ОБЕСПЕЧЕНИЕ ЦЕЛОСТНОСТИ ДАННЫХ, ПЕРЕДАВАЕМЫХ ПО КАНАЛАМ СВЯЗИ ВИРТУАЛЬНЫХ ЧАСТНЫХ СЕТЕЙ

Карпов С.С.[1], Рябинин Ю.Е.[2], Финько О.А.[3]

Аннотация

Рассматривается способ обеспечения целостности данных, передаваемых по каналам связи виртуальных частных сетей (virtual private network – VPN) крупномасштабных информационных систем, функционирующих в условиях деструктивного воздействия злоумышленника. Предлагаемый способ позволяет восстанавливать пакеты данных, подвергнутые стираниям и имитации.

***Целью исследования** является повышение устойчивости передачи данных по каналам связи VPN путём реализации процедуры восстановления стёртых пакетов и повышения уровня имитозащищённости передаваемых данных.*

***Методы исследования:** агрегирование методов криптографического контроля целостности данных и методов избыточного кодирования данных, применение методов теории марковских случайных процессов для определения вероятности обеспечения удовлетворительной поддержки приложений в условиях деструктивного воздействия злоумышленника с различными параметрами.*

***Результаты исследования:** выполнен анализ объекта исследования – VPN крупномасштабных информационных систем, позволивший сделать вывод о необходимости обеспечения защиты данных, передаваемых по каналам связи таких систем, для реализации существующих национальных и региональных стратегий экономического развития. Представлена математическая модель функционирования системы передачи данных по каналам связи VPN в условиях деструктивного воздействия злоумышленника. Предложен способ обеспечения целостности передаваемых данных на основе оригинальной схемы совместного использования известных решений, порождая синергетический эффект. Способ позволяет восстанавливать $d_{\text{мин}} - 1$ стертых пакетов данных.*

Предлагаемое решение позволяет повысить устойчивость и скорость передачи данных по каналам связи сети в условиях деструктивного воздействия злоумышленника и имитации данных.

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

DOI:10.21681/2311-3456-2021-4-81-97

Введение

Системное развитие и внедрение цифровых технологий во все сферы жизнедеятельности человека, поступательное распространение технологий интернета вещей и облачных вычислений, их интеграция в киберфизические системы и объединение таких систем в единую глобальную сеть изменяет сложившиеся экономические парадигмы и выступает одним из основных факторов конкурентноспособности как отдельных предприятий, так и целых конгломератов [1–3].

За последние несколько лет запущен ряд национальных и региональных инициатив по формированию распределённых интеллектуальных систем: «Стратегия развития информационного общества в Российской Федерации на 2017 – 2030 годы»[4], «Новая промышленная стратегия для Европы до 2030 г.»[5], «Стратегия высоких

1 Карпов Сергей Сергеевич, адъюнкт 22 кафедры (техники специальной связи) Краснодарского высшего военного орденов Жукова и Октябрьской Революции Краснознаменного училища имени генерала армии С.М. Штеменко, г. Краснодар, Россия. E-mail: karpov.sergey.sergeevich@yandex.ru

2 Рябинин Юрий Евгеньевич, кандидат технических наук, докторант 22 кафедры (техники специальной связи) Краснодарского высшего военного орденов Жукова и Октябрьской Революции Краснознаменного училища имени генерала армии С.М. Штеменко, г. Краснодар, Россия. E-mail: jurandvau@inbox.ru.

3 Финько Олег Анатольевич, доктор технических наук, профессор, профессор 22 кафедры (техники специальной связи) Краснодарского высшего военного орденов Жукова и Октябрьской Революции Краснознаменного училища имени генерала армии С.М. Штеменко, г. Краснодар; профессор кафедры информационной безопасности автоматизированных систем Северо-Кавказского федерального университета, г. Ставрополь; академический советник Российской академии ракетных и артиллерийских наук (РАРАН) г. Москва, Россия.

E-mail: ofinko@yandex.ru.

4 О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы: Указ Президента Российской Федерации от 09.05.2017 № 203. URL: http://publication.pravo.gov.ru/Document/View/0001201705100002 (дата обращения: 20.02.2021).

5 A New Industrial Strategy for Europe / Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions / European Commission – Brussels, 10.3.2020 COM(2020) 102 final. – URL: https://ec.europa.eu/info/sites/default/files/communication-eu-industrial-strategy-march-2020_en.pdf (дата обращения: 20.02.2021)

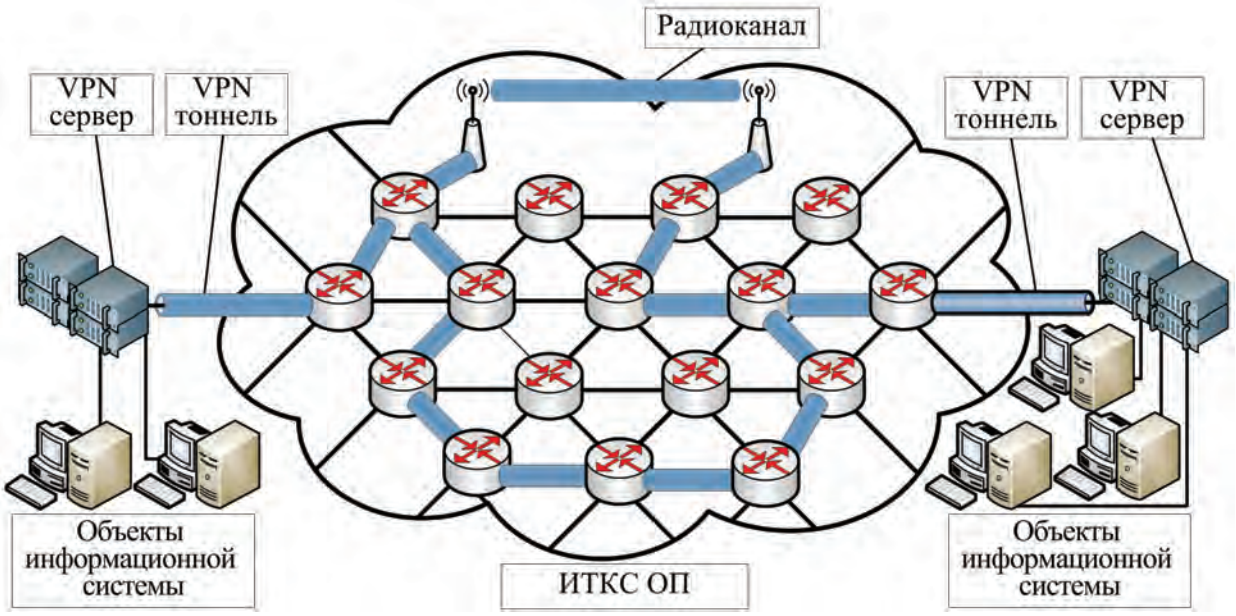


Рис. 1. Пояснение процесса передачи данных с использованием инфраструктуры ИТКС ОП

технологий 2025»[6] в Германии, «Industrie du Futer»[7] во Франции. Реализация подобных инициатив предусматривает формирование и внедрение крупномасштабных систем (в том числе и ведомственных), объединенных единой сетью связи. При этом одним из основных факторов успешной реализации существующих стратегий развития является обеспечение защиты данных, обрабатываемых интеллектуальными системами, от киберугроз.

Децентрализация систем аналитики и управленческих решений, распределенная обработка данных средствами облачных сервисов предполагает использование информационно-телекоммуникационной сети общего пользования (далее – ИТКС ОП). При этом наличие злонамеренного нарушителя предполагает организацию защищённых каналов связи в ИТКС ОП, что в настоящее время осуществляется главным образом с помощью технологий виртуальных частных сетей (virtual private network – VPN) [4, 5].

Модель злоумышленника для VPN предусматривает ряд угроз безопасности информации[8], реализуемых, в том числе, в результате воздействий на используемую для организации виртуальных каналов инфраструктуру ИТКС ОП, в частности – уязвимостей протоколов сетевого взаимодействия [6, 7]. Потери, превышение времени $t_{треб}$ доставки пакетов данных сетевого уровня модели OSI (далее – пакеты), а также блокирование элементов инфраструктуры ИТКС ОП приводят к стиранию пакетов на стороне получателя. Существующий механизм обратной связи даёт положительный результат, если стирания пакетов носят случайный характер [8]. Однако, при превышении допустимого уровня количества стёртых пакетов в VPN, удовлетворительная поддержка различных приложений становится невозможной[9].

Таким образом, повышение уровня защищённости данных, передаваемых в VPN, является актуальной задачей в рамках реализации стратегий развития информационного общества.

Анализ объекта исследования

Каналы связи VPN прокладываются в сети заблаговременно и независимо от того, существует ли поток пакетов в сети в данное время или только является топологически возможным. Для каждой конкретной VPN создается отдельный класс эквивалентности продвижения (forwarding equivalence class – FEC). Все пакеты, принадлежащие к данному классу, продвигаются через MPLS-сеть (multiprotocol label switching – многопротокольная коммутация по меткам) по одному виртуальному пути. Таким образом, передача данных в VPN преимущественно реализуется средствами технологий многопутевой маршрутизации [8].

Формирование таблиц продвижения выполняется заранее (до появления потока данных), как правило, автоматически в соответствии с топологией сети. У администратора сети (провайдера) имеется возможность корректировать таблицы FEC [8]. Согласно аналитическим исследованиям международной исследовательской и консалтинговой компании International Data Corporation

6 Die Bundesregierung / Forschung und Innovation f r die Menschen. URL: https://www.bmbf.de/upload_filestore/pub/Forschung_und_Innovation_fuer_die_Menschen.pdf (дата обращения: 20.02.2021)

7 Le Guide des technologies de l'Industrie du Futur / Enjeux et panorama des solutions. URL: http://www.industrie-dufutur.org/content/uploads/2018/03/Guide-des-Technologies_2018_V3.pdf (дата обращения: 20.02.2021)

8 Банк данных угроз безопасности информации ФСТЭК России. (дата обращения 27.11.2018) URL: https://bdu.fstec.ru/threat (дата обращения: 01.02.2021)

9 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.

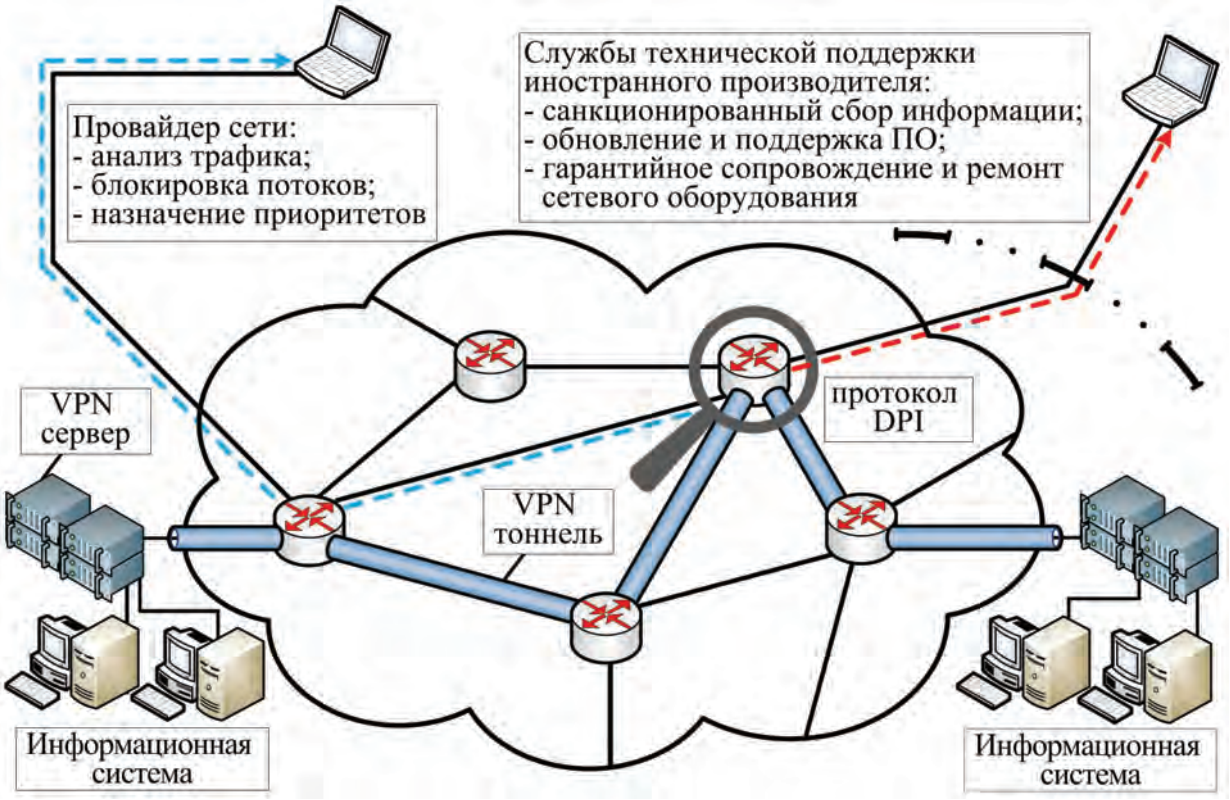


Рис. 2. Принцип использования протоколов DPI

(IDC) на протяжении последних лет абсолютными лидерами по производству сетевого оборудования и программного обеспечения для систем связи остаются компании: Cisco, Huawei, Hewlett Packard Enterprise, Arista Networks, Juniper Networks и другие[10]. Следовательно, построение таблицы коммутации каналов VPN и передача пакетов данных в канале осуществляются программными и аппаратными средствами иностранных компаний, расположенными в ИТКС ОП. Это обуславливает наличие дополнительных уязвимостей ввиду вероятного присутствия не декларируемых возможностей данного оборудования и программного обеспечения [9]. Процесс обмена данными по многомерному маршруту между объектами крупномасштабной информационной системы поясняется на рисунке 1.

Согласно результатам анализа, проведенного в работе [10] большинство узлов связи и объектов критической информационной инфраструктуры вскрываются специальными службами иностранных государств и организованными группами киберпреступников. Трафик VPN может быть идентифицирован среди множества передаваемых пакетов в сети провайдера (поставщика услуги интернет). Помимо полей адресации в заголовке IP пакета, содержащих внешние адреса объектов информационных систем, такой трафик имеет ряд отличительных признаков, благодаря которым может быть выделен методом статистического анализа. На сетевом оборудовании ИТКС ОП реализованы протоколы учёта сведений о потоках IP пакетов, обработанных на этом оборудовании. Поток определяется как однонаправленная последовательность пакетов, у которых совпадают IP адреса и номера портов источника и получателя и тип протокола. Записи протоколов учёта NetFlow (Cisco), NetStream (Huawei Technologies), JFlow (Juniper Networks) сохраняют большое количество информации о пакетах, в том числе значение поля ToS (Type of Service – тип обслуживания), информацию специфичную для транспортных протоколов, номер автономной системы и многое другое[11]. Последние версии протоколов учёта сведений о потоках IP пакетов определяют также потоки по MPLS меткам и таблицам FEC (MPLS-aware netflow). Конвенция Совета Европы[12] декларирует принцип трансграничного доступа к хранящимся компьютерным данным, а именно, право без согласия другой стороны получать доступ к общедоступным компьютерным данным независимо от их географического местоположения; получать через компьютерную систему на своей территории доступ к хранящимся на территории другой стороны компьютерным данным или получать их, если имеется законное и

10 IDC's Worldwide Quarterly Ethernet Switch and Router Trackers Show Mixed Results in Fourth Quarter of 2020. – URL: https://www.idc.com/getdoc.jsp?containerId=prUS47525621 (дата обращения: 20.02.2021)

11 Рекомендация МСЭ-Т Y.2770. Требования к углубленной проверке пакетов в сетях последующих поколений: утверждена 13-й Исследовательской комиссией в соответствии с процедурой, изложенной в Рекомендации МСЭ-Т A.8 20 ноября 2012 г. Швейцария Женева, 2014. – Текст: непосредственный.

12 Конвенция Совета Европы о преступности в сфере компьютерной информации (ETS N 185): 23 ноября 2001 г. Венгрия Будапешт, 2001. – Текст: электронный. // Гарант: справочно-правовая система. – URL: http://base.garant.ru/4089723 (дата обращения: 01.03.2021).

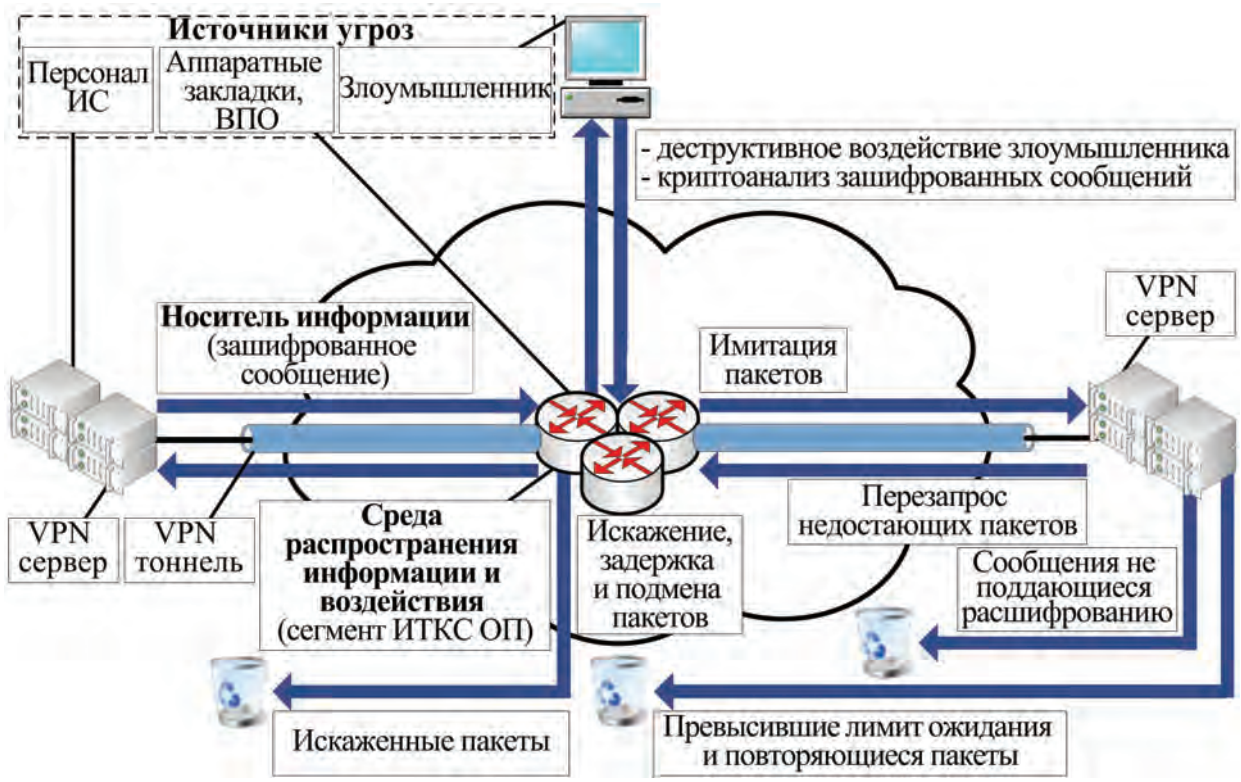


Рис. 3. Основные элементы каналов реализации угроз безопасности информации VPN

добровольное согласие лица, которое имеет законные полномочия раскрывать эти данные через такую компьютерную систему. Следовательно, данные об информационном обмене VPN, собираемые в узлах ИТКС ОП, могут передаваться для дальнейшего статистического и интеллектуального анализа третьей стороне (рис. 2). Полученные в ходе анализа временные интервалы и интенсивность использования интернет сервисов VPN, типы используемых протоколов и другие характеристики трафика могут быть использованы для реализации угроз безопасности информации.

Согласно данным, аккумулируемым и публикуемым ФСТЭК[13], злоумышленником могут быть реализованы угрозы безопасности информации в отношении элементов ИТКС ОП, являющейся базовой сетью для VPN:

- угроза физического выведения из строя средств хранения, обработки и (или) передачи информации;
- угроза вскрытия топологии вычислительной сети;
- угроза несанкционированного доступа к виртуальным каналам передачи;
- угроза использования слабостей протоколов сетевого и локального обмена данными;
- угроза несанкционированного доступа к виртуальному и физическому сетевому оборудованию из физической и виртуальной сети;
- угроза приведения системы в состояние «отказ в обслуживании» и другие.

Основные элементы каналов реализации угроз безопасности информации VPN поясняются на рисунке 3.

Деструктивное воздействие на элементы ИТКС ОП может быть эффективным для информационного обмена абонентов VPN и практически незаметным для остальных пользователей ИТКС ОП. Например, согласно данным, опубликованным на официальном сайте технической поддержки CISCO, изменение параметра MTU (maximum transmission unit – максимальная единица передачи) в одном и более элементов базовой сети VPN хотя бы на один пункт менее MTU, установленного в маршрутизаторе, использующем стек протоколов IPSec совместно с блоком аппаратного шифрования, приводит к уменьшению скорости шифрованного соединения на 50-90%. В данном случае потеря скорости такого соединения связана с процессорной коммутацией фрагментированных пакетов IPSec и их дефрагментацией перед передачей криптографическим аппаратным средствам. Таким образом, пропускная способность VPN канала уменьшается до уровня производительности, который обеспечивается шифрованием с помощью программных средств. При этом такое уменьшение MTU и последующая фрагментация пакетов не оказывает существенного влияния на скорость передачи данных абонентов сети ИТКС ОП, чей трафик не защищён криптографическим шифрованием[14]. Сце-

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

14 Устранение фрагментации IPv4, проблем с MTU, MSS и PMTUD в работе GRE и IPsec. – Текст: электронный // Официальный сайт телекоммуникационной компании CISCO. – URL: https://www.cisco.com/c/ru_ru/support/docs/ip/generic-routing-encapsulation-gre/25885-pmtud-ipfrag.html (дата обращения: 01.03.2021)

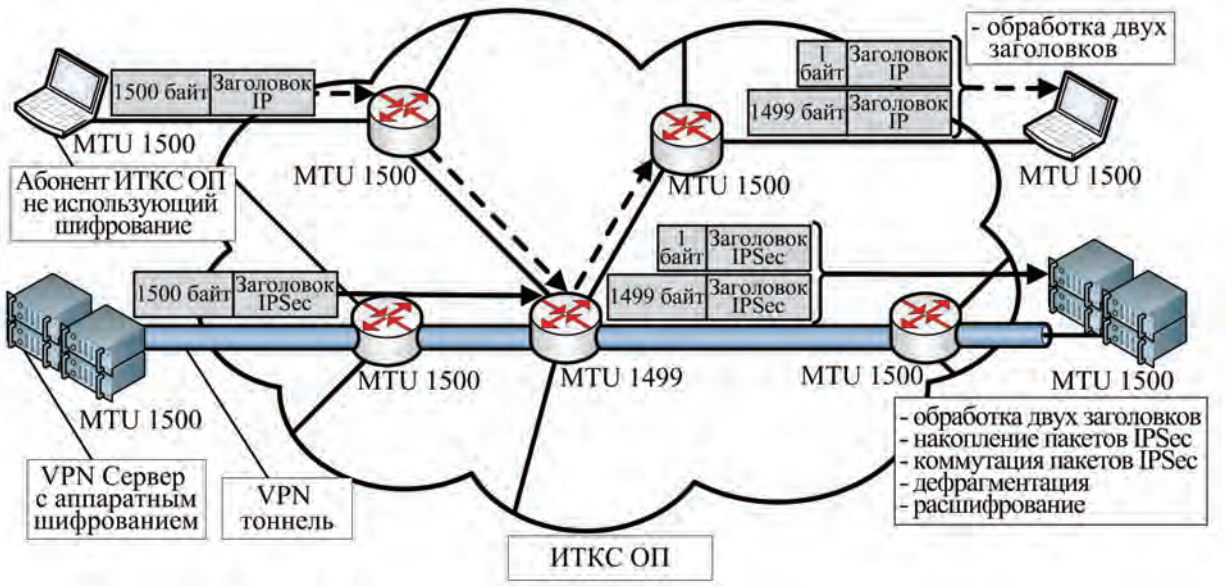


Рис. 4. Сценарий фрагментации пакетов IPSec и IP

нарий фрагментации пакетов IPSec и IP поясняется на рисунке 4.

Также снижение скорости передачи данных по каналам VPN может быть вызвано потерями или задержкой части пакетов, если число таких пакетов или величина задержки выше допустимого уровня, определённого для класса обслуживания данной сети[15]. Проблема потерь и задержек пакетов VPN может быть вызвана перегрузками в узлах (коммутаторов, маршрутизаторов и т.п.), коллизиями (наложением пакетов от разных абонентов), уменьшением пропускной способности каналов передачи данных вследствие слишком большого количества одновременно подключённых пользователей, искажений в пакете, переполнения входных буферов сетевых устройств и другими сбоями в ИТКС ОП. В системах передачи данных и сетевых приложениях, работающих в режиме реального времени, задержки пакетов равнозначны потерям, поскольку нет возможности приостанавливать процесс обработки, передачи и отображения данных в ожидании пакета или его повторной передачи. Потерянные пакеты и пакеты с ошибками в теории помехоустойчивого кодирования считаются стёртыми. При систематических ошибках и потерях пакетов их восстановление в отведённое время с использованием обратной связи затруднительно [8]. Стирание пакетов приводит к перезапуску серии IP пакетов от источника к получателю, а в случае успешной имитации пакетов VPN возможна ситуация отправки квитанции об успешном получении серии пакетов и последующей ошибки при обработке полученных данных.

Таким образом, при применении технологии VPN в интересах функционирования крупномасштабных систем и принятия управленческих решений в условиях деструктивного воздействия злоумышленника становится критически важно обеспечить устойчивость передачи данных.

Описание математической модели

Рассмотрим систему передачи данных 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 деструктивное воздействие злоумышленником на базовую сеть VPN, которой является ИТКС ОП; часть пакетов стирается, получатель ожидает повторной отправки серии пакетов от источника; число стёртых пакетов не превышает допустимый коэффициент потери пакетов[16] (вероятность потери пакета[17]);

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

15 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.

16 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).

17 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.

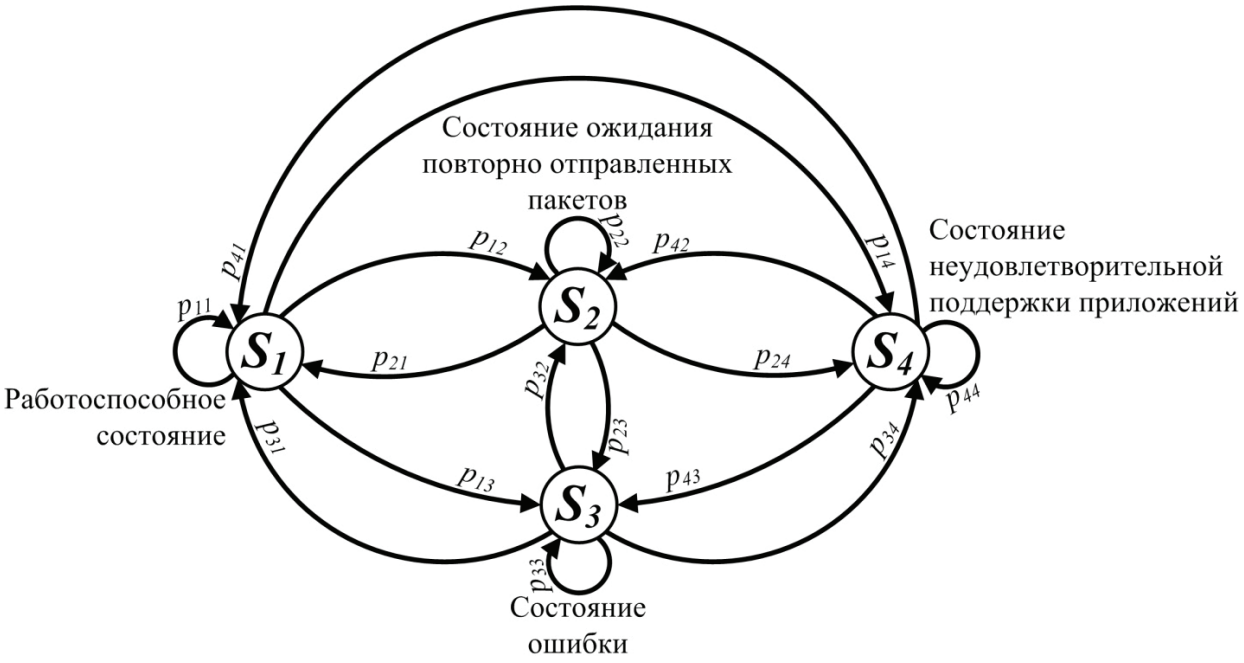


Рис. 5. Граф состояний процесса функционирования системы передачи данных по каналам связи VPN

S_4 – «состояние неудовлетворительной поддержки приложений» – в результате деструктивного воздействия злоумышленника количество потерянных пакетов превышает допустимый коэффициент потери пакетов, запускается процесс изменения параметров передачи данных по каналам связи VPN или повторный запуск процесса передачи данных.

Граф состояний процесса функционирования системы представлен на рисунке 5.

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

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

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

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

Параметры переходов $S_i \to S_j$ характеризуются вероятностями p_{ij}, зависящими от вероятности успешной доставки пакетов в условиях деструктивного воздействия злоумышленника, интенсивности имитации пакетов данных, вероятности успешной имитации данных злоумышленником, допустимого коэффициента потери пакетов для обеспечения удовлетворительной поддержки различных приложений, параметров системы передачи данных по каналам связи VPN.

При допущениях: о многопутевой независимой передаче пакетов в сети ИТКС ОП [11, 12] и, следовательно, пуассоновском характере процесса стираний пакетов в сети в результате деструктивного воздействия злоумышленника вероятность $p_{\text{отс. стираний}}$ того, что в системе при передаче последовательности пакетов отсутствуют стёртые пакеты можно определить как:

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

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

Вероятность $p_{\text{доп. ур. пот.}}$ того, что в системе количество потерянных пакетов не превышает допустимого значения, т.е. количество пакетов принятых без стираний обратно пропорционально допустимому коэффициенту потери пакетов:

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

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

Вероятность $p_{\text{отс. усп. имит.}}$ 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 – интенсивность имитационного воздействия злоумышленника (отношение числа полученных сымитированных злоумышленником пакетов к числу пакетов информационного сообщения), M – длина информационного сообщения (количество сетевых пакетов).

Вероятности p_{11}, p_{21}, p_{31} и p_{41} того, что в системе в процессе передачи данных 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 процессе передачи данных по каналам связи VPN число потерянных пакетов не превышает порог, соответствующий уровню удовлетворительной поддержки различных приложений, и, при этом, успешная имитация пакетов отсутствует:

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

Вероятности p_{13}, p_{23}, p_{33} и p_{43} успешной имитации пакетов в каналах связи VPN:

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

Вероятности p_{14}, p_{24}, p_{34} и p_{44} того, что в каналах связи VPN успешная имитация пакетов отсутствует и, при этом, поддержка различных приложений не осуществляется на удовлетворительном уровне:

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

В целях исследования системы передачи данных по каналам связи VPN по построенному графу состояний (рис. 5) составим систему уравнений:

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

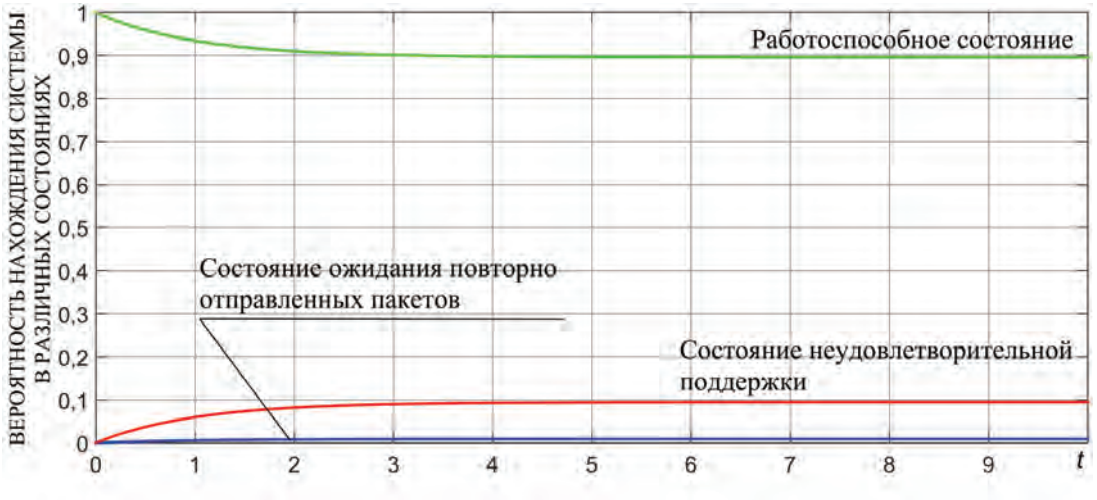
Изменяя параметры системы в пределах устойчивости уравнений в соответствии с условиями функционирования, получим динамику значений вероятности нахождения системы в различных состояниях. Результаты исследования системы в условиях деструктивного воздействия злоумышленника, при которых коэффициент потери пакетов значительно ниже допустимого, представлен на рисунке 6а. При этом вероятность нахождения системы в состоянии неудовлетворительной поддержки различных приложений не превышает 10%.

Результаты исследования системы в условиях имитационного воздействия злоумышленника с интенсивностью γ равной информационному обмену (при допущении вероятности успешной имитации, определяемой методом полного перебора значения поля аутентификации заголовка пакета IPSec) представлены на рисунке 6б. Злоумышленником могут быть использованы более совершенные алгоритмы, отличные от метода полного перебора, а также уязвимости протокола IPSec для успешной имитации пакетов. Таким образом, в результате имитации данных злоумышленником вероятность нахождения системы в работоспособном состоянии может быть значительно снижена.

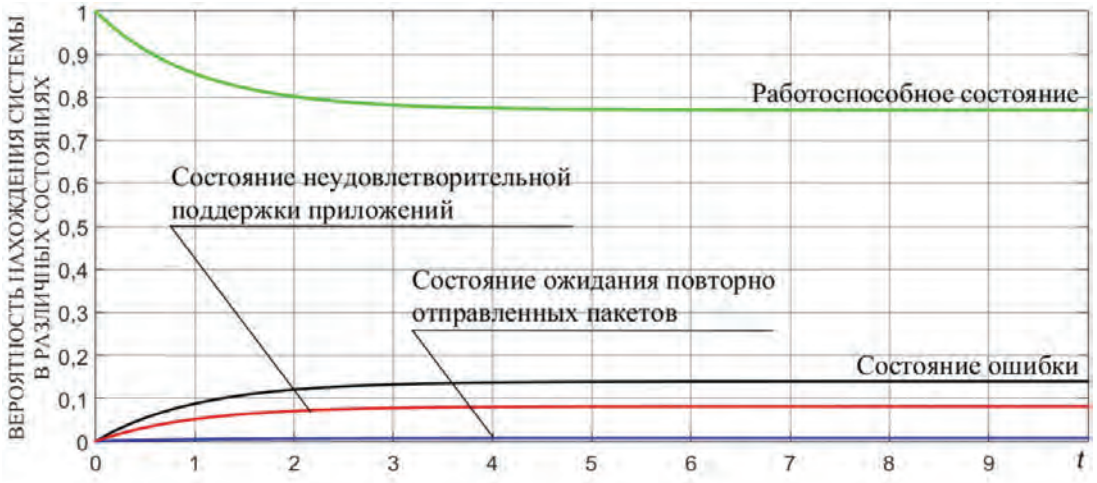
Результаты исследования системы в условиях деструктивного воздействия злоумышленника при приближении значения коэффициента потери пакетов μ к допустимому значению (на интервале времени от 0 до t) представлены на рисунке 6в. Для решения системы уравнений (1) численным методом использовался метод Рунге-Куты с фиксированным шагом интегрирования. Одними из действенных методов обеспечения целостности передаваемых данных являются методы помехоустойчивого кодирования[18] и криптографические методы, реализующие вычисление имитовставки. Предлагаемое далее решение является развитием более ранних решений авторов [13–15].

Передающая сторона выполняет мониторинг канала связи виртуальной частной сети на предмет деструктивного воздействия злоумышленника посредством обратной связи или с помощью развёрнутых сенсоров в сети. В случае обнаружения таких воздействий на передающей стороне оценивают коэффициент потери пакетов и принимают решение о целесообразности применения предлагаемого способа.

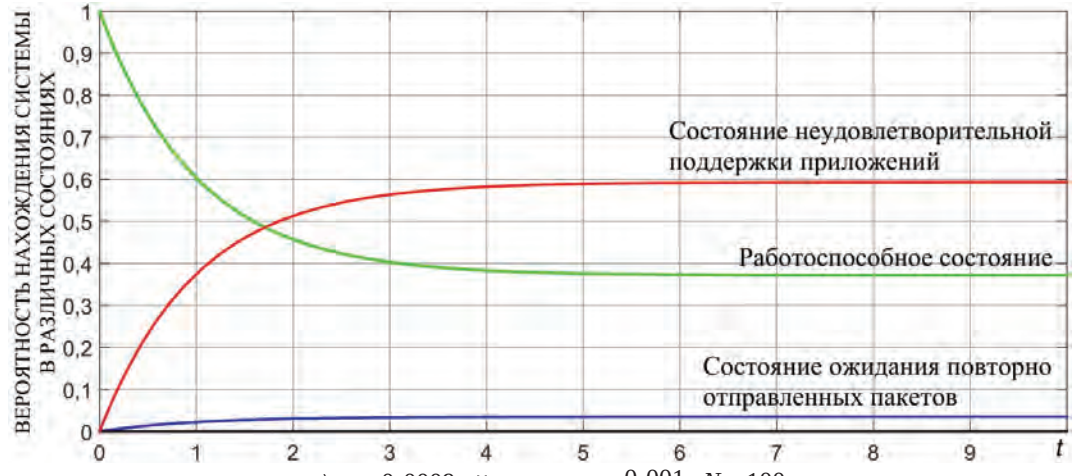
18 Кубицкий В.И. Восстановление стертых пакетов в компьютерных сетях // Научный вестник МГТУ ГА. – 2011. – №169. – С. 65-72.



а) $\mu = 0,0001$, $\mu_{\text{допустимое}} = 0,001$, $N = 100$



б) $\mu = 0,0001$, $\mu_{\text{допустимое}} = 0,001$, $N = 100$, $\lambda = 0,000016$, $\gamma = 1$, $M = 10000$



в) $\mu = 0,0009$, $\mu_{\text{допустимое}} = 0,001$, $N = 100$

Рис. 6. Динамика изменения вероятности нахождения системы в различных состояниях: а) в нормальных условиях, б) при имитирующем воздействии злоумышленника, в) при деструктивном воздействии злоумышленника

В случае принятия положительного решения определяют параметры помехоустойчивого кодирования: количество информационных пакетов D, количество избыточных пакетов R, линейно зависимых от информационных, и размер скользящего окна N. Параметры определяются согласно методике, разрабатываемой с учётом требований нормативно-правовых актов по защите информации, соответствующей VPN, или на основании результатов моделирования деструктивного воздействия злоумышленника на конкретный объект информатизации.

Оценка коэффициента потери пакетов в канале связи VPN может осуществляться передающей стороной с использованием моделей рабочих характеристик протокола TCP и данных, полученных от сенсоров[19]. При отсутствии таких данных оценка качества канала может осуществляться передающей стороной путём расчёта коэффициента потери пакетов по имеющейся статистике повторно передаваемых последовательностей пакетов:

$$\mu_{\text{потери пакетов}} = \left(\frac{Q}{G+Q}\right)^{\frac{1}{N}},$$

где G – количество доставленных последовательностей пакетов, Q – количество повторно отправленных последовательностей пакетов, N – размер скользящего окна в пакетах.

Описание этапа кодирования. При поступлении на вход криптомаршрутизатора последовательности из M сетевых пакетов $\mathbf{C}_1,\ldots,\mathbf{C}_M$ внутренней сети информационной системы тело каждого информационного пакета и его заголовок с адресами внутренней сети зашифровываются. Далее полученные зашифрованные информационные пакеты $\mathbf{H}_1, \ldots, \mathbf{H}_M$ делят на группы из D информационных пакетов. Для каждого информационного пакета $\mathbf{H}_i$ вырабатывают имитовставку $\mathbf{L}_{\mathbf{H}_i}^{(k_i)}$ по ключу k_i ($i=1, 2, \ldots, D$), например, по ГОСТ Р 34.12-2015[20]. Имитовставка добавляется к информационным пакетам $\mathbf{H}_i$:

$$\mathbf{Y}_i = \mathbf{H}_i \| \mathbf{L}_{\mathbf{H}_i}^{(k_i)} = \begin{bmatrix} h_1 & h_2 & \cdots & h_n \end{bmatrix} \| \begin{bmatrix} l_1 & \cdots & l_m \end{bmatrix},$$

$$= \begin{bmatrix} y_1 & y_2 & \cdots & y_n & y_{n+1} & \cdots & y_{n+m} \end{bmatrix}$$

где «||» – символ операции конкатенации; n и m – длины (в битах) пакета и имитовставки соответственно; h, l и y – двоичные символы информационного пакета $\mathbf{H}_i$, имитовставки $\mathbf{L}_i$ и сформированного пакета $\mathbf{Y}_i$ соответственно.

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 $\mathbf{A}_{D\times R}$ отображает зависимость R избыточных пакетов от D информационных пакетов. Проверочная матрица должна соответствовать требованиям:

- количество единиц в строке матрицы $\mathbf{A}_{D\times R}$ должно быть не менее $d_{\text{мин}}-1$, где $d_{\text{мин}}$ – минимальное кодовое расстояние;
- сумма над $GF(2)$ двух любых строк не должна иметь менее $d_{\text{мин}}-2$ единиц [16].

Формирование избыточных пакетов $\mathbf{W}_j$ ($j=1, 2, \ldots, R$) осуществляется произведением над $GF(2)$ проверочной матрицы $\mathbf{A}_{D\times R}$ на вектор-строку из D информационных пакетов $\mathbf{Y}_{1\times D}$:

$$\mathbf{W}_{1\times R} = \mathbf{Y}_{1\times D} \otimes \mathbf{A}_{D\times R} =$$

$$= \begin{bmatrix} \mathbf{Y}_1 & \mathbf{Y}_2 & \cdots & \mathbf{Y}_D \end{bmatrix} \otimes \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,R} \\ a_{2,1} & a_{2,2} & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ a_{D,1} & \cdots & \cdots & a_{D,R} \end{pmatrix} =$$

$$= \begin{pmatrix} a_{1,1}\mathbf{Y}_1 \oplus a_{2,1}\mathbf{Y}_2 \oplus \cdots \oplus a_{D,1}\mathbf{Y}_D \\ a_{1,2}\mathbf{Y}_1 \oplus a_{2,2}\mathbf{Y}_2 \oplus \cdots \oplus a_{D,2}\mathbf{Y}_D \\ \cdots \\ a_{1,R}\mathbf{Y}_1 \oplus a_{2,R}\mathbf{Y}_2 \oplus \cdots \oplus a_{D,R}\mathbf{Y}_D \end{pmatrix}^{\mathrm{T}} = \quad (2)$$

$$= \begin{bmatrix} \mathbf{W}_1 & \mathbf{W}_2 & \cdots & \mathbf{W}_R \end{bmatrix}$$

или решением системы из уравнений:

$$\mathbf{W}_j = \bigoplus_{i=1}^{D} a_{i,j}\mathbf{Y}_i \quad (3)$$

где «$\otimes$» – произведение матриц над $GF(2)$, «$\oplus$» – сумма над $GF(2)$, $a_{i,j}$ – элементы проверочной матрицы $\mathbf{A}_{D\times R}$, «T» – символ операции транспонированная.

Для каждого из R избыточных пакетов вырабатывают по ключу k_j имитовставку $\mathbf{L}_{\mathbf{W}_j}^{(k_j)}$, которая добавляется к пакету:

$$\mathbf{Z}_j = \mathbf{W}_j \| \mathbf{L}_{\mathbf{W}_j}^{(k_j)}.$$

Процесс кодирования поясняется с помощью рисунка 7. Далее информационные и избыточные пакеты передают по многомерному маршруту в ИТКС ОП. Каждый информационный и избыточный пакет передают по максимально независимым друг от друга маршрутам ИТКС ОП.

На приёмной стороне выполняется проверка целостности пакетов, по результатам которой принимается решение о необходимости стирания пакета. Неприбывшие пакеты (превысившие лимит ожидания $t_{\text{треб}}$) при-

19 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.

20 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.

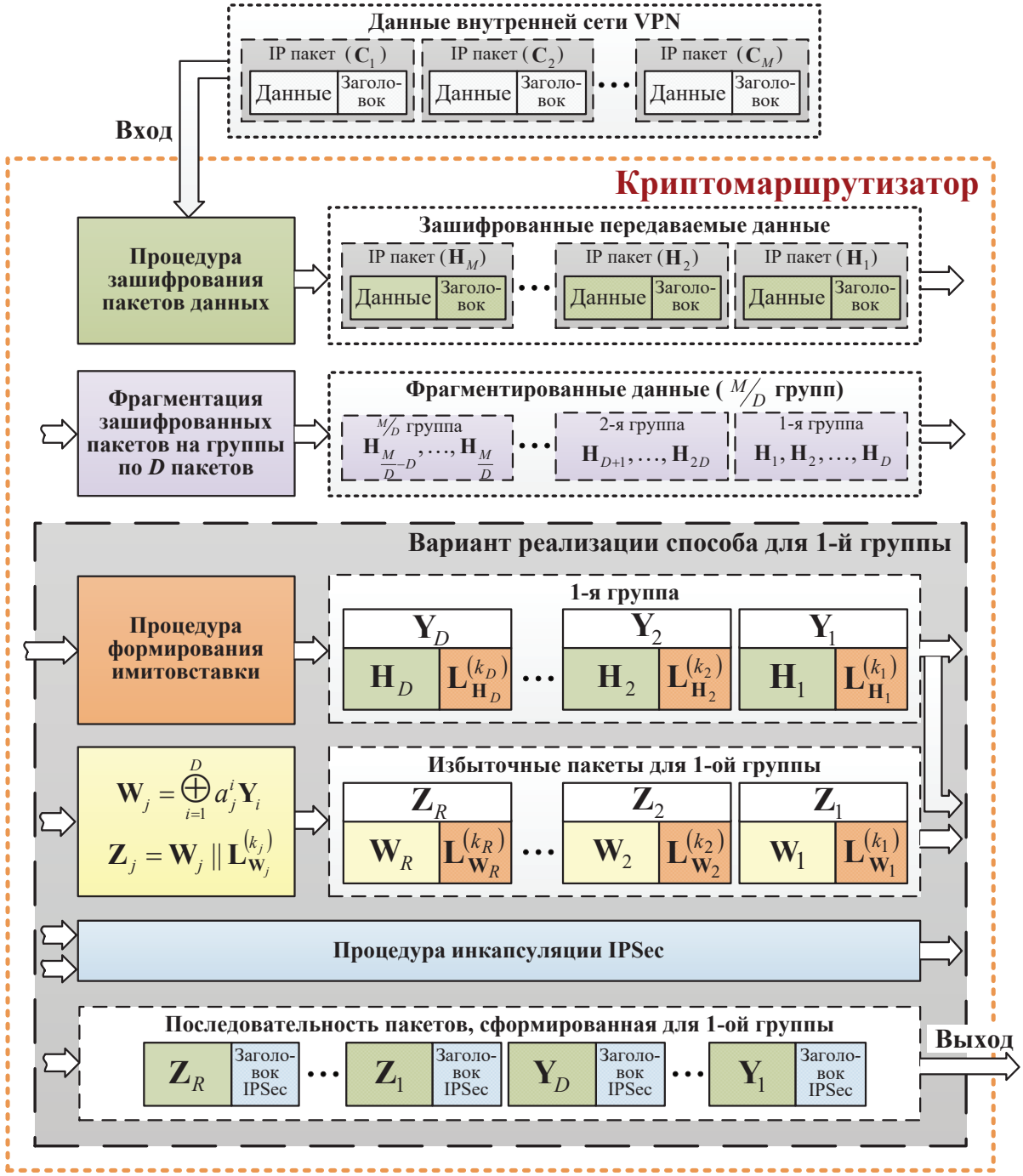


Рис. 7. Пояснение процесса кодирования данных в VPN

нимаются стёртыми. Таким образом, на принимающей стороне выполняется локализация стертых пакетов в общей последовательности из $D+R$ пакетов и определяется «обобщенный синдром стираний» (рис. 8). Из пакетов, прошедших проверку, формируют линейный разделимый избыточный код, который затем декодируют с исправлением стираний (восстановлением пакетов).

Описание этапа декодирования. Восстановление стёртых пакетов сводится к решению уравнения (2) или системы уравнений (3) над $GF(2)$. В случае, если количество стёртых пакетов превышает $d_{\text{мин}}-1$, но не превышает значение R, предварительно выполняется проверка совместности системы уравнений над $GF(2)$. Для этого система уравнений представляется в виде матрицы коэффициентов при переменных, далее находится её детерминант:

$$\Delta = \bigoplus_{\alpha_1,\alpha_2,\ldots,\alpha_n} b_{\alpha_1,1} \cdot b_{\alpha_2,2} \cdot \ldots \cdot b_{\alpha_n,n},$$

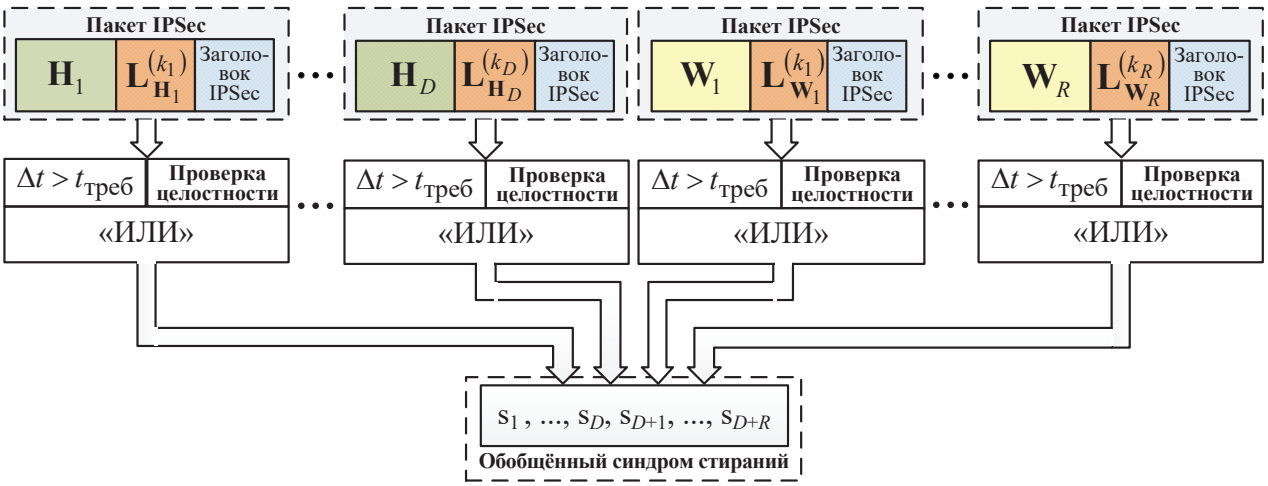


Рис. 8. Пояснение процедуры нахождения «обобщенного синдрома стираний»

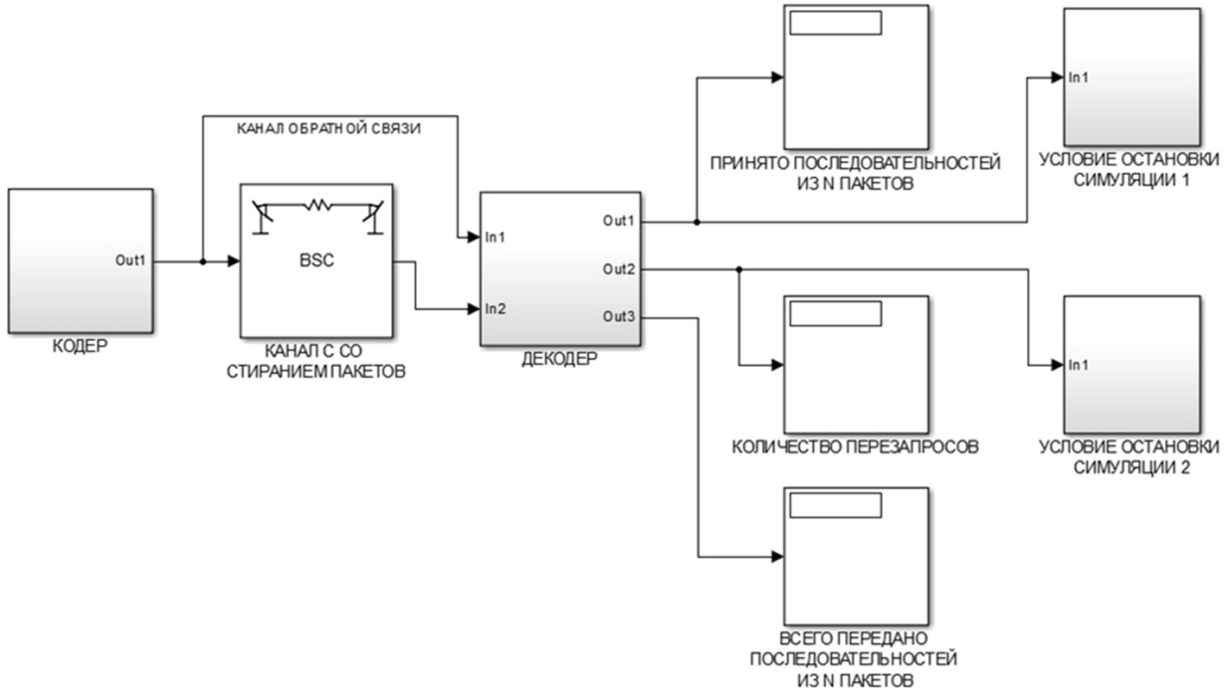


Рис. 9. Обобщённая структурная схема модели способа обеспечения целостности данных, передаваемых по каналам связи VPN, выполненная в среде Simulink

где $b_{i,j}$ – элементы матрицы коэффициентов при переменных системы уравнений над $GF(2)$, $\alpha_1, \alpha_2, \ldots, \alpha_n$ – все возможные перестановки первых индексов соответственно [18].

Если в системе отсутствуют линейно зависимые уравнения, то детерминант матрицы коэффициентов при переменных системы уравнений равен единице. Далее криптографическим методом проверяют целостность пакетов, восстановленных посредством декодирования избыточного кода. При положительном результате проверки получатель отправляет передающей стороне сообщение об успешной доставке последовательности пакетов.

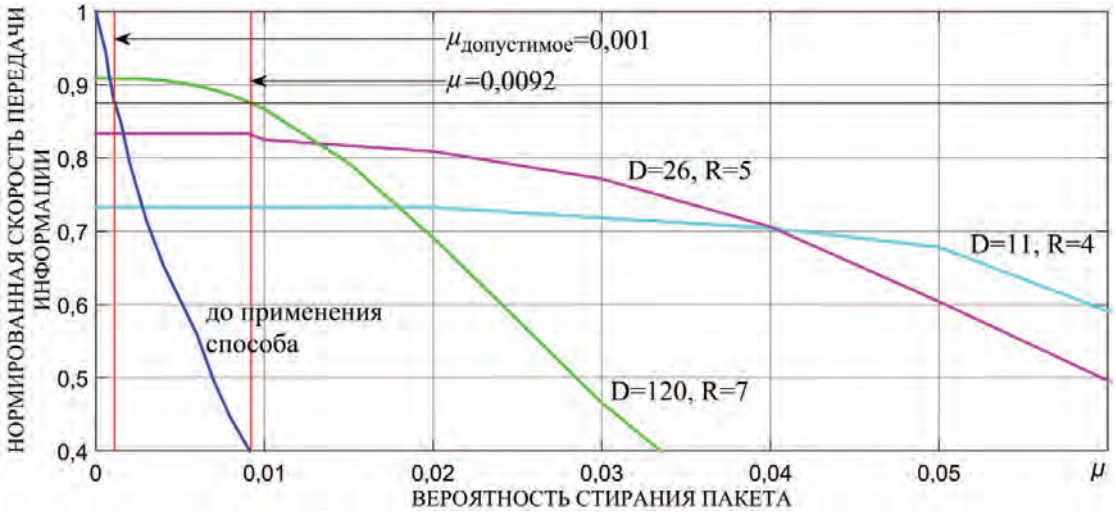
Примем допущение о том, что алгоритмы контроля целостности пакетов идеальны и имитовставка с вероятностью равной единице обнаруживает пакет с признаками нарушения целостности. Тогда использование дополнительного криптографического средства контроля позволяет локализовать позиции стираний. Это наделяет предлагаемый способ возможностью восстановления всех до $d_{\text{мин}} - 1$ и до 80% $d_{\text{мин}}$ стёртых пакетов.

Моделирование системы передачи данных по каналам связи VPN

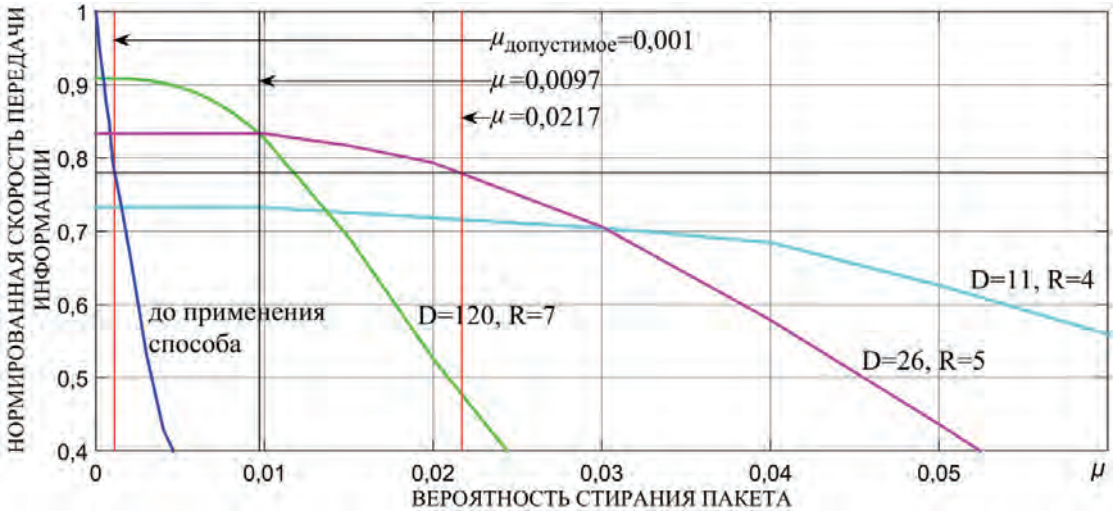
Обратной стороной применения помехоустойчивого кодирования является введение избыточности и, как следствие, уменьшение скорости передачи полезной информации в условиях отсутствия деструктивного воздействия злоумышленника. Следовательно, целесообразно использовать адаптивные методы помехоустойчивого кодирования, соответствующие уровню деструктивного воздействия злоумышленника. Имитационное моделирование предлагаемого способа в среде динамического модельно-ориентированного проектирования Simulink позволяет точнее определить его границы применения с конкретными параметрами (рис. 9).

Полученные в результате имитационного моделирования зависимости нормированной скорости передачи информации от значений вероятности стирания пакета при различных параметрах D, R и N представлены на рисунке 10.

Для оценки эффективности применения предлагаемого способа с конкретными параметрами исследуем ранее построенную математическую модель, представив ее в виде марковского процесса смены состояний (рис. 5) с учётом корректирующей способности применяемого кодирования и использования имитовставки.



а) $N = 100$



б) $N = 200$

Рис. 10. Зависимости нормированной скорости передачи информации от вероятности стирания пакета при $\mu_{\text{допустимое}} = 0,001$ *в условиях применения предлагаемого способа с различными параметрами* D *и* R*: а) при* $N = 100$*, б) при* $N = 200$

Вероятность $p'_{\text{отс. стираний}}$ безошибочного приёма последовательности из N пакетов с учётом корректирующей способности кода:

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

где «$\lceil a \rceil$» – округление a к большему целому.

Вероятность $p'_{\text{доп. ур. пот.}}$ того, что в системе количество потерянных пакетов не превышает допустимого уровня с учётом корректирующей способности кода:

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

Вероятность $p'_{\text{доп. ур. пот.}}$ отсутствия успешной имитации пакетов данных при применении имитовставки:

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

где λ' – вероятность успешного подбора коллизии злоумышленником имитовставки.

Результаты исследования системы в условиях применения предлагаемого способа при наличии имитационного воздействия с интенсивностью γ, равной информационному обмену в системе, представлены на рисунке 11а. Использование имитовставки позволяет значительно снизить вероятность нахождения системы в «состоянии ошибки» (рис. 5).

Результаты исследования системы в условиях применения предлагаемого способа при деструктивном воздействии злоумышленника и приближении значения коэффициента потери пакетов к допустимому значению представлено на рисунке 11б.

Результаты применения предлагаемого способа с параметрами $N = 200$, $D = 120$, $R = 7$ и $D = 26$, $R = 5$ при $\mu = 0{,}0097$ и $\mu_{\text{допустимое}} = 0{,}001$ представлены на рисунке 12. Из рисунков 10б и 12 следует, что для достижения максимально положительного результата требуется применение многомерного подхода к выбору параметров предлагаемого способа.

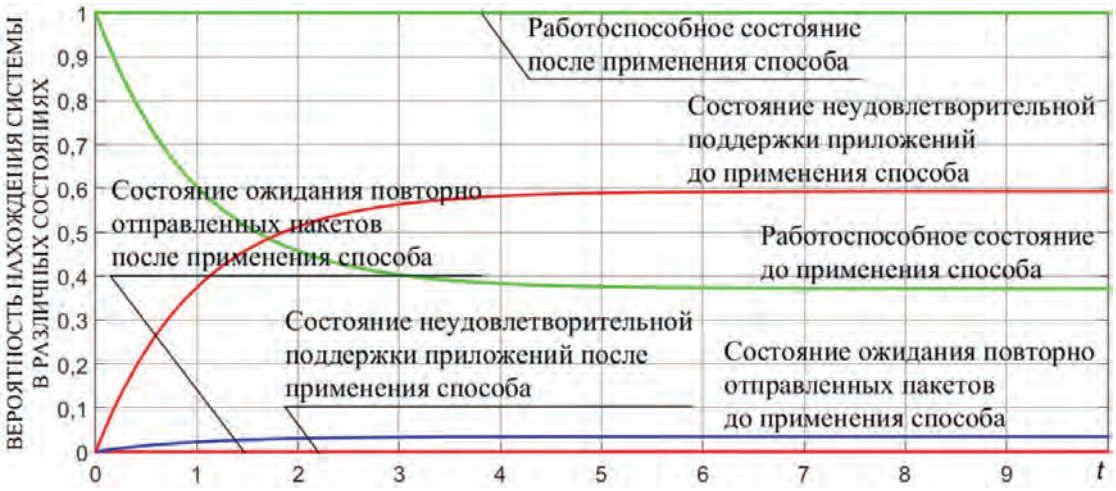
На рисунке 13 представлены зависимости вероятности обеспечения удовлетворительной поддержки приложений от вероятности стирания пакета в условиях применения предлагаемого способа с различными параметрами.

Заключение

Совместное использование методов криптографического контроля целостности данных и методов восстановления данных на основе избыточного линейного кодирования позволило получить синергетический эффект, выражающийся в возможности восстановления до $d_{\text{мин}} - 1$ пакетов, подвергшихся стираниям (при допущении об идеальных свойствах используемой имитовставки). Таким образом предложенный способ позволяет повысить устойчивость и скорость передачи данных по каналам VPN в условиях деструктивных воздействий на них злоумышленника.

Векторный характер вычислений над $GF(2)$ обуславливает высокую скорость реализации операций кодирования и декодирования стандартными вычислительными средствами, в том числе, при их программной реализации. Полученные данные подтверждаются результатами имитационного моделирования.

а) $\mu = 0{,}0001$, $\mu_{\text{допустимое}} = 0{,}001$, $\lambda = 0{,}000016$, $\gamma = 1$, $M = 10000$, $N = 100$, $D = 120$, $R = 7$



б) $\mu = 0,0009$, $\mu_{\text{допустимое}} = 0,001$, $N = 100$, $D = 120$, $R = 7$

Рис. 11. Динамика изменения вероятности нахождения системы в различных состояниях:
а) до и после применения предлагаемого способа в условиях имитации пакетов данных злоумышленником
б) до и после применения предлагаемого способа в условиях деструктивного воздействия злоумышленника

Рис. 12. Динамика изменения вероятности нахождения системы в различных состояниях в условиях деструктивного воздействия злоумышленника и применения предлагаемого способа с различными параметрами при $\mu = 0,0097$, $\mu_{\text{допустимое}} = 0,001$, $N = 200$

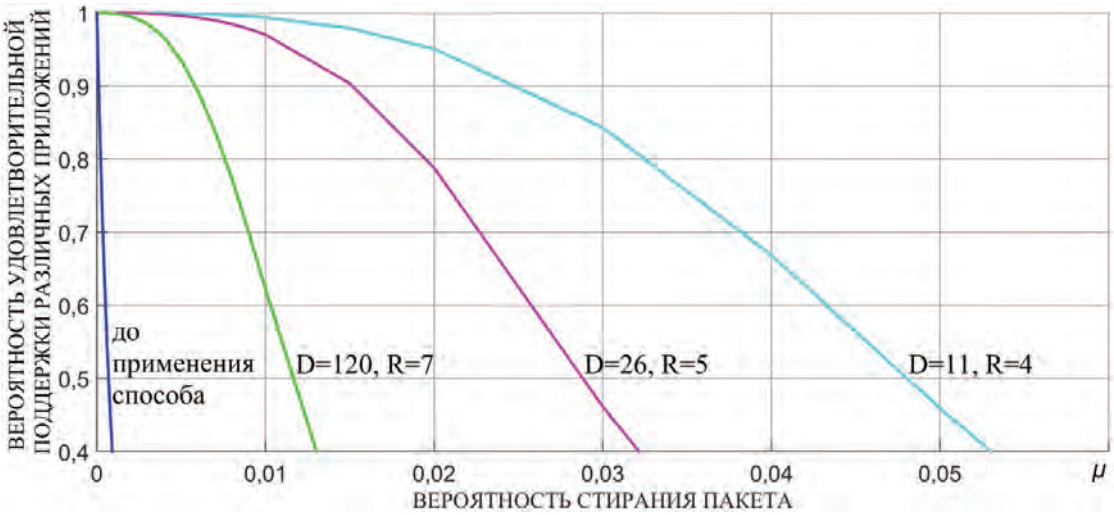


Рис. 13. Зависимость вероятности удовлетворительной поддержки различных приложений от вероятности стирания пакета в условиях применения предлагаемого способа с различными параметрами

Литература

1. Шваб К. Четвертая промышленная революция. – М: Эксмо, 2021. – 208 с.
2. Гулин К.А. Тренды четвертой промышленной революции (рецензируется: Шваб К. Четвертая промышленная революция: монография: пер. с англ. – М.: Изд-во «Э», 2017) / К.А. Гулин, В.С. Усков // Экономические и социальные перемены: факты, тенденции, прогноз. – 2017. – Т. 10. – № 5. – С. 216-221.
3. Маслов В.И., Четвертая промышленная революция: истоки и последствия / В.И. Маслов, И.В. Лукьянов // Вестн. моск. ун-та., сер. 27. Глобалистика и геополитика, 2017. № 2. – С. 38–48.
4. 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.
5. 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.
6. 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).
7. Макаренко С.И. Время сходимости протоколов маршрутизации при отказах в сети // Системы управления, связи и безопасности. – 2015. – № 2. – С. 45-98.
8. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы: Юбилейное издание. – СПб.: Питер, 2020. – 1008 с.
9. Стародубцев Ю.И. Техносферная война как основной способ разрешения конфликтов в условиях глобализации / Ю.И. Стародубцев, П.В. Закалкин, С.А. Иванов // Военная мысль. – 2020. – № 10. – С. 16-21.
10. Макаренко С.И. Сетецентрическая война – принципы, технологии, примеры и перспективы: монография / С.И. Макаренко, М.С. Иванов. – СПб: Наукоёмкие технологии, 2018. – 898 с.
11. Kawano R., Yasudo R., Matsutani H., Amano H. K-optimized path routing for high-throughput data center networks. // In Proceedings - 2018 6th International Symposium on Computing and Networking, CANDAR 2018 (Takayama, Japan, November 27-30, 2018). IEEE, 2018, pp. 99–105. DOI: 10.1109/CANDAR.2018.00020.
12. Lu Y., Chen G., Li B., Tan K., Xiong Y., Cheng P., Zhang J., Chen E., Moscibroda T. Multi-path transport for RDMA in datacenters. In Proceedings 15th USENIX Symposium on Networked Systems Design and Implementation (NSDI 18) (Renton, WA, USA, April 9–11, 2018). pages 357–371, 2018.
13. 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.
14. 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.
15. 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.
16. Moon T. Error Correction Coding: Mathematical Methods and Algorithms: Second Edition. – Hoboken, New Jersey, USA: Wiley, 2020. – 992 p.

ENSURING THE INTEGRITY OF DATA TRANSMITTED OVER THE COMMUNICATION CHANNELS OF VIRTUAL PRIVATE NETWORKS

Karpov S.S.[21], Ryabinin Ju.E.[22], Finko O.A.[23]

Annotation

A method of ensuring the integrity of data transmitted over communication channels of VPNs of large-scale information systems functioning in the conditions of the destructive influence of the attacker is considered. The proposed method allows to recover data packets subjected to erasure and imitation.

***The purpose of the research** is to increase the stability of data transmission over VPN communication channels by implementing the procedure for recovering erased IP-packets and increasing the level of imitation security of the transmitted data.*

***Research methods:** aggregation of methods of cryptographic control of data integrity and methods of redundant coding of data, application of methods of the theory of Markov random processes to determine the probability of providing satisfactory support for applications in conditions of destructive influence of an attacker with various parameters.*

***Research results:** analysis of the object of research – VPN of large-scale information systems was carried out. It leads to the conclusion about the need to protect data transmitted through such communication channels for the implementation of national strategies for economic development. A mathematical model of the functioning of a data transmission system over a VPN communication channel under the conditions of a destructive influence of an attacker is presented. A method is proposed to ensure the integrity of transmitted data based on an original scheme for sharing known solutions, generating a synergistic effect. The method allows recovering $d_{\min} - 1$ erased data packets.*

The proposed solution makes it possible to increase the stability and speed of data transmission over the communication channels of the network in the conditions of the destructive influence of the attacker and the imitation of data by the attacker.

***Keywords:** information security and protection, VPN, cryptographic insertion, packet erasure, error-correcting coding, VPN protection against cyber threats, multipath routing, multidimensional route.*

References

1. Shvab K. Chetvertaya promyshlennaya revolyuciya. – M: Eksmo, 2021. – 208 s.
2. Gulin K.A. Trendy chetvertoj promyshlennoj revolyucii (recenziruetsya: Shvab K. Chetvertaya promyshlennaya revolyuciya: monografiya: per. s angl. – M.: Izd-vo «E», 2017) / K.A. Gulin, V.S. Uskov // Ekonomicheskie i social'nye peremeny: fakty, tendencii, prognoz. – 2017. – T. 10. – № 5. – S. 216-221.
3. Maslov V.I., Chetvertaya promyshlennaya revolyuciya: istoki i posledstviya / V.I. Maslov, I.V. Lukyanov // Vestn. mosk. un-ta., ser. 27. Globalistika i geopolitika, 2017. № 2. – S. 38–48.
4. Ivanov V.G. Model' tekhnicheskoj osnovy sistemy upravleniya special'nogo naznacheniya v edinom informacionnom prostranstve na osnove konvergentnoj infrastruktury sistemy svyazi: monografiya. – SPb.: Politekh-press, 2018. – 214 s.
5. Vorobyov S.P., Davydov A.E., Efimov V.V., Kurnosov V.I. Infokommunikacionnye seti. Tom 1: Infokommunikacionnye seti: klassifikaciya, struktura, arhitektura, zhiznennyj cikl, tekhnologii: enciklopediya. – SPb.: Naukoemkie tekhnologii, 2019. – 739 s.
6. Makarenko S.I. Eksperimental'noe issledovanie reakcii seti svyazi i effektov peremarshrutizacii informacionnyh potokov v usloviyah dinamicheskogo izmeneniya signal'no-pomekhovoj obstanovki // Zhurnal radioelektroniki. – 2016. – № 4. – URL: http://jre.cplire.ru/jre/apr16/4/text.html (data obrashcheniya: 01.03.2021).
7. Makarenko S.I. Vremya skhodimosti protokolov marshrutizacii pri otkazah v seti // Sistemy upravleniya, svyazi i bezopasnosti. – 2015. – № 2. – S. 45-98.

21 Sergey Karpov, postgraduate student at the Department 22 (special communication technology), Krasnodar Higher Military Orders of Zhukov and the October Revolution Red Banner School named after General of the Army S.M. Shtemenko. Krasnodar, Russia.

E-mail: karpov.sergey.sergeevich@yandex.ru.

22 Jurii Ryabinin, Ph.D. of Engineering Sciences, doctoral candidate of holder of an Advanced Doctorate in Engineering Sciences at the Department 22 (special communication technology), Krasnodar Higher Military Orders of Zhukov and the October Revolution Red Banner School named after General of the Army S.M. Shtemenko. Krasnodar, Russia. E-mail: jurandvau@inbox.ru.

23 Oleg Finko, Dr.Sc., Professor, Professor at the Department 22 (special communication technology), Krasnodar Higher Military Orders of Zhukov and the October Revolution Red Banner School named after General of the Army S.M. Shtemenko, Krasnodar, Russia, Professor at the Department of information security of automated systems, North Caucasus Federal University, Stavropol, Russia, Academic Advisor of the Russian Academy of Rocket and Artillery Sciences (RARAN), Krasnodar, Russia. E-mail: ofinko@yandex.ru.

8. Olifer V., Olifer N. Komp'yuternye seti. Principy, tekhnologii, protokoly: Yubilejnoe izdanie. – SPb.: Piter, 2020. – 1008 s.
9. Starodubczev U.I. Tekhnosfernaya vojna kak osnovnoj sposob razresheniya konfliktov v usloviyakh globalizaczii / U.I. Starodubczev, P.V. Zakalkin, S.A. Ivanov // Voennaya mysl`. – 2020. – № 10. – S. 16-21.
10. Makarenko S.I. Setecentricheskaya vojna – principy, tekhnologii, primery i perspektivy: monografiya / S.I. Makarenko, M.S. Ivanov. – SPb: Naukoyomkie tekhnologii, 2018. – 898 s.
11. Kawano R., Yasudo R., Matsutani H., Amano H. K-optimized path routing for high-throughput data center networks. // In Proceedings — 2018 6th International Symposium on Computing and Networking, CANDAR 2018 (Takayama, Japan, November 27-30, 2018). IEEE, 2018, pp. 99–105. DOI: 10.1109/CANDAR.2018.00020.
12. Lu Y., Chen G., Li B., Tan K., Xiong Y., Cheng P., Zhang J., Chen E., Moscibroda T. Multi-path transport for RDMA in datacenters. In Proceedings 15th USENIX Symposium on Networked Systems Design and Implementation (NSDI 18) (Renton, WA, USA, April 9–11, 2018). pages 357–371, 2018.
13. 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.
14. Samoylenko D.V., Finko O.A., Eremeev M.A. Raspredelyonnaya obrabotka i zashchita informacii v gruppirovke kompleksov s bespilotnymi letatel'nymi apparatami // Teoriya i tekhnika radiosvyazi. – 2017. – № 4. – S. 93-100.
15. Samoylenko D.V., Finko O.A. Pomekhoustojchivaya peredacha dannyh v radiokanalah robototekhnicheskih kompleksov na osnove polinomial'nyh klassov vychetov // Naukoemkie tekhnologii v kosmicheskih issledovaniyah Zemli. – 2016. – T.8. – № 3. – S. 49-55.
16. Moon T. Error Correction Coding: Mathematical Methods and Algorithms: Second Edition. – Hoboken, New Jersey, USA: Wiley, 2020. — 992 p.