СПОСОБ УСТОЙЧИВОЙ К ДЕСТРУКТИВНЫМ ВОЗДЕЙСТВИЯМ ПЕРЕДАЧИ ИНФОРМАЦИИ ПО КАНАЛАМ СВЯЗИ ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ

Карпов С.С., Рябинин Ю.Е.

Краснодарское высшее военное орденов Жукова и Октябрьской революции Краснознамённое училище имени генерала Армии С.М.Штеменко,
Россия, г. Краснодар, ул. Красина, д. 4
karpov.sergey.sergeevich@yandex.ru, jurandvau@inbox.ru,

Финько О.А.

Краснодарское высшее военное орденов Жукова и Октябрьской Революции Краснознамённое училище имени генерала армии С.М.Штеменко,
Россия, г. Краснодар, ул. Красина, д. 4;
Северо-Кавказский федеральный университет,
Россия, г. Ставрополь, ул. Пушкина, д. 1;
Российская академия ракетных и артиллерийских наук (РАРАН),
г. Москва, 1-я Мясниковская ул., д. 3, стр. 3
ofinko@yandex.ru

Аннотация: Рассматривается способ обеспечения устойчивого обмена данными в виртуальных частных сетях крупномасштабных информационных систем, функционирующих в условиях деструктивных информационно-технических воздействий злоумышленника. Предлагаемый способ позволяет восстанавливать информационные пакеты, подвергнутых стираниям и имитации.

Ключевые слова: безопасность и защита информации, виртуальные частные сети, криптографическая имитовставка, стирание пакетов, помехоустойчивое кодирование, защита VPN от киберугроз.

Введение

Распространение передовых достижений в сфере телекоммуникаций обуславливает переход на новый уровень автоматизации – управление интеллектуальными системами в режиме реального времени в постоянном взаимодействии с внешней средой, объединение таких систем в единую глобальную сеть [1]. За последние несколько лет запущено несколько национальных и региональных инициатив по формированию распределённых интеллектуальных систем: «Стратегия развития информационного общества в Российской Федерации на 2017 – 2030 годы», «Новая промышленная стратегия для Европы до 2030 г.», «Стратегия высоких технологий 2025» в Германии, «Industrie du Futer» во Франции. Условием реализации существующих стратегий является обеспечение защиты линий управления и обмена данными интеллектуальных систем от киберугроз.

Децентрализация систем аналитики и управленческих решений, использование облачных сервисов предполагает использование информационно-телекоммуникационной сети общего пользования (далее – ИТКС ОП) для обмена данными. Организация защищённых каналов связи в ИТКС ОП осуществляется, главным образом, с помощью технологии виртуальных частных сетей (virtual private network – VPN) [2, 3].

Модель злоумышленника для VPN предусматривает ряд угроз безопасности информации[58], реализуемых, в том числе, в результате воздействий на инфраструктуру ИТКС ОП, использования уязвимостей протоколов сетевого взаимодействия [4, 5]. Потери, превышение времени доставки пакетов, а также блокирование элементов инфраструктуры ИТКС ОП, выражаются в стирании пакетов на стороне получателя. Существующий механизм обратной связи даёт положительный результат, если стирания пакетов носят случайный характер [6]. Однако, при превышении количества стёртых пакетов в VPN допустимого уровня не может быть осуществлена удовлетворительная поддержка различных приложений[59,60].

---

[58] *Банк данных угроз безопасности информации ФСТЭК России. 27.11.2018. – URL: https://bdu.fstec.ru/threat (дата обращения: 01.02.2021).*

[59] *Об утверждении Требований к организационно-техническому обеспечению устойчивого функционирования сети связи общего пользования : Приказ Министерства информационных технологий и связи Российской Федерации от 27.09.2007 № 113. – URL: https://digital.gov.ru/ru/documents/3921/ (дата обращения: 20.02.2021).*

[60] *Рекомендация МСЭ-Т Y.1541. Требования к сетевым показателям качества для служб, основанных на протоколе IP : утверждена 12-й Исследовательской комиссией в соответствии с процедурой, изложенной в Рекомендации МСЭ-Т A.8 22 февраля 2006 г.. Швейцария Женева, 2007.*

Целью исследования является снижение вероятности неудовлетворительной поддержки и ошибок приложений за счёт *решения задачи* восстановления стёртых пакетов и повышения уровня имитозащищенности передаваемых в VPN данных.

1 Математическая модель

Рассмотрим систему передачи информации по каналам связи VPN, которая с течением времени изменяет своё состояние с некоторой вероятностью под воздействием деструктивных инициирующих событий. Формализуем рассматриваемый процесс в виде марковского процесса смены состояний и примем следующие необходимые для исследования дискретные состояния моделируемой системы:

S_1 – «работоспособное состояние» – система функционирует в нормальном режиме;

S_2 – «состояние ожидания повторно отправленных пакетов» – осуществляется информационно-техническое воздействие (ИТВ) злоумышленником на базовую сеть VPN, часть пакетов стирается, получатель ожидает повторной отправки серии пакетов от источника, число потерянных пакетов не превышает допустимый коэффициент потерь пакетов;

S_3 – «состояние ошибки» – в случае успешной имитации пакеты считаются принятыми, при дальнейшей обработке сообщения возникает ошибка, происходит перезапуск процесса передачи информации;

S_4 – «состояние неудовлетворительной поддержки приложений» – в результате ИТВ злоумышленником количество потерянных пакетов превышает допустимый коэффициент потерь пакетов, запускается процесс изменения параметров передачи информации по каналам связи VPN или повторный запуск процесса передачи информации. Граф состояний процесса функционирования системы представлен на рисунке 1.

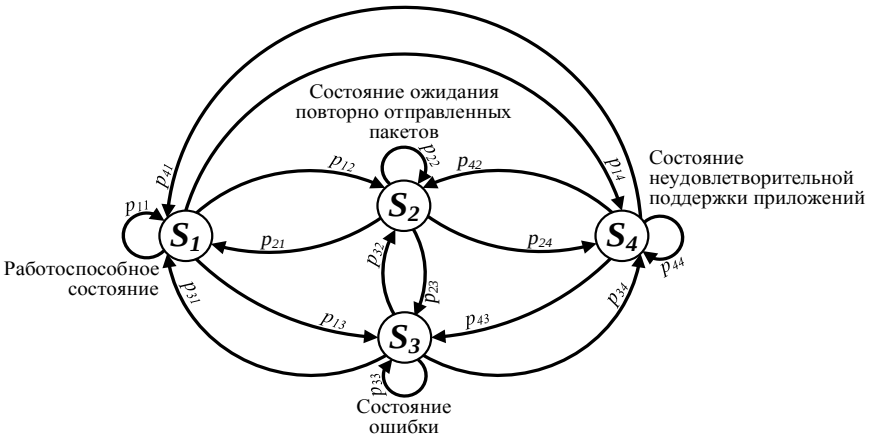

Рис. 1. Граф состояний процесса функционирования системы передачи информации по каналам связи ведомственной VPN

В начальный момент времени система находится в «работоспособном состоянии». При отсутствии деструктивных ИТВ на элементы базовой сети VPN и отсутствии имитирующих воздействий злоумышленником, система возвращается в «работоспособное состояние»: $S_1 \rightarrow S_1$, $S_2 \rightarrow S_1$, $S_3 \rightarrow S_1$, $S_4 \rightarrow S_1$.

В случае ИТВ злоумышленником на базовую сеть VPN происходят потери пакетов. Если их количество не превышает допустимый коэффициент потерь пакетов, система переходит в «состояние ожидания повторно отправленных пакетов»: $S_1 \rightarrow S_2$, $S_2 \rightarrow S_2$, $S_3 \rightarrow S_2$, $S_4 \rightarrow S_2$.

Если злоумышленнику удалось осуществить успешную имитацию пакетов передаваемого информационного сообщения, система переходит в «состояние ошибки»: $S_1 \rightarrow S_3$, $S_2 \rightarrow S_3$, $S_3 \rightarrow S_3$, $S_4 \rightarrow S_3$.

Если злоумышленнику не удалось осуществить успешную имитацию пакетов, однако, при этом, в результате ИТВ злоумышленником происходят потери пакетов, превышающие допустимый коэффициент потери пакетов, система переходит в «состояние неудовлетворительной поддержки пакетов»: $S_1 \rightarrow S_4$, $S_2 \rightarrow S_4$, $S_3 \rightarrow S_4$, $S_4 \rightarrow S_4$.

Параметры переходов $S_i \rightarrow S_j$ характеризуются вероятностями p_{ij}, зависящими от вероятности успешной доставки пакетов в условиях ИТВ злоумышленником, интенсивности имитации пакетов данных, вероятности успешной имитации данных злоумышленником, допустимого коэффициента

потери пакетов для обеспечения удовлетворительной поддержки различных приложений, параметров системы передачи информации по каналам связи VPN.

При допущении о пуассоновском характере процесса стираний пакетов в сети в результате ИТВ злоумышленником, вероятность того, что в системе передачи информации по каналам связи VPN отсутствуют стёртые пакеты определяется как [7]:

$$p_{\text{отс. стираний}} = e^{-\mu N},$$

где μ – вероятность стирания пакетов (коэффициент потери пакетов в сети), N – количество пакетов в последовательности (размер скользящего окна).

Вероятность того, что в системе не произошло ни одной успешной имитации пакета при передаче информационного сообщения равна:

$$p_{\text{отс. усп. имит.}} = e^{-\lambda\gamma M},$$

где λ – вероятность успешной имитации пакета данных злоумышленником, γ – вероятность имитационного воздействия злоумышленником, M – длина информационного сообщения в пакетах.

Вероятность того, что в системе количество потерянных пакетов не превышает допустимого значения, т.е. будет принято без стираний число пакетов обратное допустимому коэффициенту потери пакетов:

$$p_{\text{доп. ур. пот.}} = e^{-\mu\mu^{-1}_{\text{допустимое}}},$$

где $\mu_{\text{допустимое}}$ – допустимый коэффициент потерь пакетов, при котором обеспечивается удовлетворительная поддержка различных приложений.

Вероятности p_{11}, p_{21}, p_{31} и p_{41} того, что в системе в процессе передачи информации по каналам связи VPN осуществляется удовлетворительная поддержка различных приложений, отсутствуют стёртые и успешно сымитированные пакеты:

$$p_{11} = p_{21} = p_{31} = p_{41} = p_{\text{доп. ур. пот.}} \cdot p_{\text{отс. стираний}} \cdot p_{\text{отс. усп. имит.}}.$$

Вероятности p_{12}, p_{22}, p_{32} и p_{42} того, что в системе в процессе передачи информации по каналам связи VPN имеются стёртые пакеты в последовательности передаваемых пакетов, но осуществляется удовлетворительная поддержка различных приложений и отсутствуют успешно сымитированные пакеты:

$$p_{12} = p_{22} = p_{32} = p_{42} = p_{\text{доп. ур. пот.}} \cdot \left(1 - p_{\text{отс. стираний}}\right) \cdot p_{\text{отс. усп. имит.}}.$$

Вероятности p_{13}, p_{23}, p_{33} и p_{43} того, что в системе в процессе передачи информации по каналам связи VPN имеются успешно сымитированные пакеты:

$$p_{13} = p_{23} = p_{33} = p_{43} = 1 - p_{\text{отс. усп. имит.}}.$$

Вероятности p_{14}, p_{24}, p_{34} и p_{44} того, что в системе в процессе передачи информации по каналам связи VPN отсутствуют успешно сымитированные пакеты, но не осуществляется удовлетворительная поддержка различных приложений:

$$p_{14} = p_{24} = p_{34} = p_{44} = \left(1 - p_{\text{доп. ур. пот.}}\right) \cdot p_{\text{отс. усп. имит.}}.$$

2 Исследование модели

В целях исследования системы передачи информации по каналам связи VPN по описанному графу состояний (рис. 1) составим систему дифференциальных уравнений Колмогорова [8]:

$$\begin{cases} \frac{dP_1(t)}{dt} = -p_{12}P_1(t) - p_{13}P_1(t) - p_{14}P_1(t) + p_{21}P_2(t) + p_{31}P_3(t) + p_{41}P_4(t); \\ \frac{dP_2(t)}{dt} = -p_{21}P_2(t) - p_{23}P_2(t) - p_{24}P_2(t) + p_{12}P_1(t) + p_{32}P_3(t) + p_{42}P_4(t); \\ \frac{dP_3(t)}{dt} = -p_{31}P_3(t) - p_{32}P_3(t) - p_{34}P_3(t) + p_{13}P_1(t) + p_{23}P_2(t) + p_{43}P_4(t); \\ \frac{dP_4(t)}{dt} = -p_{41}P_4(t) - p_{42}P_4(t) - p_{43}P_4(t) + p_{14}P_2(t) + p_{24}P_2(t) + p_{34}P_3(t); \\ \frac{dP_1(t)}{dt} + \frac{dP_2(t)}{dt} + \frac{dP_3(t)}{dt} + \frac{dP_4(t)}{dt} = 1. \end{cases}$$

Изменяя параметры системы в пределах устойчивости уравнений в соответствии с условиями функционирования получены финальные вероятности нахождения системы в различных состояниях.

3 Описание предлагаемого способа

Одними из действенных методов обеспечения удовлетворительной поддержки различных приложений системой передачи информации являются методы помехоустойчивое кодирование [9] и применение имитовставки. Предлагаемое далее решение является развитием более ранее решений авторов [10-12].

Передающая сторона выполняет мониторинг канала связи виртуальной частной сети на предмет ИТВ злоумышленником посредством обратной связи или с помощью развёрнутых сенсоров в сети. В случае обнаружения таких воздействий на передающей стороне оценивают коэффициент потерь пакетов и принимают решение о применении предлагаемого способа.

Далее, определяют параметры помехоустойчивого кодирования: количество информационных пакетов *D*, количество линейно зависимых от информационных пакетов избыточных пакетов *R*, размер скользящего окна *N*. Параметры определяются согласно методике, разработанной с учётом требований нормативно-правовых актов по защите информации, соответствующей VPN, или на основании результатов моделирования деструктивного воздействия злоумышленником на конкретный объект информатизации.

Оценка коэффициента потерь пакетов в канале связи VPN может осуществляться передающей стороной с использованием моделей рабочих характеристик TCP и данных, полученных от сенсоров[61]. При отсутствии данных от сенсоров оценка качества канала может осуществляться передающей стороной путём расчёта коэффициента потерь пакетов по имеющейся статистике повторно передаваемых последовательностей пакетов:

$$\mu_{\text{потери пакетов}} = \left(1 - \frac{C}{C+L}\right)^{\frac{1}{N}},$$

где *C* – количество доставленных последовательностей пакетов, *L* – количество повторно отправленных последовательностей пакетов, *N* – размер скользящего окна в пакетах.

Далее, передаваемую последовательность сетевых пакетов делят на группы из *D* информационных пакетов. Для каждого информационного пакета H_i вырабатывают по ключу k_q ($g = 1..D$) имитовставку $I_{H_i}^{(k_g)}$, например, по ГОСТ Р 34.12-2015[62]. Имитовставка добавляется к информационным пакетам H_i:

$$H_i^{(I)} = H_i \,||\, I_{H_i}^{(k_g)},$$

где «||» – операция конкатенации.

Для каждой последовательности из *D* информационных пакетов формируют *R* избыточных пакетов линейно зависимых от *D* информационных пакетов. Проверочная матрица для формирования *R* избыточных пакетов из *D* информационных $A_{D\times R}$ отображает зависимость *R* избыточных пакетов от *D* информационных пакетов. Проверочная матрица должна соответствовать требованиям:

---

[61] *Рекомендация МСЭ-Т Y.1541. Требования к сетевым показателям качества для служб, основанных на протоколе IP : утверждена 12-й Исследовательской комиссией в соответствии с процедурой, изложенной в Рекомендации МСЭ-Т A.8 22 февраля 2006 г. Швейцария Женева, 2007.*

[62] *ГОСТ Р 34.12-2015. Информационная технология. Криптографическая защита информации. Блочные шифры : национальный стандарт Российской Федерации : издание официальное : утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 19 июня 2015 г. № 749-ст : введен впервые : дата введения 2016-01-01. – Москва: Стандартинформ, 2017.*

- все R комбинаций из D информационных пакетов должны быть различны и линейно независимы;
- комбинация информационных пакетов не может быть нулевой;
- количество единиц в строке матрицы $A_{D\times R}$ должно быть не менее $d_{\text{мин}}-1$, где $d_{\text{мин}}$ – минимальное кодовое расстояние [13].

Формирование избыточных пакетов осуществляется произведением над $GF(2)$ проверочной матрицы $A_{D\times R}$ на вектор-столбец из D информационных пакетов $H^{(I)}_{D\times 1}$:

$$W_{R\times 1} = A'_{D\times R} \otimes H^{(I)}_{D\times 1} \quad (1)$$

или решением системы из уравнений:

$$W_j = \bigoplus_{i=1}^{D} \alpha_j^i H_i^{(I)}, \quad (2)$$

где «$\otimes$» – произведение матриц над $GF(2)$, «$\oplus$» – сумма над полем $GF(2)$, α_j^i – элементы проверочной матрицы $A_{D\times R}$

Для каждого из R избыточных пакетов вырабатывают по ключу k_g ($g = 1..R$), имитовставку $I_{W_j}^{(k_g)}$, имитовставка добавляется к пакету:

$$W_j^{(I)} = W_j \| I_{W_j}^{(k_g)}.$$

Далее, информационные и избыточные пакеты по *многомерному* маршруту передают на приёмную сторону, на которой в каждом пакете проверяют имитовставку. Пакеты, не прошедшие проверку, удаляют. Из пакетов, прошедших проверку, формируют линейный разделимый избыточный код, который затем декодируют с исправлением стираний. Восстановление стёртых пакетов сводится к решению уравнения (1) или системы уравнений (2) над $GF(2)$. В случае, если количество стёртых пакетов превышает корректирующую способность построенного кода, но не превышает количество избыточных пакетов, предварительно выполняется проверка совместности системы уравнений над $GF(2)$. Для этого система уравнений представляется в виде матрицы коэффициентов при переменных, далее находится её детерминант:

$$\Delta = \bigoplus_{\alpha_1,\alpha_2,\ldots,\alpha_n} b_1^{\alpha_1} \cdot b_2^{\alpha_2} \cdot \ldots \cdot b_n^{\alpha_n},$$

где b^i_j – элементы матрицы коэффициентов при переменных системы уравнений над $GF(2)$, $\alpha_1, \alpha_2, \ldots \alpha_n$ – все возможные перестановки верхних индексов соответственно [14].

Если в системе отсутствуют линейно зависимые уравнения, то детерминант матрицы коэффициентов при переменных системы уравнений равен единице. В восстановленных в результате декодирования пакетах проверяют имитовставку. При успешном восстановлении получатель отправляет передающей стороне сообщение об успешной доставке последовательности пакетов.

Используем допущение о том, что алгоритмы контроля целостности пакетов идеальны и имитовставка с вероятностью равной единице обнаруживает нарушение целостности пакета. Тогда предлагаемый способ позволяет гарантированно восстанавливать до $d_{\text{мин}}-1$ стёртых пакетов и с вероятностью до 80% $d_{\text{мин}}$ стёртых пакетов, где $d_{\text{мин}}$ – минимальное кодовое расстояние.

4 Исследование модели в условиях применения предлагаемого способа

Обратной стороной применения помехоустойчивого кодирования является внесение избыточности и, как следствие, уменьшение скорости передачи полезной информации. Следовательно, целесообразно применять адаптивное помехоустойчивое кодирование, осуществлять выбор параметров соразмерно деструктивному воздействию злоумышленником на процесс информационного обмена в системе. Имитационное моделирование в среде динамического модельно-ориентированного проектирования Simulink предлагаемого способа позволяет точнее определить границы применения предложенного способа с конкретными параметрами.

Результаты моделирования способа устойчивой к деструктивным воздействиям передачи информации по каналам связи виртуальных частных сетей с различными значениями параметров D, R и N представлены на рис. 2.

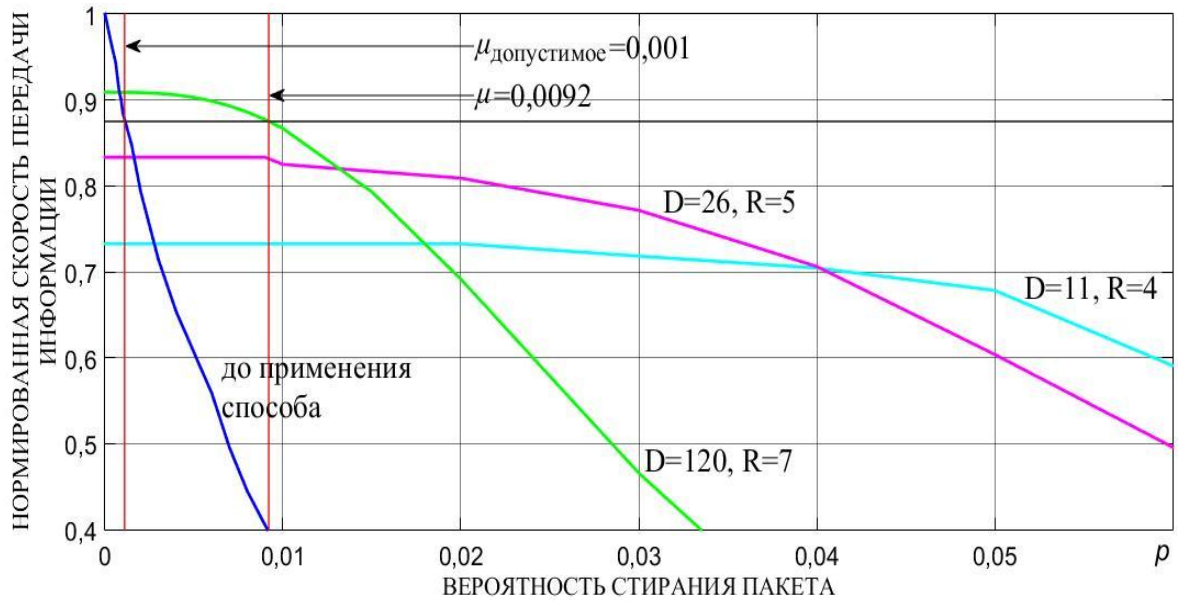

Рис. 2. Зависимость нормированной скорости передачи информации от вероятности стирания пакета до и после применения предлагаемого способа с различными параметрами D и R при N=100, $\mu_{допустимое}$=0,001

Для оценки эффективности применения предлагаемого способа с конкретными параметрами применим ранее описанную математическую модель в виде марковского процесса смены состояний (рис. 1) с учётом корректирующей способности применяемого кодирования и используемой имитовставки. Вероятность безошибочного приёма последовательности из N пакетов с учётом корректирующей способности кода, используемого в предлагаемом способе:

$$p'_{\text{отс.стираний}} = \left(\sum_{i=0}^{d_{\min}-1} C_{D+R}^{i} \mu^{i} \left(1-\mu\right)^{D+R-i} + 0{,}8 \cdot C_{D+R}^{d_{\min}} \cdot \mu^{d_{\min}} \cdot \left(1-\mu\right)^{D+R-d_{\min}} \right)^{\left\lceil \frac{N}{D+R} \right\rceil}.$$

Вероятность того, что в системе не произошло ни одной успешной имитации пакета при передаче информационного сообщения с учётом применения имитовставки:

$$p'_{\text{отс.усп.имит.}} = e^{-\lambda\lambda'\gamma M},$$

где λ' – вероятность подбора злоумышленником имитовставки, применяемой для контроля целостности полученных и восстановленных пакетов.

Вероятность того, что в системе количество потерянных пакетов не превышает допустимого уровня с учётом корректирующей способности кода, используемого в предлагаемом способе:

$$p'_{\text{доп.ур.пот.}} = \left(\sum_{i=0}^{d_{\min}-1} C_{D+R}^{i} \mu^{i} \left(1-\mu\right)^{D+R-i} + 0{,}8 \cdot C_{D+R}^{d_{\min}} \cdot \mu^{d_{\min}} \cdot \left(1-\mu\right)^{D+R-d_{\min}} \right)^{\left\lceil \frac{\mu_{\text{допустимое}}^{-1}}{D+R} \right\rceil}.$$

Результаты исследования системы в условиях применения предлагаемого способа при ИТВ злоумышленником и приближении значения коэффициента потери пакетов к допустимому значению представлены на рис. 3. Для решения уравнений численным методом использовался метод Рунге-Куты [15] с фиксированным шагом интегрирования.

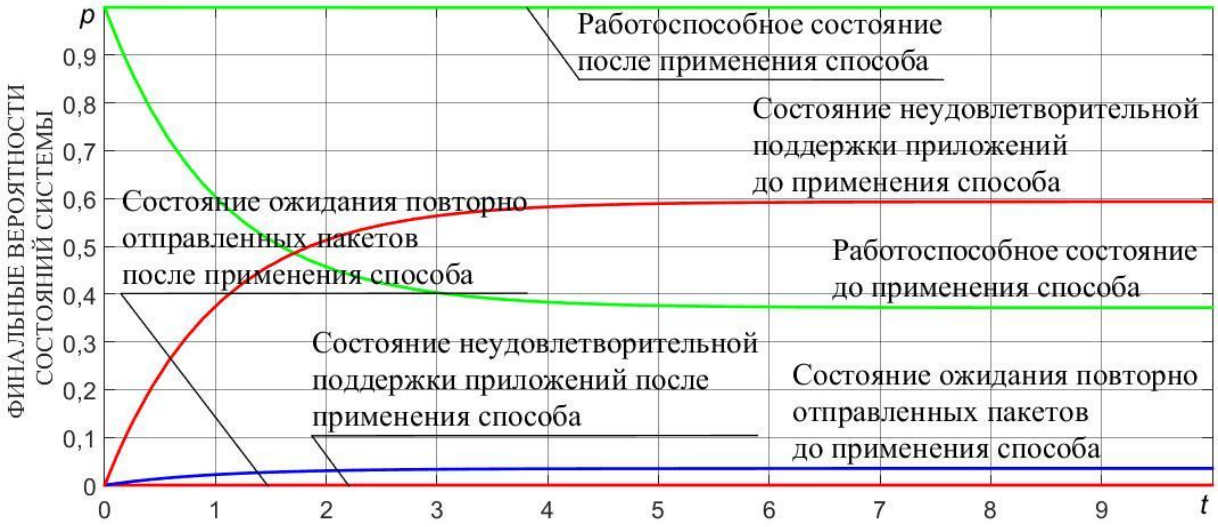

Рис. 3. Динамика значений вероятности нахождения системы в различных состояниях при μ=0,0009, $\mu_{допустимое}$=0,001, N=100, D=120, R=7 до и после применения предлагаемого способа в условиях ИТВ злоумышленником

Заключение

Применение предлагаемого способа позволяет повысить устойчивость передачи, а также скорость передачи информации по каналам связи VPN в условиях деструктивных воздействий злоумышленником.

Литература

1. *Шваб К.* Четвертая промышленная революция. – М: Эксмо, 2021. – 208 с.
2. *Иванов В.Г.* Модель технической основы системы управления специального назначения в едином информационном пространстве на основе конвергентной инфраструктуры системы связи : монография. – СПб.: Политех-пресс, 2018. – 214 с.
3. *Воробьев С.П., Давыдов А.Е., Ефимов В.В., Курносов В.И.* Инфокоммуникационные сети. Том 1: Инфокоммуникационные сети: классификация, структура, архитектура, жизненный цикл, технологии : энциклопедия. – СПб.: Наукоемкие технологии, 2019. – 739 с.
4. *Макаренко С.И.* Экспериментальное исследование реакции сети связи и эффектов перемаршрутизации информационных потоков в условиях динамического изменения сигнально-помеховой обстановки // Журнал радиоэлектроники. – 2016. – № 4. – URL: http://jre.cplire.ru/jre/apr16/4/text.html (дата обращения: 01.03.2021).
5. *Макаренко С.И.* Время сходимости протоколов маршрутизации при отказах в сети // Системы управления, связи и безопасности. – 2015. – № 2. – С. 45-98.
6. *Олифер В., Олифер Н.* Компьютерные сети. Принципы, технологии, протоколы : учебник для ВУЗов. – М.: Питер, 2016. – 992 с.
7. *Вентцель Е.С.* Теория вероятностей. – М.: Наука, 1969. – 576 с.
8. *Дынкин Е.Б.* Марковские процессы. – М.: Гос. изд-во физико-математической литературы, 1963. – 861 с.
9. *Кубицкий В.И.* Восстановление стёртых пакетов в компьютерных сетях // Научный вестник МГТУ ГА. – 2011. – № 169. – С. 65-72.
10. *Samoylenko D.V., Eremeev M.A., Finko O.A.* A method of providing the integrity of information in the group of robotic engineering complexes based on crypt-code constructions // Automatic control and computer sciences. 2017. vol. 51. № 8. pp. 965-971. doi: 10.3103/S0146411617080181.
11. *Самойленко Д.В., Финько О.А., Еремеев М.А.* Распределённая обработка и защита информации в группировке комплексов с беспилотными летательными аппаратами // Теория и техника радиосвязи. – 2017. – № 4. – С. 93-100.
12. *Самойленко Д.В., Финько О.А.* Помехоустойчивая передача данных в радиоканалах робототехнических комплексов на основе полиномиальных классов вычетов // Наукоемкие технологии в космических исследованиях Земли. – 2016. – Т.8. – № 3. – С. 49-55.
13. *Березюка Н.Т.* Кодирование информации двоичные коды – Харьков: Вища школа, – 1978 – 252 с.
14. *Боревич З.И.* Определители и матрицы. – М.: Наука, 1970 – 200 с.
15. *Деккер К., Вервер Я.* Устойчивость методов Рунге-Кутты для жестких нелинейных дифференциальных уравнений. – М.: Мир, 1988. – 336 с.