K. A. Shcheglov, Graduate Student, **A. Yu. Shcheglov,** Professor, e-mail: info@npp-itb.spb.ru,
St. Petersburg National research university of IT, Mechanics and Optics, Russia

The Reservation Methods Capabilities to Enhance Integral Information and Operational Security Level of Modern Informational Systems

We do research informational system elements reservation problem. We do illustrate the principal difference of setting the task for informational system elements reservation (to enhance functional reliability and informational security level). We identified and justified the fundamental contradictions of using reservation methods in informational security, which place limits on their effective practical usage while solving information security problems like enhancing confidential level, integrity and availability of information, including contradictions, which prevent effective solutions based on known reservation methods (in context of functional reliability and informational system security level enhancing problem). We do suggest the reservation method with dividing information between informational system elements, which allows to solve problem of enhancing integral information and operational security level and also define an assessment of its effectiveness.

Keywords: *informational system, reservation, reliability, resiliency, informational security, information accessibility, confidential information, information integrity, information operational security*

References

1. **Polovko A. M., Gurov S. V.** *Osnovy teorii nadezhnosti.* SPb.: BHV-Peterburg. 2006. 704 p.
2. **Bogatyrev V. A.** Nadezhnost' i jeffektivnost' rezervirovannyh komp'juternyh setej. *Informacionnye tehnologii.* 2006. N. 9. P. 25—30.
3. **Bogatyrev V. A., Bogatyrev S. V., Bogatyrev A. V.** Nadezhnost' klasternyh vychislitel'nyh sistem s dublirovannymi svjazjami serverov i ustrojstv hranenija. *Informacionnye tehnologii.* 2013. N. 2. P. 27—32.
4. **GOST** R 53114—2008. *Zashhita informacii. Obespechenie informacionnoj bezopasnosti v organizacii*, 2009.
5. **Shcheglov K. A., Shcheglov A. Ju.** Jekspluatacionnye harakteristiki riska narushenij bezopasnosti informacionnoi sistemy. *Nauchno-tehnicheskij vestnik informacionnyh tehnologij, mehaniki i optiki.* 2014. N. 1 (89). P. 129—139.
6. **Shcheglov K. A., Shcheglov A. Ju.** Matematicheskie modeli jekspluatacionnoj informacionnoj bezopasnosti. *Voprosy zashhity informacii.* 2014. Vyp. 106. N. 3. P. 52—65.

УДК 004.023

М. А. Перегудов, адъюнкт, e-mail: maxaperegudov@mail.ru,
А. А. Бойко, канд. техн. наук, доц., зам. нач. отдела, e-mail: algeminy@mail.ru,
Военный учебно-научный центр Военно-воздушных сил "Военно-воздушная академия имени профессора Н. Е. Жуковского и Ю. А. Гагарина" (г. Воронеж)

Оценка защищенности сети пакетной радиосвязи от имитации абонентских терминалов на уровне процедуры случайного множественного доступа к среде типа S-ALOHA

Предложена математическая модель, позволяющая оценить защищенность сети пакетной радиосвязи от деструктивных воздействий, направленных на имитацию абонентских терминалов на уровне процедуры случайного множественного доступа к среде типа S-ALOHA.

Ключевые слова: *сеть пакетной радиосвязи, S-ALOHA, деструктивное воздействие, марковская модель, защищенность*

Введение

Современные сети пакетной радиосвязи (СПР) нередко подвергаются деструктивным воздействиям [1], целью которых является нарушение конфиденциальности, целостности и доступности информации. Одним из основных способов деструктивных воздействий на СПР является имитация злоумышленником ложных соединений от имени абонентских терминалов (АТ).

На начальном этапе информационного взаимодействия установление соединения между АТ и средством коммутации и управления (СКУ) в СПР реализуется в процедуре случайного множественного

доступа к среде (далее — СМДС). Для таких современных стандартов связи, как GSM, TETRA, LTE, базовой процедурой, СМДС является S-ALOHA. Для СПР стандарта TETRA ряд потенциально возможных деструктивных воздействий, имитирующих АТ на уровне процедуры СМДС, приведена в работе [2]. Сегодня известны модели процедуры СМДС типа S-ALOHA [3—8], рассматривающие информационный конфликт между АТ и СКУ. Модели [3—7] позволяют оценить успешность доставки пакетов и стабильность функционирования процедуры СМДС типа S-ALOHA, а модель [8] наряду с успешностью доставки пакетов и стабильностью функционирования дополнительно определяет объем доступного временного ресурса канала множественного доступа и учитывает деструктивные воздействия, направленные на создание коллизий в канале множественного доступа, не предоставляя при этом возможности для оценки защищенности СПР от деструктивных воздействий, направленных на имитацию АТ на уровне процедуры СМДС типа S-ALOHA.

Цель работы — разработка математической модели, позволяющей оценить защищенность СПР от деструктивных воздействий, направленных на имитацию абонентских терминалов на уровне процедуры случайного множественного доступа к среде типа S-ALOHA.

Описательная модель процесса имитации АТ на уровне процедуры СМДС типа S-ALOHA

Функциональная схема процесса имитации АТ на уровне процедуры СМДС типа S-ALOHA показана на рис. 1.

В состав схемы входят N АТ, СКУ СПР и злоумышленник. Процедура СМДС реализует двустороннее взаимодействие между конкурирующими АТ и СКУ следующим образом. АТ по линии "вверх" осуществляют первичную (ПП) и вторичную (ВП) передачу пакетов с запросом на получение доступа к среде в любой дискретный временной интервал t ($t = 1, 2, ...$) продолжительностью τ (далее — временной слот) с вероятностями p_0 и p_r соответственно. СКУ по линии "вниз" широковещательно отправляет пакеты с рекомендуемыми для АТ значениями первичной p_0^* и вторичной p_r^* передачи пакетов. Одновременно в СПР $N - Y(t)$ АТ осуществляют первичную передачу пакетов и $Y(t)$ АТ — вторичную передачу. В один временной слот каждый АТ может передать один пакет. Передача считается успешной, если во временном слоте она инициирована только одним АТ. Иначе в канале СМДС возникает коллизия, и АТ, участвующие в создании коллизии, при неполучении пакета подтверждения успешной доставки через некоторое время отправляют вторичные пакеты повторно. До окончания времени ожидания от СКУ пакета подтверждения успешной доставки такие АТ не генерируют первичные пакеты и считаются блокированными [6].

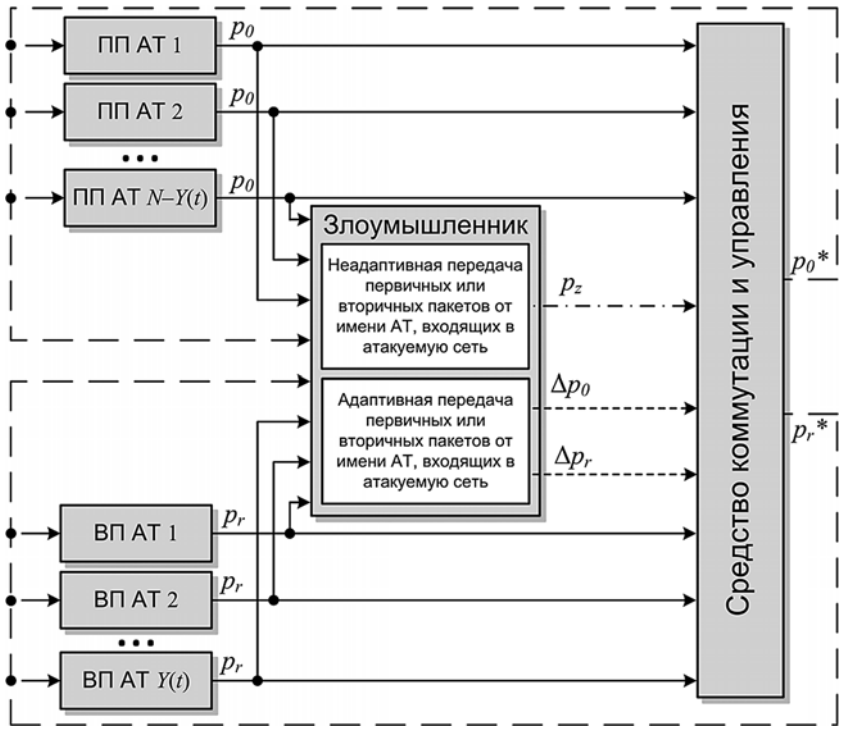

Рис. 1. Функциональная схема процесса имитации АТ СПР на уровне процедуры СМДС типа S-ALOHA

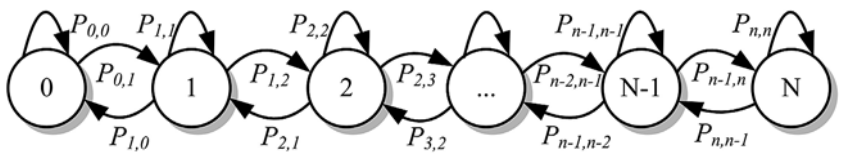

Рис. 2. Граф состояний марковской цепи, описывающей процесс имитации АТ СПР на уровне процедуры СМДС типа S-ALOHA

Злоумышленник в интересах имитации АТ, входящих в СПР, может реализовать в каждом временном слоте один из двух способов деструктивных воздействий. *Первый способ* реализуется неадаптивно (без анализа линии "вверх") и заключается в передаче по линии "вверх" с вероятностью p_z фальсифицированных пакетов от имени N — X АТ, участвующих в пер-

вичной передаче, и X АТ, участвующих во вторичной передаче. *Второй способ* деструктивных воздействий реализуется адаптивно (с анализом линии "вверх") и заключается в передаче по линии "вверх" с вероятностями Δp_0 и Δp_r фальсифицированных пакетов соответственно от имени $N - Y(t)$ АТ, участвующих в первичной передаче, и $Y(t)$ АТ, участвующих во вторичной передаче.

При успешной передаче злоумышленником пакетов от имени АТ СПР такие терминалы не получат подтверждения об успешной доставке пакетов, следующих за пакетами злоумышленника. При этом блокируются АТ СПР и их успешно доставленные пакеты. В противном случае успешно доставленные пакеты АТ СПР являются неблокированными.

Математическая модель процесса имитации АТ на уровне процедуры СМДС типа S-ALOHA

Для оценки защищенности СПР на уровне процедуры СМДС типа S-ALOHA (далее — СМДС) представим процесс имитации АТ в виде цепи Маркова с дискретными временем и состояниями, описывающей процесс гибели и размножения. Граф состояний такой цепи показан на рис. 2.

Модель включает $N + 1$ состояние. Номер состояния соответствует числу блокированных АТ в СПР. Рассматриваемая цепь Маркова описывается матрицей переходов $P = [p_{i,j}]$, где $i, j = 1, \ldots, N$. За один временной слот СПР в модели может переместиться на одно состояние назад (успешная передача АТ, входящим в СПР, вторичного пакета) или на одно состояние вперед (успешная передача злоумышленником первичного или вторичного пакета).

Пусть в текущем временном слоте S_1 — число одновременно переданных первичных пакетов АТ СПР; S_2 — число одновременно переданных вторичных пакетов этими АТ; Q_l — число переданных злоумышленником пакетов от имени АТ в зависимости от способа деструктивного воздействия и режима передачи АТ ($l = 1, 2$):

$$Q_l = \begin{cases} U_l, \text{ при первом способе;} \\ W_l, \text{ при втором способе,} \end{cases} \qquad (1)$$

где U_1 — число неадаптивно переданных злоумышленником пакетов от имени $N - X$ АТ, участвующих в первичной передаче; U_2 — число неадаптивно переданных злоумышленником пакетов от имени X АТ, участвующих во вторичной передаче; W_1 — число адаптивно переданных злоумышленником пакетов от имени $N - Y(t)$ АТ, участвующих в первичной передаче; W_2 — число адаптивно переданных злоумышленником пакетов от имени $Y(t)$ АТ, участвующих во вторичной передаче.

Тогда вероятность перехода $p_{i,j}$ имеет вид

$$p_{i,j} = \begin{cases} P_i^{S_1=0} P_i^{S_2=1} P_i^{Q_1=0} P_i^{Q_2=0}, \\ \text{если } (j = i-1) \wedge (i \neq 0); \\ P_i^{S_1=1} P_i^{S_2=0} P_i^{Q_1=0} P_i^{Q_2=0} + \\ + P_i^{S_1=1} P_i^{S_2=0} P_i^{Q_1=1} + \\ + P_i^{S_1=1} P_i^{S_2=0} P_i^{Q_2=1} + \\ + P_i^{S_1=1} P_i^{S_2=1} + P_i^{S_1=1} P_i^{S_2>1} + \\ + P_i^{S_1>1} + P_i^{S_1=0} P_i^{S_2>1} + \\ + P_i^{S_1=0} P_i^{S_2=0} P_i^{Q_1=0} P_i^{Q_2=0} + \\ + P_i^{S_1=0} P_i^{S_2=1} P_i^{Q_1=1} + \\ + P_i^{S_1=0} P_i^{S_2=1} P_i^{Q_2=1}, \text{ если } j = i; \\ P_i^{S_1=0} P_i^{S_2=0} P_i^{Q_1=1} + \\ + P_i^{S_1=0} P_i^{S_2=0} P_i^{Q_2=1}, \\ \text{если } (j = i+1) \wedge (i \neq N). \end{cases} \qquad (2)$$

где

$$P_i^{S_1=0} = [1-p_0]^{N-i};\ P_i^{S_1=1} = (N-i)p_0[1-p_0]^{N-i-1};$$

$$P_i^{S_1>1} = 1 - [1-p_0]^{N-i} - (N-i)p_0[1-p_0]^{N-i-1};$$

$$P_i^{S_2=0} = [1-p_r]^i;\ P_i^{S_2=1} = ip_r[1-p_r]^{i-1};$$

$$P_i^{S_2>1} = 1 - [1-p_r]^i - ip_r[1-p_r]^{i-1};$$

$$P_i^{Q_1=1} = \begin{cases} P_i^{U_1=1} \text{ при первом способе;} \\ P_i^{W_1=1} \text{ при втором способе;} \end{cases}$$

$$l = 1, 2;$$

$$P_i^{U_1=1} = p_z(N-X)N^{-1};$$

$$P_i^{W_1=1} = (N-i)\Delta p_0[1-\Delta p_0]^{N-i-1};$$

$$P_i^{U_2=1} = p_z X N^{-1};\ P_i^{W_2=1} = i\Delta p_r[1-\Delta p_r]^{i-1};$$

$$P_i^{Q_1=0} = \begin{cases} P_i^{U_1=0} \text{ при первом способе;} \\ P_i^{W_1=0} \text{ при втором способе;} \end{cases}$$

$$P_i^{U_1=0} = 1 - p_z(N-X)N^{-1};\ P_i^{W_1=0} = [1-\Delta p_0)]^{N-i};$$

$$P_i^{U_2=0} = 1 - p_z X N^{-1};\ P_i^{W_2=0} = [1-\Delta p_r]^i.$$

Для нахождения предельных вероятностей моделируемых состояний рассматриваемой цепи Маркова решается система линейных алгебраических уравнений [9]. Обобщенное решение такой системы имеет вид:

$$P_i = A_i\left(1 + \sum_{i=1}^{N} A_i\right)^{-1}, \qquad (3)$$

где

$$A_0 = 1;\ \forall i \in [1,\ N] A_i = \prod_{k=0}^{i} \frac{p_{k,\,k+1}}{p_{k+1,\,k}}.$$

Вышеизложенная математическая модель процесса имитации АТ на уровне процедуры СМДС отражает конкуренцию при доступе к каналу СМДС между АТ СПР и злоумышленником, влияющую:

- на успешность доставки неблокированных пакетов АТ СПР;
- на среднее число блокированных АТ СПР в каждом временном слоте.

Поэтому под защищенностью СПР от имитации АТ на уровне процедуры СМДС будем понимать вероятность успешной доставки неблокированных пакетов АТ СПР с учетом уровня блокированных АТ такой сети в каждом временном слоте. Показатель защищенности СПР от имитации АТ на уровне процедуры СМДС определяется следующим образом:

$$\Phi = P^{nsc}(1 - P^{blk}), \qquad (4)$$

где P^{nsc} — вероятность успешной доставки неблокированных пакетов АТ СПР; P^{blk} — вероятность блокирования злоумышленником АТ такой сети.

С использованием вероятностей состояний P_i и числа блокированных АТ СПР i в каждом моделируемом состоянии получим вероятность блокирования злоумышленником АТ на уровне процедуры СМДС P^{blk} в каждом временном слоте:

$$P^{blk} = N^{-1} \sum_{i=0}^{N} iP_i. \qquad (5)$$

При успешной доставке злоумышленником пакетов от имени АТ СПР с вероятностью P^{fsc} успешно доставленные пакеты АТ такой сети блокируются с такой же вероятностью. Тогда вероятность успешной доставки неблокированных пакетов АТ СПР P^{nsc} в каждом временном слоте имеет следующий вид:

$$P^{nsc} = \begin{cases} P^{sc} - P^{fsc}, \text{ если } P^{sc} - P^{fsc} > 0; \\ 0, \text{ если } P^{sc} - P^{fsc} \leqslant 0, \end{cases} \qquad (6)$$

где P^{sc} — вероятность успешной доставки пакетов АТ СПР.

Вероятности успешной доставки пакетов АТ СПР P^{sc} и успешной доставки злоумышленником пакетов от имени АТ такой сети P^{fsc} рассчитываются для каждого временного слота аналогично выражению (5):

$$P^{sc} = \sum_{i=0}^{N} P_i P_i^{sc};\ P^{fsc} = \sum_{i=0}^{N} P_i P_i^{fsc}, \qquad (7)$$

где P_i^{sc} — вероятность успешной доставки пакетов АТ СПР в каждом моделируемом состоянии i, а P_i^{fsc} — вероятность успешной доставки злоумышленником пакетов от имени АТ такой сети в состоянии i.

В соответствии с выражением (2) в каждом моделируемом состоянии i вероятность успешной доставки пакетов АТ СПР P_i^{sc} с учетом [3—7] и деструктивных воздействий, направленных на имитацию АТ процедуры СМДС типа S-ALOHA, вычисляется для каждого временного слота следующим образом:

$$P_i^{sc} = P_i^{S_1=1} P_i^{S_2=0} P_i^{Q_1=0} P_i^{Q_2=0} + P_i^{S_1=0} P_i^{S_2=1} P_i^{Q_1=0} P_i^{Q_2=0} =$$

$$= \begin{cases} ((N-i)p_0[1-p_0]^{N-i-1}[1-p_r]^i + \\ + [1-p_0]^{N-i} i p_r [1-p_r]^{i-1})(1-p_z(N-X)N^{-1}) \times \\ \times (1 - p_z X N^{-1}) \text{ при первом способе;} \\ ((N-i)p_0[1-p_0]^{N-i-1}[1-p_r]^i + \\ + [1-p_0]^{N-i} i p_r [1-p_r]^{i-1}) \times \\ \times [1-\Delta p_0]^{N-i}[1-\Delta p_r]^i \text{ при втором способе,} \end{cases} \qquad (8)$$

а вероятность успешной доставки злоумышленником пакетов от имени АТ такой сети

$$P_i^{fsc} = P_i^{S_1=0} P_i^{S_2=0} P_i^{Q_1=1} + P_i^{S_1=0} P_i^{S_2=0} P_i^{Q_2=1} =$$

$$= \begin{cases} [1-p_0]^{N-i}[1-p_r]^i p_z \text{ при первом способе;} \\ [1-p_0]^{N-i}[1-p_r]^i((N-i)\Delta p_0[1-\Delta p_0]^{N-i-1} + \\ + i\Delta p_r[1-\Delta p_r]^{i-1}) \text{ при втором способе.} \end{cases} \qquad (9)$$

Информационная технология оценки защищенности СПР от имитации АТ на уровне процедуры СМДС типа S-ALOHA

Информационная технология оценки защищенности СПР от имитации АТ на уровне процедуры СМДС типа S-ALOHA состоит в выполнении следующих шагов алгоритма, блок-схема которого представлена на рис. 3.

Шаг 1. Устанавливают интервал анализа линий "вверх", "вниз" канала СМДС СПР ΔT.

Шаг 2. Записывают в базу данных пакеты, передаваемые каждым АТ СПР по линии "вверх", и подтверждения об успешной доставке этих пакетов, передаваемые СКУ по линии "вниз", в течение интервала ΔT. Затем сопоставляют пакеты и подтверждения об успешной доставке этих пакетов. По результатам сопоставления определяют тип пакета: первичный или вторичный. Правила определения типа пакета следующие:

- передаваемый пакет, следующий за пакетом, на который АТ получил подтверждение об успешной его доставке, является первичным;
- передаваемый пакет, следующий за пакетом, на который АТ не получил подтверждение об успешной его доставке, является вторичным.

Так как для выполнения шага 4 требуются записанные в предыдущем интервале анализа ΔT первичные и вторичные пакеты, передаваемые каждым АТ СПР, то в целях непрерывной оценки защищенности СПР от имитации АТ на уровне процедуры СМДС дополнительно введем в алгоритм **шаг 3**, аналогичный шагу 2.

Шаг 4. Вычисляют среднее число первичных O и вторичных R пакетов, переданных АТ СПР:

$$O = N^{-1} \sum_{k=1}^{N} O_k;\ R = N^{-1} \sum_{k=1}^{N} R_k, \qquad (10)$$

где O_k — число первичных пакетов, переданных k-м АТ СПР; R_k — число вторичных пакетов, переданных k-м АТ такой сети; $k = 1, 2, ..., N$; N — общее число АТ СПР.

Число первичных O_k и вторичных R_k пакетов, переданных каждым АТ СПР, определяют путем суммирования в базе данных ячеек, соответствующих первичным или вторичным пакетам.

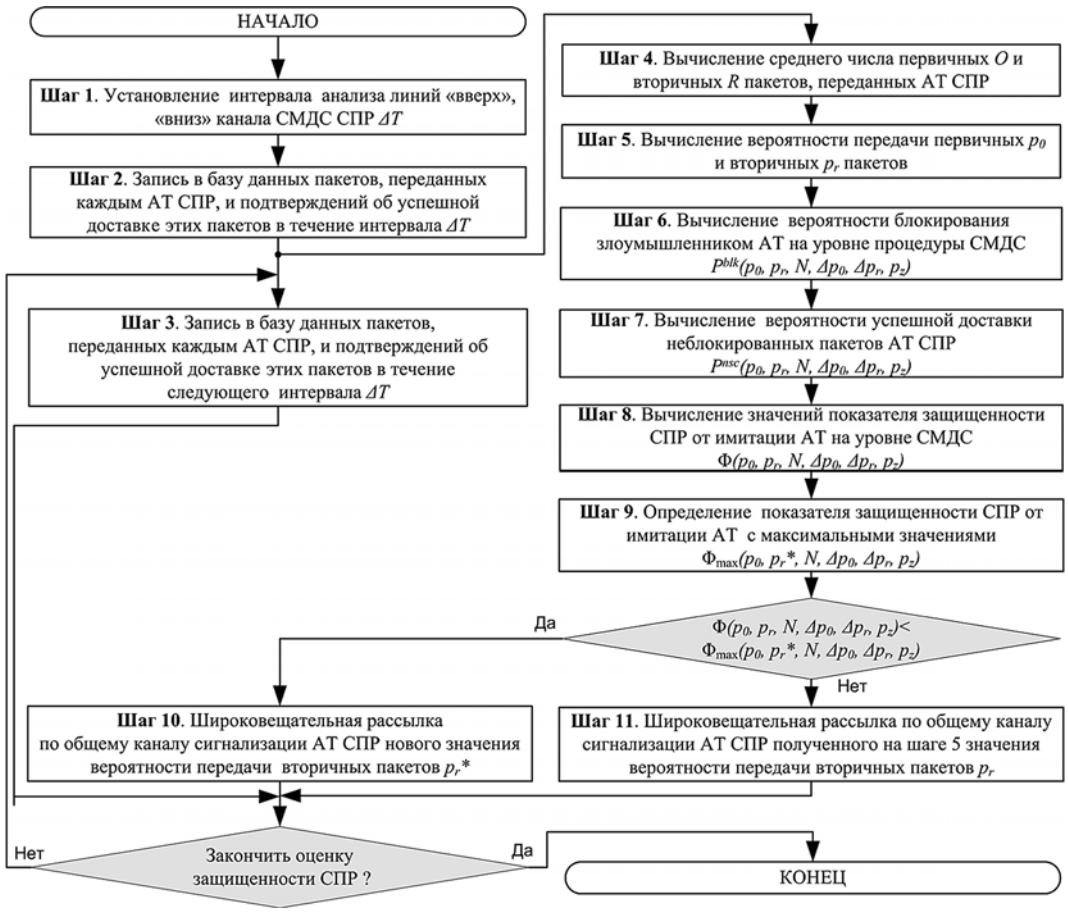

Рис. 3. Информационная технология оценки защищенности одноранговой СПР от имитации АТ на уровне процедуры СМДС типа S-ALOHA

Шаг 5. Определяют вероятности передачи первичных p_0 и вторичных p_r пакетов АТ СПР в каждом временном слоте t ($t = 1, 2, ...$) продолжительностью τ следующим образом:

$$p_0 = OM^{-1};\ p_r = RM^{-1};\ M = \Delta T\tau^{-1}, \qquad (11)$$

где M — число временных слотов продолжительностью τ в интервале анализа ΔT.

Шаги 6—8 выполняются на основании полученных значений p_0 и p_r.

Шаг 6. Вычисляют в каждом временном слоте с использованием аналитического выражения (5) значения вероятности блокирования злоумышленником АТ на уровне процедуры СМДС P^{blk} в точках, являющихся значениями вероятности передачи злоумышленником первичных Δp_0 или вторичных Δp_r пакетов от имени АТ СПР.

Шаг 7. Вычисляют по формулам (6)—(9) вероятность успешной доставки неблокированных пакетов АТ СПР P^{nsc} для каждого временного слота.

Шаг 8. Вычисляют по полученным значениям вероятностей блокирования АТ СПР P^{blk} и успешной доставки неблокированных пакетов АТ такой сети P^{nsc} с использованием выражения (4) значения показателя Ф защищенности СПР от имитации АТ на уровне СМДС типа S-ALOHA.

Шаг 9. Определяют показатель защищенности СПР от имитации АТ на уровне СМДС с максимальными значениями Φ_{max}, изменяя значения вероятности передачи вторичных пакетов p_r.

Если полученные значения на шаге 8 меньше максимальных значений показателя защищенности СПР от имитации АТ, то выполняют шаг 10, иначе — шаг 11.

Шаг 10. Рассылают широковещательно по общему каналу сигнализации СПР новое значение вероятности передачи вторичных пакетов p_r^*.

Шаг 11. Рассылают широковещательно по общему каналу сигнализации СПР полученное на шаге 5 значение вероятности передачи вторичных пакетов p_r.

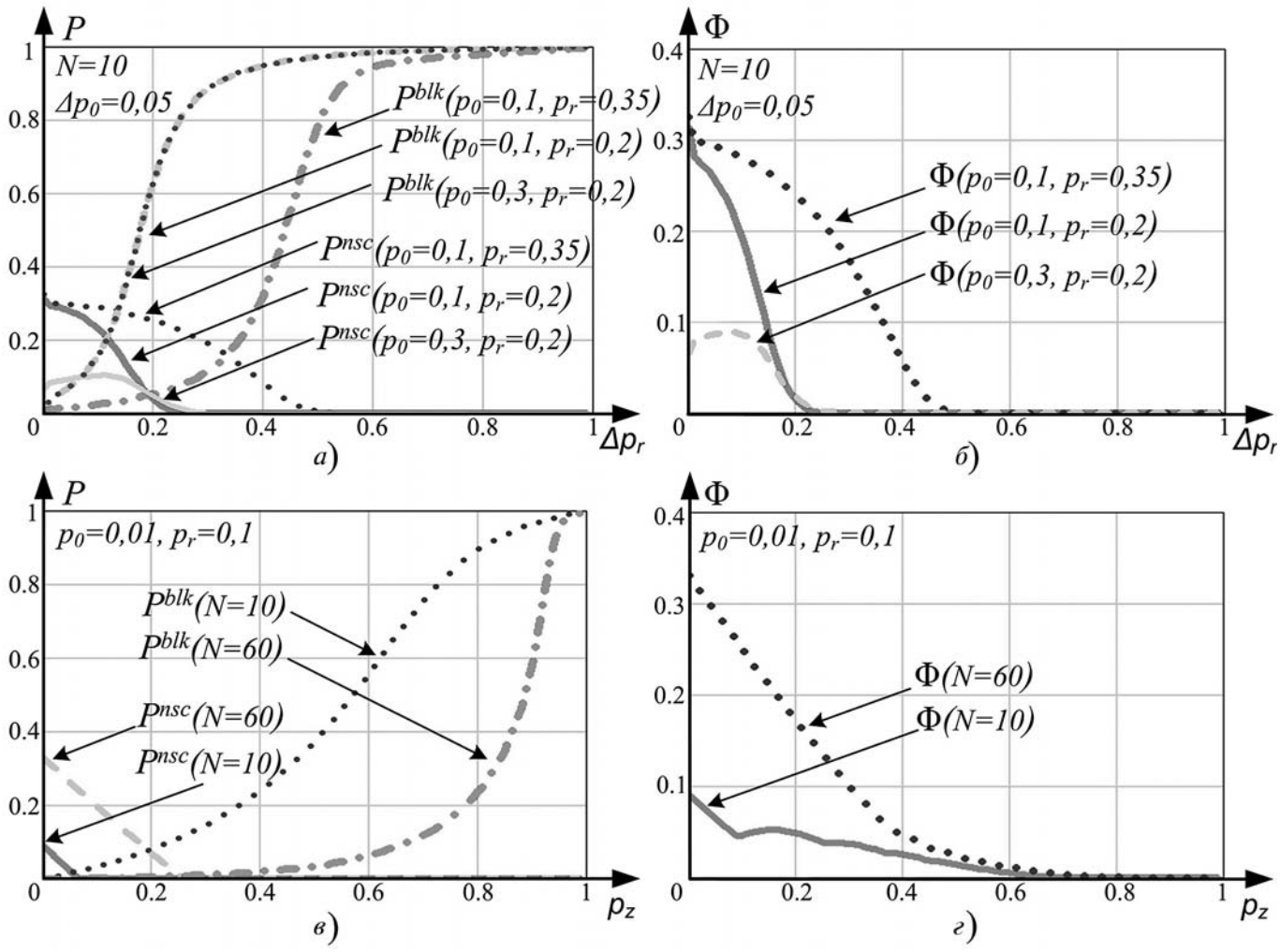

Рис. 4. Зависимости вероятностей успешной доставки неблокированных пакетов АТ СПР, блокирования АТ такой сети и показателя защищенности СПР от имитации АТ на уровне процедуры СМДС от параметров ДВ

Управлять значением вероятности передачи вторичных пакетов p_r, например, в транковых сетях стандарта TETRA, возможно путем изменения значения времени ожидания перед вторичными передачами и разрешенного числа вторичных передач, передаваемых в сообщениях ACCESS-DEFINE общего канала сигнализации, [2].

Предложенный алгоритм справедлив как для одноранговой СПР, так и для многоприоритетной сети с незначительными отличиями. Для многоприоритетной СПР в алгоритм добавляют шаг определения числа АТ каждого приоритета СПР. При этом шаги 4—11 выполняют для каждого приоритета такой сети. В шагах 10, 11 широковещательно рассылают не только вероятность передачи вторичных пакетов для каждого приоритета СПР, но и число АТ.

Результаты моделирования

Результаты моделирования процесса имитации АТ СПР на уровне процедуры СМДС типа S-ALOHA с параметрами управления поведением такой сети p_0, p_r, N и параметрами деструктивных воздействий Δp_0, Δp_r, p_z показаны на рис. 4.

Анализ рис. 4 позволяет сделать следующие выводы.

Во-первых, при увеличении вероятности передачи вторичных пакетов АТ СПР и числа АТ такой сети наблюдается уменьшение вероятности блокирования АТ СПР (рис. 4, *а*, *в*) и увеличение вероятности успешной доставки неблокированных пакетов АТ СПР (рис. 4, *а*, *в*), которые приводят к увеличению значения показателя защищенности СПР от имитации АТ на уровне процедуры СМДС (рис. 4, *б*, *г*).

Во-вторых, с ростом вероятности передачи первичных пакетов АТ СПР вероятность блокирования АТ такой сети не изменяется (рис. 4, *а*), а вероятность успешной доставки неблокированных пакетов АТ СПР уменьшается (рис. 4, *а*). В этих условиях на рис. 4, *б* наблюдается снижение значений показателя защищенности СПР от имитации АТ на уровне процедуры СМДС (рис. 4, *б*).

Для обеспечения защищенности СПР от имитации АТ на уровне процедуры СМДС типа S-ALOHA требуется выработка таких значений параметров управления поведением сети p_0, p_r и N, при которых будут созданы неблагоприятные условия для деструктивных воздействий, направленных на имитацию АТ СПР. В многоприоритетных сетях в целях повышения скорости доступа к каналу СМДС для АТ с наивысшим приоритетом снижают их число. С учетом результатов моделирования при уменьшении числа АТ с наивысшим приоритетом, объединенных в сегмент СПР, снижается защищенность такого сегмента. Поэтому наиболее уязвимыми будут АТ с наивысшим приоритетом.

Заключение

Таким образом, предложена модель, позволяющая проводить оценку защищенности сети пакетной радиосвязи от имитации абонентских терминалов на уровне процедуры случайного множественного доступа к среде типа S-ALOHA с использованием аналитических зависимостей, основывающихся на применении теории вероятностей, марковских процессов и определяющих вероятности успешной доставки неблокированных пакетов абонентских терминалов сети пакетной радиосвязи и блокирования этих терминалов.

Модель применима при проектировании многоприоритетных сетей пакетной радиосвязи, при разработке системы управления поведением таких сетей, включающей адаптивную защиту от имитации абонентских терминалов и алгоритмы процедуры случайного множественного доступа к среде типа S-ALOHA, разрешающие коллизии.

Список литературы

1. **Бойко А. А., Дьякова А. В.** Способ разработки тестовых удаленных информационно-технических воздействий на пространственно распределенные системы информационно-технических средств // Информационно-управляющие системы. 2014. № 3. С. 84—92.

2. **Перегудов М. А., Бойко А. А.** Об адаптивной защите транковых сетей связи стандарта TETRA от деструктивного программного воздействия // Техника средств связи: Научно-техн. сб. СПб.: Изд-во Политехн. ун-та, 2013. Вып. 2 (141). С. 218—221.

3. **Kleinrock L., Lam S. S.** On stability of packet switching in a random multiaccess broadcast channel // 7th Hawaii Int. Conf. on Syst. Sci.: Proc. Special Subconf. on Comput. Nets, Honolulu, Hawaii, Jan. 8—10, 1974. P. 73—77.

4. **Carleial A. B., Hellman M. E.** Bistable behavior of ALOHA-type systems // IEEE Trans. Commun. 1975. V. 23. P. 401—410.

5. **Onozato Y., Nogochi S.** On the thrashing cusp in slotted ALOHA systems // IEEE Trans. Commun. 1985. V. 33. P. 1171—1182.

6. **Abramson N.** The ALOHA system-another alternative for computer communications // Fall Joint Comput. Conf.: AFIPS Conf. Proc, Montvale, N. J., 1970. V. 37. P. 281—285.

7. **Kobayashi H., Onozato Y., Huynh D.** An approximate method for design and analysis of an ALOHA system // IEEE Trans. Commun. 1977. V. 25. P. 148—158.

8. **Перегудов М. А., Бойко А. А.** Модель процедуры случайного множественного доступа к среде типа S-ALOHA // Информационно-управляющие системы. 2014. № 6. С. 75—81.

9. **Таха Хемди А.** Введение в исследование операций. 7-е изд. М.: Издательский дом "Вильямс", 2005. 912 с.

M. A. Peregudov, Adjunct, e-mail: maxaperegudov@mail.ru,
A. A. Boyko, Associate Professor, e-mail: algemmy@mail.ru,
Military Education-Science Center of Military Air Forces "Professor N. E. Zhukovsky and Yu. A. Gagarin Military Air Academy", 394064,Voronezh, Russian Federation

Estimation of Security of a Network Packet Radio from Imitation of User's Terminals at Level of the Procedure of Random Multiple Access to the Environment Type S-ALOHA

Modern network packet radio are often subjected to destructive impact, one of the main ways which is to simulate user's terminals at the level of the procedure of random multiple access to the environment type S-ALOHA. Existing models procedure of random multiple access environment does not provide the ability to estimation of security of a network packet radio from imitation of users terminals at level of the procedure of random multiple access to the environment type S-ALOHA. The proposed model for assessment of the security of the network packet radio from imitation of user's terminals at the level of the procedure of random multiple access to the environment type S-ALOHA using analytical dependences, based on the application of probability theory, Markov processes and determining the probability of successful delivery unblocking packages user's terminals and determining the probability of blocking these terminals. Model can be applied in the design of many priority networks packet radio, at system engineering of management by behavior of such networks, including adaptive protection against imitation of user's terminals and algorithms of the procedure of random multiple access to the environment type S-ALOHA, resolving collisions.

Keywords: *network packet radio, S-ALOHA, destructive impact, Markov model, security*

References

1. **Boyko A. A., Djakova A. V.** Sposob razrabotki testovyh udalennyh informacionno-tehnicheskih vozdeistvij na prostranstvenno raspredelennye sistemy informacionno-tehnicheskih sredstv. *Informatsionno-upravliaiushchie sistemy*. 2014. N. 3. P. 84—92.

2. **Peregudov M. A., Boyko A. A.** Ob adaptivnoj zashhite trankovyh setej svjazi standarta TETRA ot destruktivnogo programmnogo vozdejstvija. *Tehnika sredstv svjazi: Nauchno-tehn. sb.* SPb.: Izd-vo Politehn. un-ta, 2013. Vyp. 2 (141). P. 218—221.

3. **Kleinrock L., Lam S. S**. On stability of packet switching in a random multiaccess broadcast channel. *7th Hawaii Int. Conf. on Syst. Sci.: Proc. Special Subconf. on Comput. Nets, Honolulu, Hawaii, Jan. 8—10.* 1974. P. 73—77.

4. **Carleial A. B., Hellman M. E.** Bistable behavior of ALOHA-type systems. *IEEE Trans. Commun*. 1975. V. 23. P. 401—410.

5. **Onozato Y., Nogochi S.** On the thrashing cusp in slotted ALOHA systems. *IEEE Trans. Commun*. 1985. V. 33. P. 1171—1182.

6. **Abramson N.** The ALOHA system-another alternative for computer communications. *Fall Joint Comput. Conf.: AFIPS Conf. Proc, Montvale, N. J*. 1970. V. 37. P. 281—285.

7. **Kobayashi H., Onozato Y., Huynh D.** An approximate method for design and analysis of an ALOHA system. *IEEE Trans. Commun*. 1977. V. 25. P. 148—158.

8. **Peregudov M. A., Boyko A. A.** Model' procedury sluchajnogo mnozhestvennogo dostupa к srede tipa S-ALOHA. *Informatsionno-upravliaiushchie sistemy*. 2014. N. 6.

9. **Taha Hemdi A.** *Vvedenie v issledovanie operacij*. 7-e izd. M.: Izdatel'skij dom "Vil'jams", 2005. 912 p.

Теоретический и прикладной научно-технический журнал

ПРОГРАММНАЯ ИНЖЕНЕРИЯ

ISSN 2220-3397

В журнале освещаются состояние и тенденции развития основных направлений индустрии программного обеспечения, связанных с проектированием, конструированием, архитектурой, обеспечением качества и сопровождением жизненного цикла программного обеспечения, а также рассматриваются достижения в области создания и эксплуатации прикладных программно-информационных систем во всех областях человеческой деятельности.

Журнал распространяется только по подписке.

Оформить подписку можно через подписные Агентства или непосредственно в редакции журнала.

Подписные индексы по каталогам:
«*Роспечать*» — **22765;** «*Пресса России*» — **39795**

107076, Москва, Стромынский пер., 4
Тел./факс: (499) 269-55-10
e-mail: prin@novtex.ru
http://novtex.ru/pi.html