Шамсимухаметов Д.Р., Курапов А.А., Любогощев М.В., Хоров Е.М.* Неразличимость трафика по открытым параметрам TLS при использовании Encrypted ClientHello // Информационные процессы. 2023. Т. 23, № 2-1. С. 231-240. DOI:10.53921/18195822_2023_23_2_231. EDN OWPLIR.

19. *Perugini L., Vesco A*. On the integration of Self-Sovereign Identity with TLS 1.3 handshake to build trust in IoT systems // Internet of Things. 2024. Т. 25. С. 101103. https://doi.org/10.1016/j.iot.2024.101103

20. *Виноградов С.Э*. Сетевой протокол TLS // Международная научно-техническая конференция молодых ученых БГТУ им. В.Г. Шухова, посвященная 170-летию со дня рождения В.Г. Шухова : Сборник докладов, Белгород, 16-17 мая 2023 г. Том Часть 20. Белгород: Белгородский государственный технологический университет им. В.Г. Шухова, 2023. С. 66-70. EDN XCWIZN.

21. *Xue D., Ramesh R., Jain A. et al.* OpenVPN is Open to VPN Fingerprinting // Association for Computing Machinery. Communications of the ACM. 2024. DOI:10.1145/3618117. EDN MKFVWU.