УДК 004.056.2

Модель процесса анализа сетевой активности элементов телефонной IP-сети комплексом компьютерной разведки нарушителя

А. А. Привалов[1, 3], Д. Д. Титов[1, 2]

[1] Петербургский государственный университет путей сообщения Императора Александра I, Россия, 190031, Санкт-Петербург, Московский пр., 9

[2] ОАО «Супертел», Россия, 197046, Санкт-Петербург, Петроградская наб., 38

[3] Академия войск национальной гвардии, Россия, 198206, Санкт-Петербург, ул. Л. Пилютова, 1

Для цитирования: *Привалов А. А., Титов Д. Д.* Модель процесса анализа сетевой активности элементов телефонной IP-сети комплексом компьютерной разведки нарушителя // Известия Петербургского университета путей сообщения. СПб.: ПГУПС, 2026. Т. 23, вып. 2. С. 516–530. DOI: 10.20295/1815-588X-2026-2-516-530

Аннотация

Цель: разработка и анализ стохастической модели процесса анализа сетевой активности элементов телефонной IP-сети, выполняемого комплексом компьютерной разведки (КР) нарушителя, для количественной оценки временных характеристик разведывательного цикла. **Методы:** алгоритм работы сетевого сканера представлен в виде стохастической сети (GERT-модели), где этапы обнаружения активных элементов, определения ролей узлов, типов операционных систем, портов/сервисов и анализа уязвимостей описываются дугами со своими функциями распределения времени и вероятностями успеха, а повторные запуски — петлями возврата. Для ветвей «Роль», ОС и «Порты/сервисы» получены эквивалентные изображения по Лапласу плотностей распределения, на основе которых выведены эквивалентные функции для параллельного блока и полного цикла работы сканера в режимах полного и частичного сканирования. Интегральная функция распределения, среднее время и уровень требований рассчитываются на основе полученных аналитических выражений. **Результаты:** получены компактные формулы для эквивалентной функции, функции распределения и среднего времени разведки VoIP-сети в зависимости от вероятностей успешного выполнения ключевых операций. Показано, что временные характеристики процесса имеют выраженную нелинейную зависимость от значения этих вероятностей: при их увеличении наблюдается многократное сокращение среднего времени и срока успешного завершения сканирования. Сравнение режимов полного и частичного сканирования демонстрирует ожидаемый компромисс между полнотой добываемой компьютерной разведкой информации и скоростью получения результатов. **Практическая значимость:** модель позволяет прогнозировать временные показатели работы комплекса КР в VoIP-сети, выявлять узкие места, а также количественно оценивать влияние архитектуры сети и параметров средств защиты на скорость получения нарушителем критически важной информации, что дает основу для обоснованного выбора мер по повышению киберустойчивости.

Ключевые слова: телефонная IP-сеть, комплекс компьютерной разведки, сетевой сканер, анализ сетевой активности, стохастическая сеть, GERT-модель, эквивалентная функция, полное и частичное сканирование

Введение

Телефонная IP-сеть в современных корпоративных и ведомственных инфраструктурах перестала быть узкоспециализированным голосовым сегментом. Она стала частью единой информационно-телекоммуникационной

среды, обеспечивающей критичные для управления и производственного цикла сервисы — от сигнализации и диспетчеризации до интеграции с прикладными системами, системами мониторинга и корпоративными каталогами. Переход к пакетной передаче речи и сигнализации, использование стандартных стеков TCP/IP и широкая номенклатура протоколов (SIP/RTP, H.323, MGCP, HTTP(S), SNMP, SSH и др.) объективно повышают функциональные возможности сети, но и одновременно расширяют поверхность атаки. В этих условиях ключевым фактором киберустойчивости становится не только наличие средств защиты на периметре и внутри сегментов, но и способность оператора оценить, с какой скоростью и полнотой нарушитель может построить модель сети, идентифицировать роли ее элементов, определить типы операционных систем и сервисов, а также перейти от разведки к эксплуатации уязвимостей.

На практике действия нарушителя редко представляют собой единичный акт сканирования. Компьютерная разведка (КР) — это управляемый многоэтапный процесс, в котором отдельные процедуры запускаются последовательно и параллельно, повторяются при сбоях, адаптируются к текущему состоянию сети и политике фильтрации. Сетевая активность нарушителя, как правило, включает:

- подключение к целевой ИТКС (или вход в сегмент через компрометированный узел);
- первичное выявление активных элементов;
- последующую классификацию узлов по функциональным ролям;
- определение типов ОС и версий стеков;
- перечисление портов и сервисов;
- корреляцию наблюдений с базами уязвимостей;
- формирование отчета и принятие решения о дальнейших действиях.

Существенная особенность телефонной IP-сети заключается в том, что часть ее элементов и сервисов обладает динамической природой (перерегистрация терминалов, NAT-трансляции, кластеризация call-серверов, балансировка, резервирование), а также имеет выраженную неоднородность по уровню защищенности (ядро/агрегация/доступ, серверные узлы, пограничные шлюзы, абонентские терминалы). Это приводит к тому, что время разведывательного цикла и вероятность успеха отдельных операций становятся случайными величинами, зависящими от архитектуры сети, конфигурации средств защиты, режимов мониторинга, уровня противодействия и многих других факторов.

Несмотря на очевидную практическую значимость, количественная оценка временных характеристик разведки в отношении телефонных IP-сетей часто выполняется упрощенно: либо на уровне детерминированных нормативов и экспертных оценок, либо с использованием сильно упрощенных моделей без явной аналитической связи между параметрами этапов и интегральными показателями процесса. Такие подходы затрудняют сравнение альтернативных архитектурных решений и защитных мер. Между тем именно такие вопросы непосредственно связаны с управлением рисками: временной выигрыш в пользу оператора означает дополнительный ресурс на обнаружение аномалий, реагирование и локализацию воздействия.

В настоящей статье предлагается стохастическая модель процесса анализа сетевой активности элементов телефонной IP-сети комплексом компьютерной разведки нарушителя, основанная на представлении этапов разведки в виде стохастической сети. В модели операции процесса (поиск активных элементов, определение роли узлов, идентификация

типов ОС, выявление сервисов и портов, анализ уязвимостей, формирование отчета) описываются дугами сети с заданными распределениями времени и вероятностями успешного завершения. Логика взаимодействия этапов реализуется вершинами — узлами сети, включая параллельные ветвления и синхронизацию по правилу логического «И», а также механизм повторных запусков процедур при сбоях. Такое представление позволяет перейти от качественного описания действий нарушителя к формальной модели, в которой интегральные функции распределения, математическое ожидание и дисперсия времени реализации моделируемого процесса выводятся из параметров базовых операций.

Цель работы заключается в разработке и аналитическом исследовании стохастической модели подсистемы сетевого сканирования как ядра процесса анализа сетевой активности, а также в получении выражений для вероятностно-временных характеристик полного цикла разведки.

Новизна работы состоит в том, что процесс анализа сетевой активности телефонной IP-сети рассматривается как связанный стохастический процесс с параллельными ветвями и механизмом повторов, а ключевые показатели времени разведки выводятся аналитически через эквивалентные функции, являющиеся изображением моделируемого процесса по Лапласу, и определяются моменты случайного времени реализации этого процесса.

Тем самым работа направлена на создание прикладного аппарата, позволяющего связать архитектуру и режимы защиты телефонной IP-сети с вероятностно-временными характеристиками компьютерной разведки нарушителя и использовать эту связь для обоснования организационно-технических решений по повышению устойчивости функционирования сети.

Постановка задачи

Пусть имеется телефонная IP-сеть. Процесс компьютерной разведки начинается с поэтапного обследования сети с использованием сетевого сканера, что позволяет нарушителю формировать представление о структурной связанности сети, а также о весах и ролях ее отдельных элементов. После подключения к телефонной IP-сети происходит определение ее активных элементов за некоторое время $t_{элем}$ с функцией распределения $Q(t)$. В процессе работы сетевого сканера параллельно выполняются следующие операции:

1. Определение роли узлов сети за некоторое время $t_{роль}$ с функцией распределения $R(t)$. При успешном завершении данного этапа (а вероятность этого события равна P_1) каждому ранее обнаруженному активному элементу ставится в соответствие его функциональная роль на основе совокупности выявленных сервисов, открытых портов и характеристик обрабатываемого трафика.

2. Определение типов операционных систем на обнаруженных узлах за некоторое время $t_{ОС}$ с функцией распределения $D(t)$. Условная вероятность успешного определения типов ОС полагается равной P_2.

3. Определение портов и предоставляемых сервисов на активных элементах за некоторое время $t_{АС}$ с функцией распределения $L(t)$. На этом этапе уточняется роль узлов в сети по совокупности запускаемых сервисов. Вероятность успешной реализации данного этапа равна P_3.

Выполнение описанных выше этапов позволяет нарушителю определить сетевые уязвимости за некоторое время $t_{уяз}$ с функцией распределения $O(t)$. Таким образом реализуется структурированное описание ролей узлов, типов ОС и открытых портов с привязкой к выявленным уязвимостям.

Сбой на любом из перечисленных этапов приводит к повторному запуску процедуры сканирования за некоторое время $t_{\text{повтр.}}$ с функцией распределения $M(t)$. Успешное завершение работы сетевого сканера инициирует процесс обработки и агрегирования полученной информации. На этом заключительном этапе формируется отчет о структурной связанности сети, ролях ее элементов, типах эксплуатируемых операционных систем и выявленных уязвимостях.

Требуется определить функцию распределения $F(t)$ и среднее время $\overline{T}$ успешной реализации нарушителем процесса КР.

Допущения и ограничения:

1. Доступность объектов опроса. DNS-сервер, пограничный маршрутизатор (RIP) и SNMP-агенты элементов телефонной IP-сети считаются доступными для сетевого сканера в пределах выбранной области наблюдения; сетевые ответы трактуются как «получен / не получен» (успех/неудача) в рамках принятой вероятностной схемы.

2. Независимость параллельных подпроцессов. Время реализации частных процессов считается независимыми случайными величинами. Взаимодействия через общие ресурсы, а также корреляции задержек в базовой постановке не учитываются.

3. Стационарность параметров. Параметры распределений $L(t)$, $N(t)$, $O(t)$, $M(t)$ и вероятности P_i, $i = \overline{1,3}$ предполагаются постоянными на интервале анализа.

Решение

Описанный в постановке задачи процесс работы комплекса компьютерной разведки представлен в виде стохастической сети (рис. 1).

Функции распределения времени реализации частных этапов имеют вид:

$$R(t) = 1 - e^{-rt};\ D(t) = 1 - e^{-dt};\ L(t) = 1 - e^{-lt};$$

$$O(t) = 1 - e^{-ot};\ Q(t) = 1 - e^{-qt};\ M(t) = 1 - e^{-mt};$$

где $R = \dfrac{1}{t_a}; L = \dfrac{1}{t_b}; O = \dfrac{1}{t_c}; Q = \dfrac{1}{t_g}; M = \dfrac{1}{t_{повт.}};$

t_a, t_b, t_c, t_d, t_g, $t_{\text{повт}}$, — среднее время k-го процесса работы комплекса КР.

Для аналитического вывода далее используется редуцированная модель, в которой

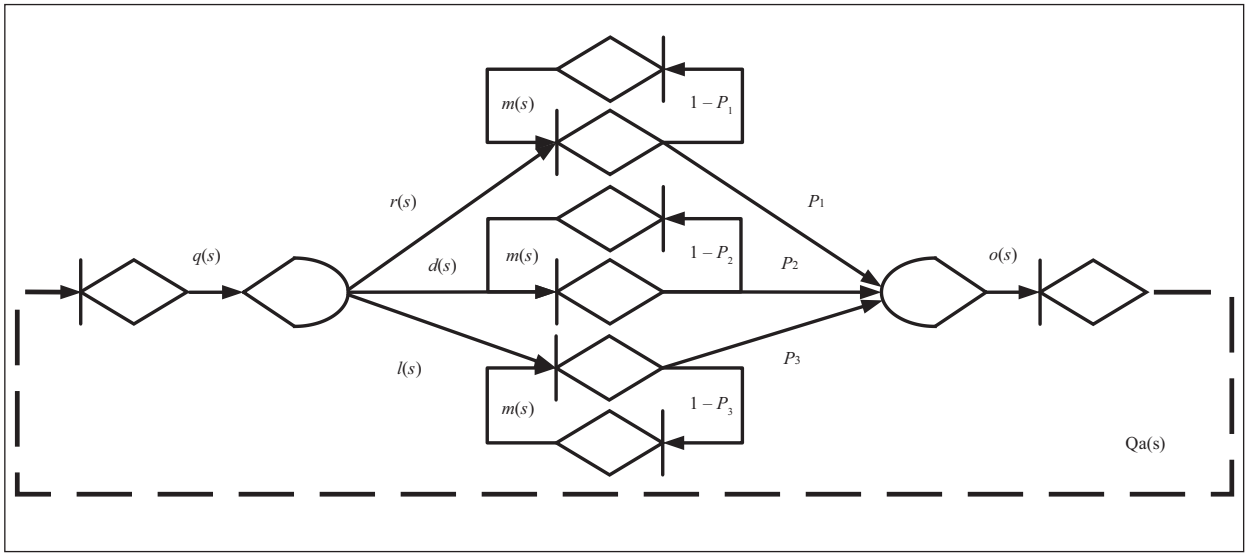

Рис. 1. Стохастическая сеть работы сетевого сканера

ключевым элементом является параллельный узел логического «И» с тремя ветвями: $r(s)$, $d(s)$, $l(s)$. Входной и выходной участки представлены последовательными блоками $q(s)$ и $o(s)$ (рис. 2).

Пусть T_R, T_D, T_L, — независимые значения времени реализации ветвей. Для логического «И» момент реализации узла:

$$T = \max\{T_R;\ T_D;\ T_L\}. \tag{1}$$

Тогда функция распределения времени реализации узла «И» равна произведению функций распределения времени реализации ветвей:

$$F_3(t) = 1 - e^{-rt} - e^{-dt} - e^{-lt} + e^{-(r+d)t} + e^{-(r+l)t} - e^{-(l+r+d)t},\ t \geq 0. \tag{2}$$

Плотность распределения:

$$f_3(t) = \frac{d}{dt}F_3(t) = re^{-rt} + de^{-dt} + le^{-lt} - (r+d)e^{-(r+d)t} - (r+l)e^{-(r+l)t} - (l+d)e^{-(l+d)t} + (l+r+d)e^{-(l+r+d)t}, t \geq 0. \tag{3}$$

После получения явного выражения для плотности $f_3(t)$, которая описывает время реализации узла «И» для трех ветвей, для удобства последующих расчетов ее целесообразно аппроксимировать гамма-распределением. Выбор гамма-распределения обусловлен тем, что при моделировании систем массового обслуживания погрешность аппроксимации функций распределения времени свершения целевых процессов оказывается достаточно малой [11]. Кроме того, данный вид распределения является встроенной функцией в абсолютном большинстве пакетов прикладных программ, широко используемых при моделировании систем и процессов.

Для определения параметров аппроксимирующего $f_3(t)$ распределения определим параметры формы и масштаба:

$$M^1_{f_3} = E\left[T_\Delta\right];\ M^2_{f_3} = E\left[T_\Delta{}^2\right];\quad D_{f_3} = M^2_{f_3} - (M^1_{f_3})^2. \tag{4}$$

$$\alpha_3 = \frac{(M^1_{f_3})^2}{D_{f_3}};\ \mu_3 = \frac{M^1_{f_3}}{D_{f_3}}. \tag{5}$$

Таким образом, фрагмент стохастической сети, соответствующий логической операции «И», характеризуется изображением неполной гамма-функции:

$$f_3(s) \approx \gamma_3 = \left(\frac{\mu_3}{\mu_3 + s}\right)^{\alpha_3},\ s \geq 0. \tag{6}$$

На рис. 3 показано сопоставление функции распределения времени реализации логического узла «И» и аппроксимирующего ее гамма-распределения. Видно, что функции практически совпадают, а максимальное отклонение не превышает 3 %. Следовательно, аппроксимация узла «И» гамма-распределением по двум

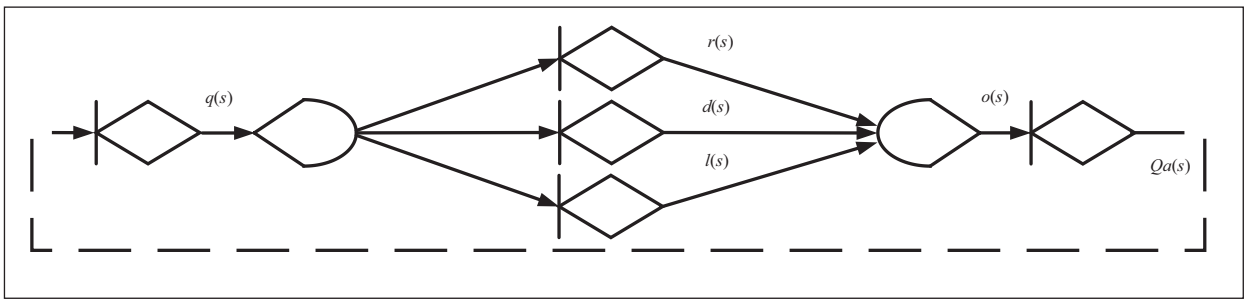

Рис. 2. Редуцированная стохастическая сеть: последовательное соединение входного блока, узла «И» (три параллельные ветви) и выходного блока

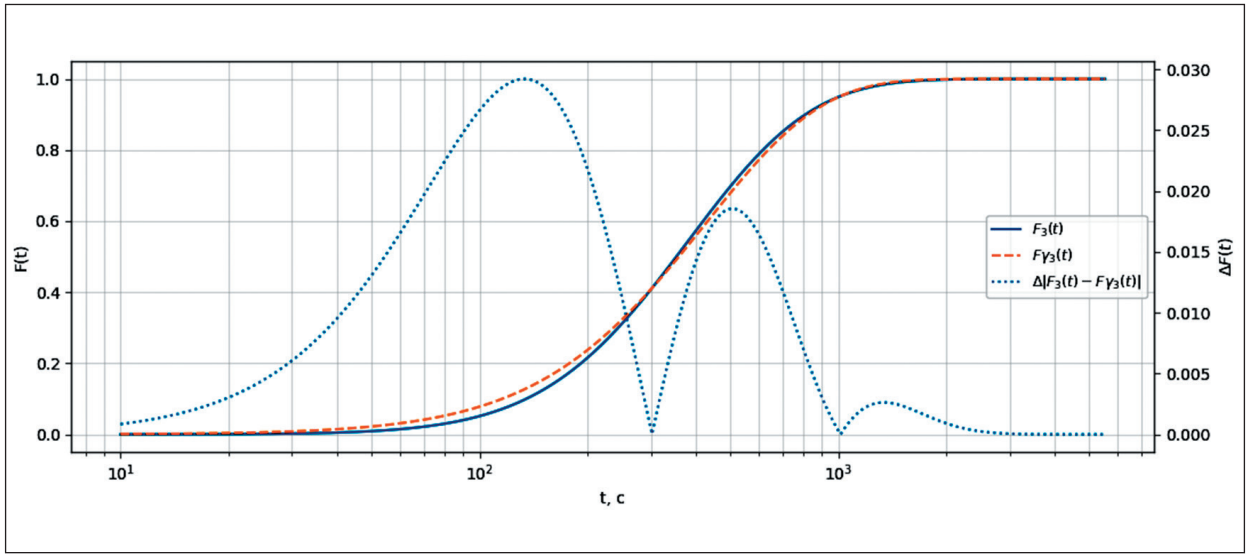

Рис. 3. Графики функции распределения времени реализации логического узла «И» и аппроксимирующего гамма-распределения

моментам обеспечивает компактную инкапсуляцию при умеренной погрешности, которая далее переносится на эквивалентную модель подсети и должна учитываться при оценке суммарного времени завершения.

Результат (6) позволяет преобразовать исходную стохастическую сеть к виду (рис. 4) и получить ее эквивалентную функцию (7):

$$Q_a(s) = \frac{q}{q+s} \cdot \frac{o}{o+s} \cdot \left(\frac{\mu_3}{\mu_3 + s} \right)^{\alpha_3}. \qquad (7)$$

Эквивалентная функция $Q_a(s)$ является изображением по Лапласу плотности времени свершения всего процесса компьютерной разведки. Для дальнейшего анализа определим первый и второй начальные моменты случайного времени свершения процесса, а затем итоговую функцию распределения.

Используя стандартные соотношения для начальных моментов:

$$E[T] = -\frac{dQ_a(s)}{ds}\bigg|_{s=0}; E[T^2] = -\frac{d^2Q_a(s)}{ds^2}\bigg|_{s=0}, \qquad (8)$$

определим дисперсию времени реализации модельного процесса:

$$D[T] = E[T^2] - (E[T])^2. \qquad (9)$$

Для получения интегральной функции распределения $F(t) = P(T \le t)$ обозначим: α — параметр формы, β — параметр масштаба. Тогда при

$$E[T] = \mu^{-1}; D[T] = \sigma^2, \qquad (10)$$

$$\alpha = \frac{\mu^{-2}}{\sigma^2}; \ \beta = \frac{\mu^{-1}}{\sigma^2} \qquad (11)$$

искомая функция распределения времени успешного выполнения задачи компьютерной разведки, выполняемой сетевым сканером, определяется как:

$$Q_a(t) = \frac{\beta^\alpha}{\Gamma(\alpha)} \int_0^t t^{\alpha-1} e^{\{-\beta t\}} dt, \qquad (12)$$

равно:

$$T = \int_0^\infty t d[Q_a(t)] = \frac{\alpha}{\beta}. \qquad (13)$$

Таким образом, поставленная задача решена.

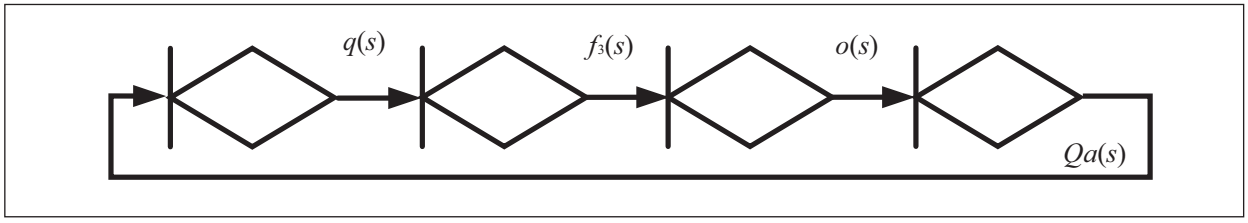

Рис. 4. Приведение редуцированной сети к последовательной структуре: $q(s) - f_3(s) - o(s)$ и формирование эквивалентной функции $Q_a(s)$

Пример расчета

В качестве исходных данных используются следующие значения времени и вероятности, соответствующие профильной полной модели процесса анализа сетевой активности элементов:

$$t_{OC} = 360 \text{ с}, t_{элем} = 200 \text{ с}, t_{AC} = 230 \text{ с},$$
$$t_{уязв.} = 300 \text{ с}, t_{роль} = 320 \text{ с}, t_{повт.} = 210 \text{ с},$$
$$P1 = 0{,}5, P2 = 0{,}5, P3 = 0{,}5.$$

На рис. 5 и 6 показаны функция распределения времени успешного выполнения задачи КР сетевым сканером и зависимость среднего времени реализации данного процесса от вероятности доступности телефонной IP-сети, под которой понимается вероятность такого события, когда нарушитель обладает аппаратными и программными средствами, обеспечивающими ему скрытое подключение к защищаемой сети.

Таким образом, при среднем уровне подготовки нарушителя — специалиста в области компьютерной разведки и невысокой вероятности доступности сети через 25,8 минуты телефонная IP-сеть будет вскрыта и нарушитель определит ее основные уязвимости.

Анализ полученных результатов

Предельная оценка минимального времени компьютерной разведки и влияние профиля сканера на гарантированное завершение процесса

Минимально достижимое время реализации компьютерной разведки целесообразно оценивать как предельную нижнюю границу процесса, соответствующую идеализированному случаю отсутствия сбоев и повторов, то есть при $P_i = 1$ для всех вероятностных этапов. В этом режиме строится эталонный график функции распределения $Q_a(t) = Pr\{T \le t\}$, который задает наилучшую возможную динамику завершения: при любых $P_i < 1$ кривая $Q_a(t)$ неизбежно смещается влево, а вероятность завершения к моменту времени t оказывается не выше эталонной.

Для полного профиля операций в предельном случае $P_i = 1$ получены ориентиры: по среднему времени $T_{min} = \Sigma T_{mcin} = 16{,}5$ минуты и по уровню гарантированного завершения $t_{0,95} \approx 29{,}5$ минуты, что соответствует пересечению кривой распределения с прямой $Q_a(t) = 0{,}95$. Представленные графики позволяют проследить диапазоны времени для различных видов сканеров, задаваемые профилем применяемых операций (рис. 7). Укороченные профили обеспечивают более раннее достижение заданного уровня $Q_a(t)$, но формируют менее информативный результат; расширенные профили повышают обоснованность и точность местоопределения, однако увеличивают длительность процесса, что проявляется сдвигом кривых вправо и ростом $t_{0,95}$.

Показано, что усложнение профиля операций компьютерной разведки принципиально не может привести к сокращению времени добывания разведданных, нижняя граница которого соответствует лучшему времени «самого лучшего»

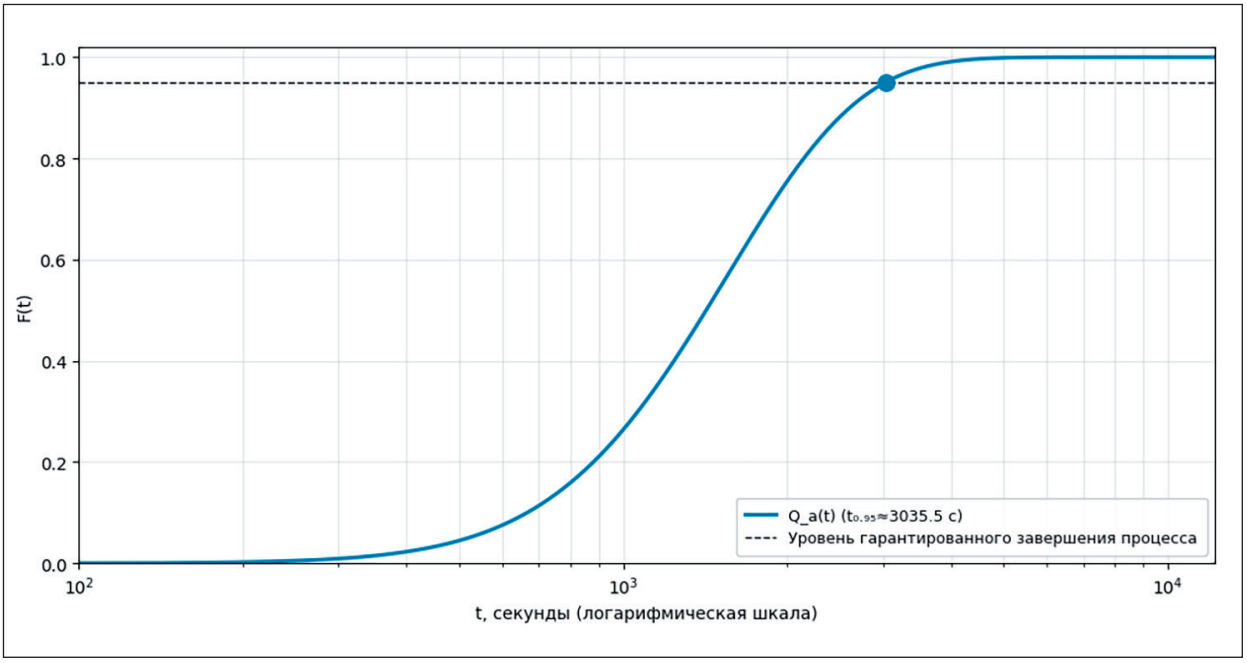

Рис. 5. Функция распределения времени успешного выполнения задачи КР сетевым сканером

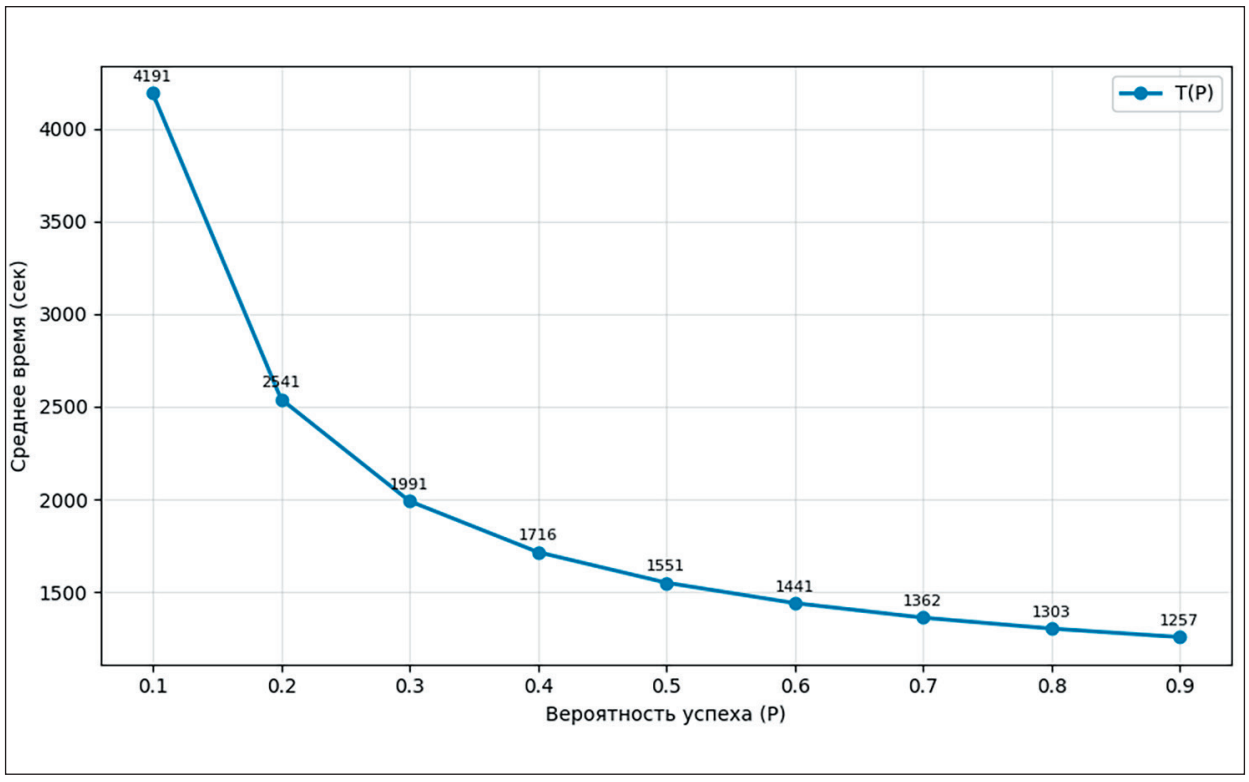

Рис. 6. График зависимости среднего времени реализации данного процесса от вероятности доступности телефонной IP-сети

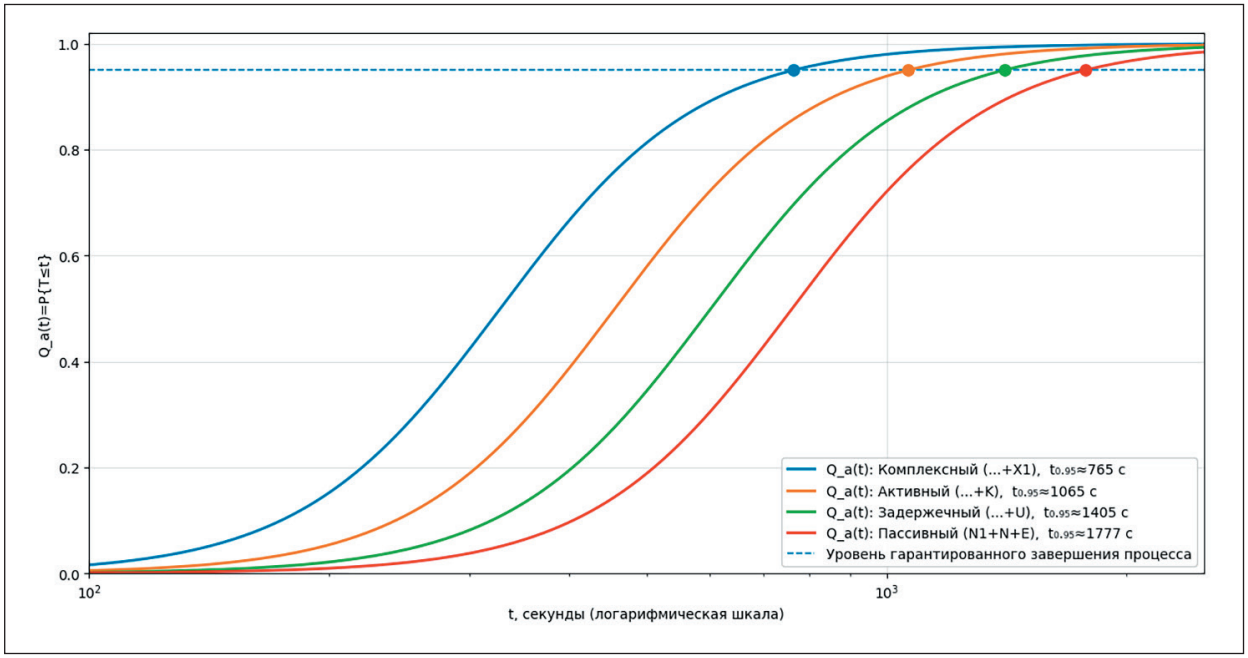

Рис. 7. Предельные функции распределения времени завершения компьютерной разведки

эталонного режима. Поскольку ни один практический сканер не обеспечивает единичную характеристику успеха на всех стадиях, рассчитанный эталон при $P_i = 1$ следует рассматривать как предельный, а нижнюю границу времени для выбранного профиля операций как:

$$Q^*_a(t) = \lim_{P_1 \to 1, \ldots, P_n \to 1} Q_a(t; P_1, \ldots, P_n). \quad (14)$$

Доступность сети как ограничивающий фактор компьютерной разведки и сценарии поведения нарушителя

Доступность к телефонной IP-сети в рамках модели КР должна рассматриваться как входная вероятностная характеристика, определяющая сам факт запуска полного профиля разведывательных операций. Она задается параметром $P_{\text{дост}}$ — вероятностью успешного установления доступа/сеанса на одной попытке и определяется совокупностью факторов физической и логической достижимости: состоянием каналов и маршрутизации, эксплуатационной готовностью сегмента, политиками сегментации и фильтрации (ACL/Firewall), требованиями аутентификации/туннелирования, ограничениями по частоте и объему обращений, а также воздействиями внешних условий (перегрузка, регламентные работы, деградация качества связи).

В модели КР влияние доступности формализуется как дополнительное звено перед основным профилем операций: при $P_{\text{дост}} << 1$ возникают вынужденные повторы попыток входа с задержкой, что приводит к сдвигу функции распределения $Q_a(t) = Pr\{T \le t\}$ вправо и росту среднего времени. На рис. 8 приведены функции при различных значениях вероятностей доступности. С практической точки зрения характер кривых задает поведенческую развилку нарушителя: при высокой доступности он способен опираться на активные стадии и планировать получение результата в ограниченном окне времени; при средней доступности стратегия смещается к работе в расширенном

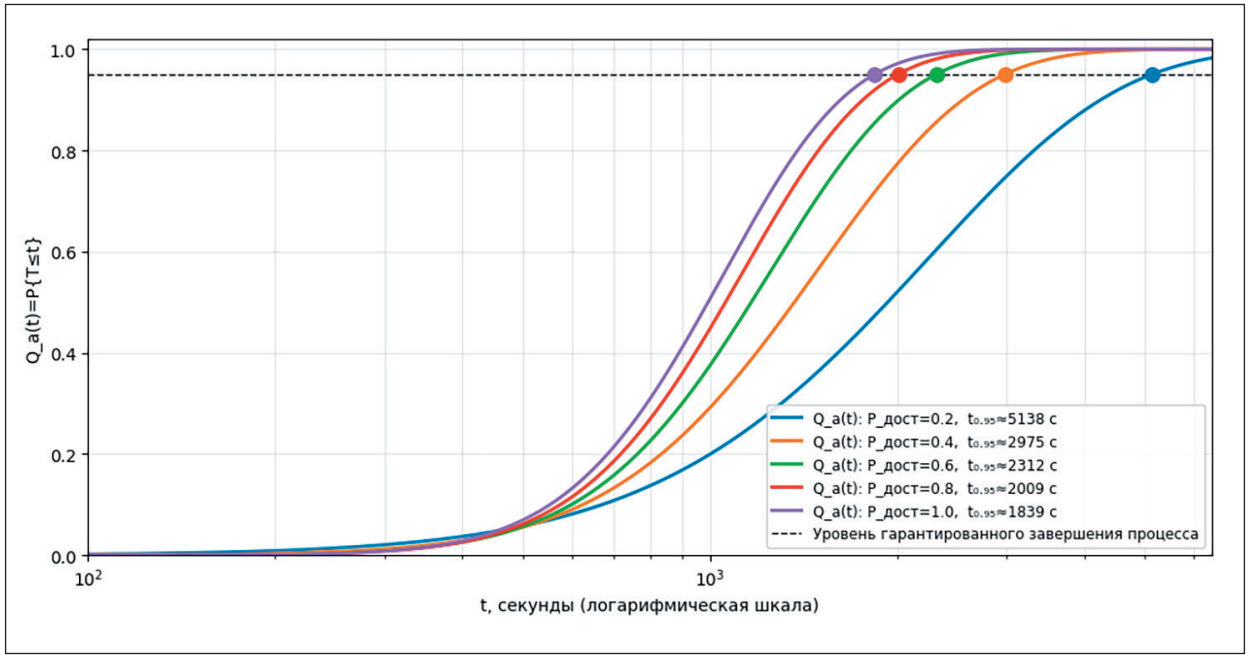

Рис. 8. Влияние вероятности доступности сети на функции распределения времени КР

временном окне с учетом вероятностного ожидания и повторяемости попыток; при низкой доступности становится рациональным минимизировать зависимость от мгновенного доступа, переносить акцент на подготовительные/пассивные стадии и организацию процесса как долговременного, поскольку именно ограничение по $P_{\text{дост}}$ начинает доминировать над временными затратами последующих процедур и фактически определяет достижимые сроки завершения.

Рекомендации по направлениям защиты от компьютерной разведки нарушителя

С учетом полученных зависимостей целесообразно выстраивать защиту как управляемое воздействие на параметры модели КР нарушителя, обеспечивающее сдвиг функции распределения $Q_a(t) = Pr\{T \le t\}$ вправо, и рост квантиля гарантированного завершения $t_{0,95}$ процесса разведки за счет целенаправленного уменьшения эффективной доступности $P_{\text{дост}}$, увеличения потерь времени на повторы/ожидание, а также снижения вероятностей успешного прохождения ключевых стадий P_i: корреляция, трассировка, задержанные измерения, пиринговая интеграция посредством сегментации, фильтрации и контроля плоскости управления. Показательные результаты такого воздействия приведены на рис. 9, где видно, что меры селективного доступа дают умеренный прирост $t_{0,95}$, тогда как меры, увеличивающие повторы к подключению, формируют выраженный правый хвост и существенно увеличивают гарантированное время завершения КР.

Кроме того, комбинированный режим дополнительно снижает успешность измерительных стадий, переводя нарушителя из режима короткого активного цикла в режим длительного, многократно повторяемого накопления попыток. Таким образом, практическая стратегия защиты должна сводиться к тому, чтобы для подозрительных источников и неавторизованных контуров:

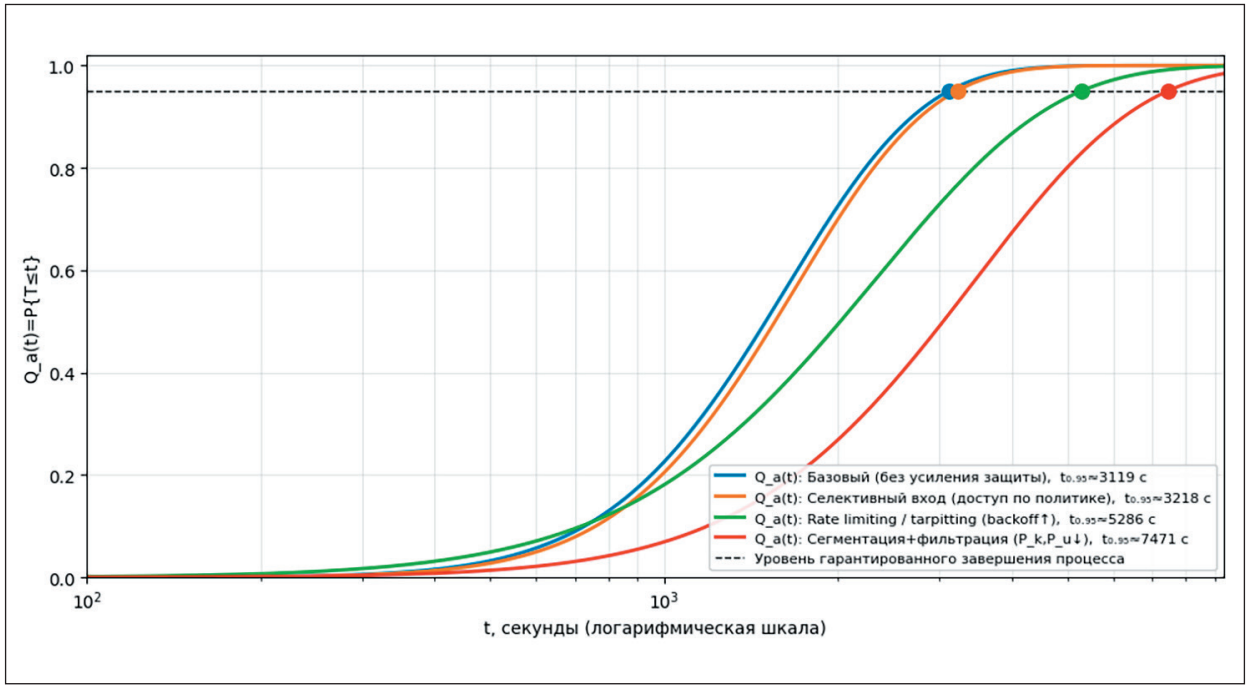

Рис. 9. Сдвиг функций распределения $Q_a(t)$ при применении мер защиты

1. Сделать вход в сеть селективным: обеспечить сохранение доступа для легитимных пользователей и доверенных узлов в штатном режиме, а для неавторизованных источников вероятность успешного установления сессии существенно снизить за счет политики безопасности, вследствие чего для нарушителя вход становится затруднительным.

2. Автоматически вводить и наращивать для подозрительных источников режим деградации доступа: лимитирование числа запросов, ограничения на число соединений, прогрессивные задержки и временные блокировки при многократных попытках, вследствие чего повторные обращения начинают сопровождаться возрастающими временными потерями.

3. Уменьшать результативность активных и задержанных стадий за счет микросегментации, закрытия межсегментных путей, минимизации экспонирования сервисов и защиты плоскости управления.

Заключение

В статье представлена стохастическая модель процесса анализа сетевой активности элементов телефонной IP-сети, выполняемого комплексом компьютерной разведки нарушителя, в которой ключевые процедуры сканирования (обнаружение активных элементов, определение ролей узлов, идентификация типов ОС, перечисление портов/сервисов и последующая корреляция с уязвимостями) описываются дугами с собственными распределениями времени и вероятностями успешного завершения, а повторные запуски при сбоях учитываются петлями возврата.

Для редуцированной структуры с параллельным узлом логического «И» получены явные выражения для функции распределе-

ния и плотности времени завершения, после чего выполнена инкапсуляция параллельного блока с использованием двухмоментной аппроксимации гамма-распределением, позволившая перейти к компактной эквивалентной функции всей подсети и на этой основе вычислять интегральную функцию распределения, математическое ожидание, дисперсию и квантили гарантированного завершения.

Показано, что временные показатели разведывательного цикла имеют выраженную нелинейную зависимость от вероятностей успеха ключевых операций: рост P_i приводит к кратному сокращению среднего времени и характерного срока завершения с эффектом насыщения в области высоких значений, а режимы полного и частичного сканирования формируют ожидаемый компромисс между быстротой и точностью собираемой компьютерной разведкой информации.

Практическая ценность предложенного подхода заключается в том, что модель задает прямую связь между режимами защиты телефонной IP-сети и вероятностно-временными характеристиками разведки нарушителя: через сдвиг $Q_a(t) = Pr\{T \leq t\}$ и рост $t_{0,95}$ можно производить обоснованный выбор мер борьбы, оценивая не только факт противодействия, но и его эффект по времени. При этом следует учитывать допущения базовой постановки. Дальнейшее развитие модели целесообразно направить на учет корреляций по общим ресурсам, нестационарность параметров при активном противодействии и калибровку распределений по данным мониторинга реальной сети, что повысит достоверность прогнозов и прикладную пригодность результатов для задач управления киберустойчивостью VoIP-сетей.

Список источников

1. Evaluating the Functioning Quality of Data Transmission Networks in the Context of Cyberattacks / A. Privalov, [et al.] // Energies. 2021. Vol. 14, no. 16. DOI: 10.3390/en14164755

2. Коцыняк М. А., Кулешов И. А., Лаута О. С. Устойчивость информационно-телекоммуникационных сетей. СПб.: Издательство Политехнического университета, 2013. 92 с.

3. Шелухин О. И. Причины самоподобия телетрафика и методы оценки показателя Херста // Электротехнические и информационные комплексы и системы. 2007. Т. 3, № 1. С. 5–14.

4. Назаров А. Н. Модели и методы расчета показателей качества функционирования узлового оборудования и структурно-сетевых параметров сетей связи следующего поколения. 2-е изд., перераб. Красноярск: Поликом, 2011. 491 с.

5. Привалов А. А., Титов Д. Д. Модель процесса работы узла коммутации технологической IP-сети при обслуживании приоритетного многопродуктового потока в условиях DDoS-атак нарушителя // Фундаментальные и прикладные научные исследования: сборник трудов X Международного конкурса научно-исследовательских работ. Уфа, 2022.

6. Привалов А. А., Титов Д. Д. Модель процесса передачи приоритетного многопродуктового потока по каналу телефонной IP-сети в условиях компьютерных атак // Инновационные научные исследования в современном мире: сборник трудов X Всерос. конкурса науч.-исслед. работ. Уфа, 2022.

7. Привалов А. А. Метод топологического преобразования стохастических сетей и его использование для анализа систем управления движением поездов // Известия Петербургского университета путей сообщения. СПб.: ПГУПС. 2017. Т. 14, № 1. С. 137–148.

8. Шибанов А. П. Нахождение плотности распределения времени исполнения GERT-сети на основе эквивалентных упрощающих преобразований // Автоматика и телемеханика. 2003. № 2. С. 117–126.

9. Духвалов А.П. Кибератаки на критически важные объекты — вероятная причина катастроф // Вопросы кибербезопасности. 2014. №3 (4). С. 50–53.

10. Scarfone K., Mell P., Brewer T. NIST SP 800-115: Technical Guide to Information Security Testing and Assessment. National Institute of Standards and Technology, 2008.

11. Мартин Дж. Системный анализ передачи данных. Т. 2. Проектирование систем передачи данных / под ред. В.С. Лапина. М.: Мир, 1975. 431 с.

Дата поступления: 30.01.2026
Решение о публикации: 10.04.2026

Контактная информация:
ПРИВАЛОВ Андрей Андреевич — доктор воен. наук, профессор кафедры «Электрическая связь»;
aprivalov@inbox.ru
ТИТОВ Даниил Дмитриевич — аспирант;
titovdd178@gmail.com

Model for Analyzing Network Activity of Elements in a Telephone IP Network Using an Intruder's Computer Reconnaissance System

A. A. Privalov[1, 3], D. D. Titov[1, 2]

[1] Emperor Alexander I Petersburg State Transport University, 9 Moskovsky ave., St. Petersburg, 190031, Russia

[2] Supertel OJSC, 38 Petrogradskaya emb., St. Petersburg, 197046, Russia

[3] National Guard Academy, 1 L. Pilyutova st., St. Petersburg, 198206, Russia

For citation: *Privalov A. A., Titov D. D.* Model for Analyzing Network Activity of Elements in a Telephone IP Network Using an Intruder's Computer Reconnaissance System // Proceedings of Petersburg State Transport University, 2026. Vol. 23, iss. 1. Pp. 516–530. DOI: 10.20295/1815-588X-2026-1-516-530 (In Russian)

Abstract

Objective: to develop and analyze a stochastic model of the process of analyzing the network activity of elements of a telephone IP network performed by an intruder's computer intelligence (CI) complex to quantify the time characteristics of the intelligence cycle. **Methods:** the network scanner's algorithm is presented as a stochastic network (GERT model), where the stages of detecting active elements, determining the roles of nodes, types of operating systems, ports/services, and analyzing vulnerabilities are described by arcs with their own time distribution functions and success probabilities, and repeated launches are represented by return loops. For the Role, OS, and Ports/Services branches, equivalent Laplace images of the distribution densities are obtained, based on which equivalent functions are derived for the parallel block and the full cycle of the scanner's operation in full and partial scan modes. The integral distribution function, average time, and level of requirements are calculated based on the obtained analytical expressions. **Results:** compact formulas for the equivalent function, distribution function, and average time of VoIP network intelligence are obtained, depending on the probabilities of successful completion of key operations. It is shown that the time characteristics of the process have a pronounced nonlinear dependence on the values of these probabilities: as the probabilities increase, the average time and the time required for successful completion of the scan decrease significantly. A comparison of full and

partial scan modes demonstrates the expected compromise between the completeness of the information obtained by computer intelligence and the speed of obtaining results. **Practical significance:** the model allows for predicting the time characteristics of the CI complex's operation in a VoIP network, identifying "bottlenecks", and quantifying the impact of network architecture and security measures on the speed at which an intruder can obtain critical information, providing a basis for making informed decisions to enhance cyber resilience.

Keywords: telephone IP network, computer intelligence complex, network scanner; network activity analysis, stochastic network, GERT model, equivalent function, full and partial scanning

References

1. Privalov A., et al. Evaluating the Functioning Quality of Data Transmission Networks in the Context of Cyberattacks, *Energies*, 2021, vol. 14, no. 16. DOI: 10.3390/en14164755

2. Kotsynyak M.A., Kuleshov I.A., Lauta O.S. Ustojchivost′ informatsionno-telekommunikatsionnykh setej [Stability of Information and Telecommunication Networks], Saint-Petersburg, *Izdatel'stvo Politekhnicheskogo universiteta [Polytechnic University Press]*, 2013, 92 p. (In Russian)

3. Shelukhin O.I. Prichiny samopodobiya teletrafika i metody otsenki pokazatelya Khersta [Causes of Self-Similarity in Teletraffic and Methods for Estimating the Hurst Exponent], *Elektrotekhnicheskie i informatsionnye kompleksy i sistemy [Electrical and Information Complexes and Systems]*, 2007, vol. 3, no. 1, pp. 5–14. (In Russian)

4. Nazarov A.N. Modeli i metody rascheta pokazatelej kachestva funktsionirovaniya uzlovogo oborudovaniya i strukturno-setevykh parametrov setej svyazi sleduyushchego pokoleniya [Models and Methods for Calculating the Quality Indicators of Node Equipment and the Structural and Network Parameters of Next-Generation Communication Networks], 2nd edit., Krasnoyarsk, *Polikom*, 2011, 491 p. (In Russian)

5. Privalov A.A., Titov D.D. Model′ protsessa raboty uzla kommutatsii tekhnologicheskoj IP-seti pri obsluzhivanii prioritetnogo mnogoproduktovogo potoka v usloviyakh DDoS-atak narushitelya [Model of the Process of the Technological IP Network Switching Node Operation When Servicing A Priority Multi-Product Flow under DDoS Attacks by the Intruder], *Fundamental'nye i prikladnye nauchnye issledovaniya: sb. trudov Kh Mezhdunarodnogo konkursa nauchno-issledovatel'skikh rabot [Fundamental and Applied Scientific Research: Proceedings of the 10th International Research Competition]*, Ufa, 2022. (In Russian)

6. Privalov A.A., Titov D.D. Model′ protsessa peredachi prioritetnogo mnogoproduktovogo potoka po kanalu telefonnoj IP-seti v usloviyakh komp′yuternykh atak [Model of the Process of Transmitting a Priority Multi-Product Stream over a Telephone IP Network in the Presence of Computer Attacks], *Innovatsionnye nauchnye issledovaniya v sovremennom mire: sb. Trud. Kh Vserossijskogo konkursa nauchno-issledovatel'skikh rabot [Innovative Scientific Research in the Modern World: Proceedings of the 10th All-Russian Competition of Research Papers]*, Ufa, 2022. (In Russian)

7. Privalov A.A. Metod topologicheskogo preobrazovaniya stokhasticheskikh setej i ego ispol′zovanie dlya analiza sistem upravleniya dvizheniem poezdov [Topological Transformation Method of Stochastic Networks and Its Application to the Analysis of Train Traffic Control Systems], *Izvestiya Peterburgskogo universiteta putej soobshcheniya [Proceedings of Petersburg State Transport University]*, Saint-Petersburg, 2017, vol. 14, no. 1, pp. 137–148. (In Russian)

8. Shibanov A.P. Nakhozhdenie plotnosti raspredeleniya vremeni ispolneniya GERT-seti na osnove ekvivalentnykh uproshchayushchikh preobrazovanij [Finding the Distribution Density of GERT Network Execution Time Based on Equivalent Simplifying Transformations], *Avtomatika i telemekhanika*

[Automation and Telemechanics], 2003, no. 2, pp. 117–126. (In Russian)

9. Dukhvalov A. P. Kiberataki na kriticheski vazhnye ob″ekty — veroyatnaya prichina katastrof [Cyberattacks on Critical Facilities Are a Likely Cause of Disasters], *Voprosy kiberbezopasnosti [Cybersecurity issues]*, 2014, no. 3 (4), pp. 50–53. (In Russian)

10. Scarfone K., Mell P., Brewer T. NIST SP 800-115: Technical Guide to Information Security Testing and Assessment, *National Institute of Standards and Technology*, 2008.

11. Martin Dzh. Sistemnyj analiz peredachi dannykh. T. 2. Proektirovanie sistem peredachi dannykh [System Analysis of Data Transmission. Vol. 2. Design of Data Transmission Systems], ed. V. S. Lapina, Moscow, *Izdatel'stvo "Mir" [Mir Publishers]*, 1975, 431 p.

Received: January 30, 2026
Accepted: April 10, 2026

Author's information:
Andrey A. PRIVALOV — Dr. Sci. of Military, Professor of the Department "Electrical Communications"; aprivalov@inbox.ru
aprivalov@inbox.ru
Daniil D. TITOV — Postgraduate Student; titovdd178@gmail.com