УДК: 004.772 DOI: 10.53816/23061456_2021_11–12_93

АЛГОРИТМ ПРОАКТИВНОЙ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ ФАЙЛОВОГО ОБМЕНА ОТ СЕТЕВОЙ РАЗВЕДКИ

ALGORITHM FOR PROACTIVE PROTECTION OF FILE EXCHANGE INFORMATION SYSTEMS FROM NETWORK RECONNAISSANCE

Т.В. Лебедкина

T.V. Lebedkina

Краснодарское высшее военное училище им. С.М. Штеменко

Представлен алгоритм защиты на основе управления параметрами передачи данных со средствами сетевой разведки. Описана последовательность действий, поясняющая сущность разработанного алгоритма. Сделан вывод о том, что разработанный алгоритм устраняет некоторые из недостатков аналогов и обеспечивает более высокую защищенность информационных систем файлового обмена от сетевой разведки, за счет имитации канала связи с плохим качеством. Полученные результаты свидетельствую о том, что разработанный алгоритм повышает результативность защиты информационных систем файлового обмена снижением возможностей злоумышленника по подбору имен и паролей санкционированных клиентов, а также по компрометации и преодолению им средств защиты.
Ключевые слова: информационная система, сетевая разведка, сетевые соединения, протокол, компьютерная атака.

An protection algorithm based on control of data transmission parameters with network reconnaissance tools is presented. The workflow explaining the content of the developed algorithm is described. It is concluded that the developed algorithm eliminates some of the disadvantages of analogues and provides greater protection of file exchange information systems from network reconnaissance by simulating a communication channel with poor quality. The obtained results indicate that the developed algorithm increases the effectiveness of file exchange information systems protection by reducing the adversary's ability to pick up names and passwords of authorized clients, as well as to compromise the protection tools and overcome them.
Keywords: information system, network reconnaissance, network connections, protocol, computer attack.

Введение

Одним из направлений обеспечения информационной безопасности информационных систем, позволяющем предотвращать компьютерную атаку еще на этапе сетевой разведки (СР), является проактивная защита информационных систем [1–3]. Ее сущность, применительно к информационным системам файлового обмена (ИС ФО), заключается в активном противодействии компьютерным атакам, за счет предотвращения передачи данных злоумышленником на время, необходимое службе безопасности для реализации мер защиты.

Для взаимодействия с клиентами сервер выделяет необходимые ресурсы межпроцессного взаимодействия и ожидает запросы на открытие соединения (или запросы на предоставляемый сервис). В зависимости от типа информационного ресурса, сервер может обслуживать процессы в пределах одной информационной системы (ИС) или процессы на других ЭВМ через сети передачи данных. Формат запросов клиента и сервера определяется протоколом. Протокол передачи файлов (File Transfer Protocol — FTP), применяемый в ИС ФО — это стандартный механизм для копирования файла от одного хоста другим.

Основу передачи данных FTP составляет механизм установления соединения между соответствующими портами и выбора параметров передачи. Протокол FTP предназначен для передачи файлов по TCP/IP сетям. Протокол имеет «клиент-сервер» архитектуру и использует два TCP соединения для передачи команд и откликов между клиентом и сервером (управляющее соединение), и для передачи файлов между клиентом и сервером (соединение данных). В соответствии с [5], команды FTP передаются от клиента к серверу по управляющему соединению и состоят из 3 или 4 байт. FTP сервер отвечает откликом на каждую из полученных команд, который содержит трехзначный номер (передается как три числовых символа), за которым может следовать строка текста и представляет собой подтверждение (или отказ, содержащий сообщение с кодом временной или постоянной ошибки), передаваемое в форме строк от сервера к клиенту через управляющее соединение. Диалог между FTP клиентом и FTP сервером осуществляется поэтапно (команда – отклик – команда …). После завершения передачи файлов клиент может закрыть подключение или инициировать следующую передачу.

Алгоритм защиты информационных систем файлового обмена от сетевой разведки

Алгоритм относится к области информационной безопасности и может быть использован в системах обнаружения и предотвращения компьютерных атак с целью противодействия несанкционированным воздействиям на ИС ФО.

Недостатками известных алгоритмов являются:

– относительно узкая область применения, обусловленная разрывом соединения между сервером и СР, в случае обнаружения несанкционированных воздействий;

– относительно низкая результативность защиты, которая обусловлена тем, что противодействие несанкционированной авторизации злоумышленника осуществляется за счет его блокирования после заданного количества ошибок авторизации [6], что может привести к новым попыткам несанкционированного доступа злоумышленника уже с учетом полученной информации о системе защиты ИС ФО.

Все эти алгоритмы защиты являются реактивными, реагирующими на факт уже совершенного несанкционированного воздействия. Кроме того, применение таких алгоритмов противодействия ведет к компрометации применяемых средств защиты, что способствует их последующему обходу и изменению стратегии вредоносного воздействия злоумышленником.

В связи с этим, актуальность приобретают принципиально новые алгоритмы противодействия атакам злоумышленника на ИС ФО, реализуемые уже на раннем этапе [1–3, 7, 8]. Ими являются алгоритмы проактивной защиты, затрудняющей или делающей невозможным сбор идентификаторов пользователей ИС ФО, накладывающей ограничение на используемый злоумышленником вычислительный и временной ресурс без значительных вычислительных затрат со стороны защищаемой ИС ФО и предназначен для снижения качества обслуживания запросов СР.

Основная задача заключается в противодействии вредоносной активности за счет дискриминации трафика средств СР, снижением качества обслуживания клиентов, осуществляющих несанкционированное воздействие.

Показателем эффективности динамической конфигурации параметров соединений и передачи потоков данных ИС ФО является максимизация вероятности простоя СР $P_D^{NI} \to \max$:

$$< S, C, Z, I > \to \max P_D^{NI} \mid P_D^{NI} \in \left\{ P_i \right\},$$
$$i = 1, 2, \ldots, h.$$

Теоретическая основа алгоритма — теории систем управления, вероятности, массового обслуживания, исследования операций.

В качестве основных исходных данных в алгоритме выступают:

– множество внутренних параметров алгоритма

$$Z \subseteq \left\{ S_i, \Lambda_j \right\},$$

где $S_i = \{ S_1, \ldots, S_k \}$, $\Lambda_j = \{ \lambda_1, \lambda_2, \ldots, \lambda_j \}$ — перечень моделируемых состояний системы и интенсивностей потоков событий в ней;

– C — множество входных параметров, параметры соединения управления и передачи данных, $C \subseteq \left\{ I_{c\max}, t_{зад.}, d, g, f \right\}$;

– P_i — множество выходных параметров, значения финальных вероятностей состояний ИС ФО S,

$$P_i = \lim_{t \to \infty} P_i(t),$$

где $i = 1, 2, \ldots, h$, причем число состояний конечно и из каждого из них можно за конечное число шагов перейти в любое другое;

– I — множество параметров условий функционирования;

– $N \geq 1$ — база опорных идентификаторов, санкционированных клиентов ИС ФО;

– I_c — счетчик количества неудачных попыток авторизации средства СР для доступа к информационным ресурсам сервера ИС ФО;

– $I_{c\max}$ — максимально возможное количество неудачных попыток авторизации клиента ИС ФО для доступа к информационным ресурсам сервера ИС ФО;

– M — массив памяти для хранения опорных идентификаторов санкционированных клиентов ИС ФО;

– I_s — счетчик общего количества подключений всех клиентов ИС ФО;

– $I_{s\max}$ — максимально возможное количество подключений всех клиентов ИС ФО;

– T — общее количество сформированных значений времени задержки промежуточных откликов средству СР;

– R — общее количество промежуточных откликов, которые будут направлены средству СР перед ответным откликом;

– l — счетчик сформированных промежуточных откликов;

– G — общее количество сформированных фрагментов, на которые разделяют ответный отклик, направляемый средству СР;

– F — общее количество сформированных значений времени задержки направления фрагментов ответного отклика средству СР;

– m — счетчик сформированных фрагментов, на которые разделяют ответный отклик.

Реализация предлагаемого алгоритма проактивной защиты поясняется блок-схемой последовательности действий, представленной на рис. 1.

На начальном этапе задают исходные данные (блок 1), на следующем этапе (блок 2) устанавливают сетевые соединения клиентов с сервером ИС ФО. Алгоритмы проактивной защиты ИС, реализующие механизмы проактивной защиты на транспортном уровне на этапе установления сетевого соединения, предшествующие непосредственно файловому обмену на уровне приложений в процессе работы ИС ФО, которые также могут быть применимы для защиты серверов ИС ФО от несанкционированных воздействий, достаточно полно изложены в [4, 9, 10], в связи с чем в настоящей статье не рассматриваются.

После установления сетевого TCP соединения со средством СР (блок 2) направляют (блок 3) серверу ИС ФО команды с идентификаторами средства СР, принимают (блок 4) сервером ИС ФО команды с идентификаторами средства СР и выделяют (блок 5) из принятой команды идентификаторы средства СР, по результатам сравнения (блок 6), если выделенные идентификаторы средства СР не соответствуют опорным идентификаторам санкционированных клиентов ИС ФО из массива памяти M, формируют (блок 7) ответный отклик средству СР с ложным сообщением о временной ошибке. В ином случае формируется отчет и клиенту ИС ФО предоставляется (блок 24) доступ к информационным ресурсам сервера ИС ФО.

Затем формируют (блок 8) R промежуточных откликов, которые будут направлены средству СР перед ответным откликом с ложным сообщением о временной ошибке. После этого формируют (блок 9) T значений времени задержки промежуточных откликов средству СР. Затем считывают (блок 10) промежуточный отклик и время его задержки. Затем направляют (блок 11) средству СР первый из R сформированных промежуточных откликов через первое из T сформированных значений времени задержки.

После этого считывают (блок 12) значение счетчика l сформированных промежуточных от-

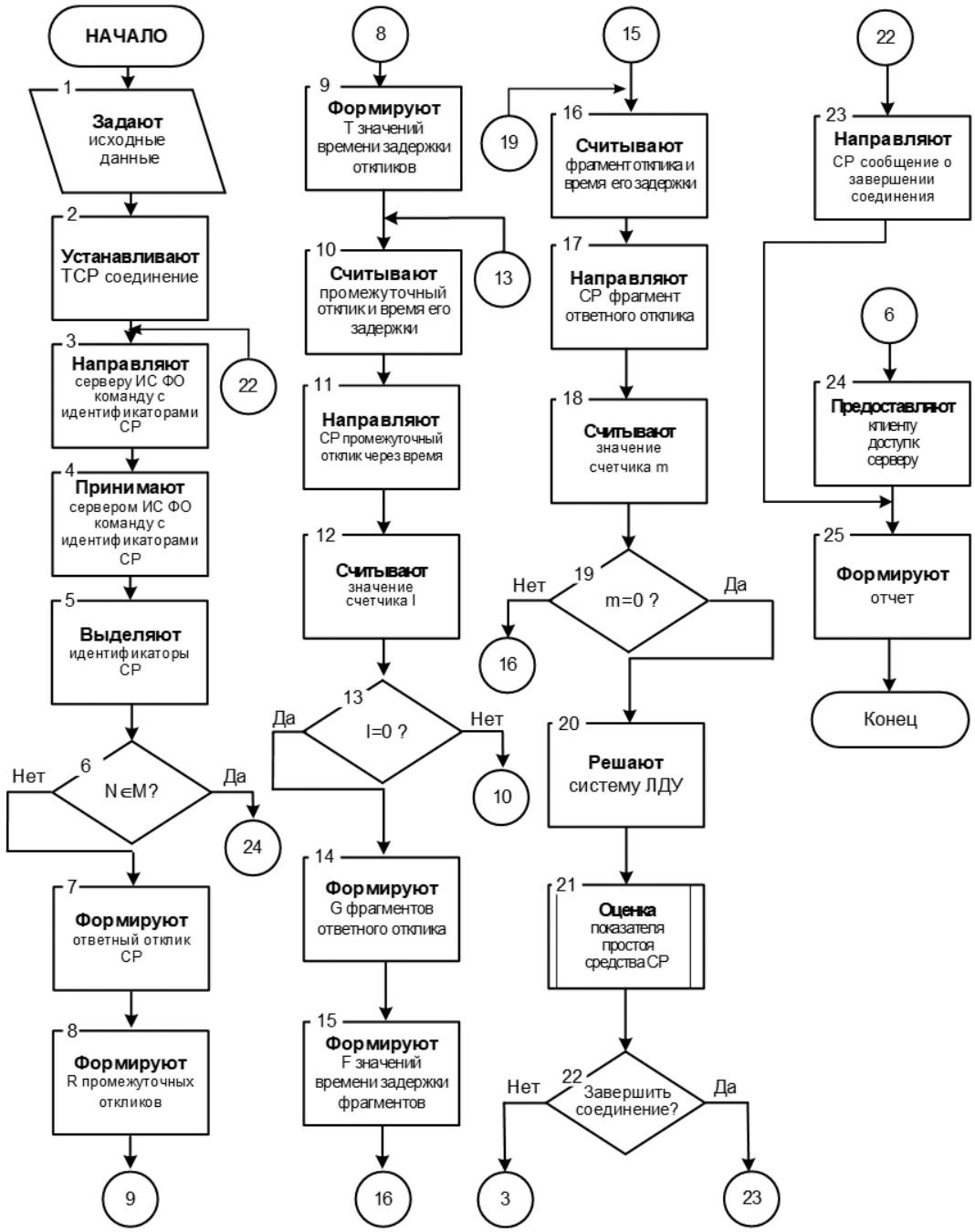

Рис. 1. Блок-схема последовательности действий, реализующая алгоритм проактивной защиты ИС ФО

кликов. Далее при невыполнении условия $l = 0$ считывают (блок 10) очередной из ранее сформированных R промежуточных откликов.

После этого направляют (блок 11) очередной из ранее сформированных R промежуточных откликов через значение времени задержки средству СР, и так до тех пор, пока не будет выполнено условие $l = 1$, указывающего на то, что все промежуточные отклики, кроме последнего, направлены средству СР. Затем для повышения результативности алгоритма, за счет снижения вероятности обнаружения злоумышленником факта использования средств защиты, применяют разбиение ответного отклика на фрагменты и направление этих фрагментов средству СР осуществляют через малые интервалы времени, чем достигают невозможность обхода средств защиты злоумышленником, за счет использования им

предварительно заданных коротких тайм-аутов ожидания ответного отклика. Для этого, после выполнения условия $l = 0$, формируют (блок 14) G фрагментов, на которые разделяют ответный отклик с ложным сообщением о временной ошибке, направляемый средству СР. Затем формируют (блок 15) F значений времени задержки для каждого из фрагментов, на которые разделяется ответный отклик средству СР. Затем считывают (блок 16) первый из G сформированных фрагментов ответного отклика и первое из F сформированных значений времени задержки. Далее направляют (блок 17) средству СР первый из G фрагментов ответного отклика через первое из Z сформированных значений времени задержки. Считывают (блок 18) значение счетчика m сформированных фрагментов ответного отклика. Этим обеспечивают учет отправленных фрагментов ответного отклика. В случае, если значение счетчика $m \neq 0$, то считывают (блок 16) очередной из ранее сформированных G фрагментов ответного отклика. После этого направляют (блок 17) очередной из ранее сформированных G фрагментов ответного отклика через значение времени задержки средству СР, и так до тех пор, пока не будет выполнено условие $m = 0$, означающее, что все фрагменты ответного отклика направлены средству СР, то есть он передан полностью.

В случае получения (блок 22) сервером ИС ФО после отправки ответного отклика команды от средства СР на завершение соединения, завершают сервером ИС ФО управляющее соединение для средства СР. После оценивания показателя простоя (блоки 20–21) средства СР формируют (блок 25) отчет. В ином случае вновь принимают от средства СР команду, проводят цикл выделения идентификаторов средства СР, его авторизации на сервере ИС ФО или при несовпадении выделенных идентификаторов средства СР с идентификаторами санкционированных клиентов ИС ФО цикл направления фрагментов ответного отклика с ложным сообщением о временной ошибке, через заданное время задержки этих фрагментов, после направления множества промежуточных откликов через заданное время их задержки.

Для оценивания простоя средства СР в разработанном алгоритме используется процесс функционирования ИС ФО. Моделируемая система S с течением времени меняет свое состояние (переходит из одного состояния в другое), возможные траектории перехода системы из состояния в состояние характеризуются ориентированным графом состояний моделируемой системы (рис. 2), с интерпретацией дискретных состояний S и интенсивностей потоков событий в ИС в условиях СР, приведенных в табл. 1. и табл. 2 соответственно.

Задавая численные значения интенсивностей λ в соответствии с условиями функционирования ИС ФО (ситуациями SIT), вектор вероятностей начальных состояний, учитывая нормировочное условие и переходя к непрерывному времени $t \to \infty$, систему линейных однородных дифференциальных уравнений (СЛОДУ) с постоянными коэффициентами решают численным методом.

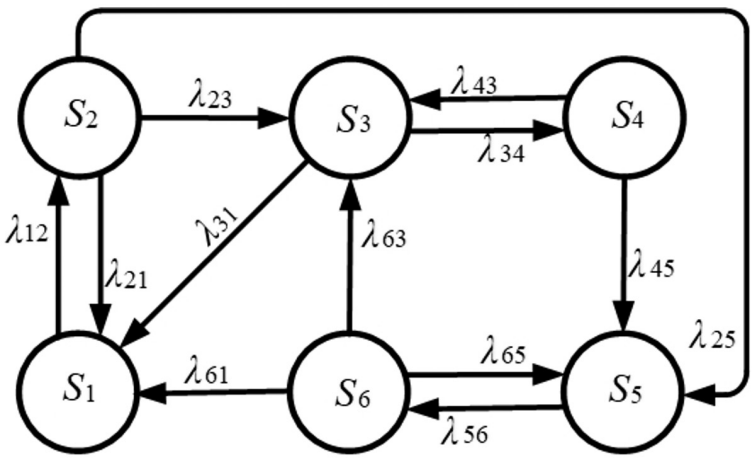

Рис. 2. Граф состояний функционирования ИС ФО

Таблица 1

Дискретные состояния ИС ФО в условиях СР

S_i	Состояния
S_1	Состояние, в котором ИС ФО находится в состоянии простоя, не принимает и не передает потоки данных
S_2	Состояние инициализации соединения средства СР (см. блоки 2–6 на рис. 1)
S_3	Состояние установления соединения средства СР и получения перед ответным откликом от сервера ИС ФО множества промежуточных откликов, направляемых через изменённые интервалы времени их задержки (ИС ФО находится в состоянии простоя, при превышении допустимого количества попыток неправильного ввода имени пользователя и пароля) (см. блоки 7–19 на рис. 1)
S_4	Состояние оценки значения показателя простоя (см. блоки 20–21 на рис. 1)
S_5	Состояние, в котором осуществляется передача и прием потоков данных между средством СР и ИС ФО (см. блоки 10, 12, 16, 18 на рис. 1)
S_6	Состояние подтверждения ИС ФО приема частей потока данных от средства СР (см. блоки 11, 17, 23 на рис. 1)

Таблица 2

Интенсивности потоков событий в ИС ФО в условиях СР

λ_{ij}	Описание потока событий
λ_{12}	Интенсивность потока событий на инициализацию (нового) соединения средством СР (см. блок 3 на рис. 1)
λ_{21}	Интенсивность потока событий на отказ в авторизации средства СР на сервере, в случае неправильного ввода имени и пароля (см. блоки 6, 23 на рис. 1)
λ_{23}	Интенсивность потока событий на увеличение времени получения средством СР ответного отклика от сервера в случае превышения попыток успешной авторизации (соединитель 6 на рис. 1)
λ_{25}	Интенсивность потока событий на передачу данных (после успешной авторизации) (см. блоки 4, 5, 24 на рис. 1)
λ_{31}	Интенсивность потока событий на разрыв соединения между средством СР и сервером в результате компрометации средств защиты (см. блок 22 на рис. 1)
λ_{34}	Интенсивность потока событий на оценку значения показателя простоя средства СР (см. блоки 20, 21 на рис. 1)
λ_{43}	Интенсивность потока событий на увеличение времени простоя средства СР (фрагментация ответного отклика, отправка промежуточных откликов, отправка ложного сообщения об ошибке) (см. блоки 7–19 на рис. 1)
λ_{45}	Интенсивность потока событий на передачу и прием потоков данных между средством СР и сервером после простоя средства СР (см. блоки 20–23 на рис. 1)
λ_{56}	Интенсивность потока событий на передачу средством СР очередной части потока данных для завершения передачи (см. блоки 10, 12, 16, 18 на рис. 1)
λ_{63}	Интенсивность потока событий на увеличение времени простоя средства СР после получения очередной части потока данных (см. блоки 7–19 на рис. 1)
λ_{65}	Интенсивность потока событий подтверждения сервером приема частей потока данных (квитирование) (см. блоки 11, 17, 23 на рис. 1)
λ_{61}	Интенсивность потока событий на закрытие канала управления (см. блок 23 на рис. 1)

$$\begin{cases} \frac{dp_1(t)}{dt} = \lambda_{21}p_2(t) + \lambda_{31}p_3(t) + \lambda_{61}p_6(t) - \lambda_{12}p_1(t), \\ \frac{dp_2(t)}{dt} = \lambda_{12}p_1(t) - (\lambda_{21} + \lambda_{23} + \lambda_{25})p_2(t), \\ \frac{dp_3(t)}{dt} = \lambda_{23}p_2(t) + \lambda_{43}p_4(t) + \lambda_{63}p_6(t) - \\ - (\lambda_{31} + \lambda_{34})p_3(t), \\ \frac{dp_4(t)}{dt} = \lambda_{34}p_3(t) - (\lambda_{43} + \lambda_{45})p_4(t), \\ \frac{dp_5(t)}{dt} = \lambda_{25}p_2(t) + \lambda_{45}p_4(t) + \lambda_{65}p_6(t) - \lambda_{56}p_5(t), \\ \frac{dp_6(t)}{dt} = \lambda_{56}p_5(t) - (\lambda_{61} + \lambda_{63} + \lambda_{65})p_6(t), \\ \sum_{i=1}^{6} p_i(t) = 1. \end{cases}$$

Здесь $p_i(t)$ — аргументы (вероятности нахождения системы в состоянии *i* в момент времени *t*); λ_{ij} — интенсивности потоков событий перехода из состояния *i* в состояние *j*.

В качестве численного метода решения СЛОДУ выбран классический метод четвертого порядка — метод Рунге-Кутта с фиксированным шагом интегрирования. Решение численным методом дает оценку не только финальных вероятностей, но и переходных процессов.

Оценим устойчивость системы к вариациям исходных данных, задавая граничные значения в стратегиях противодействующих сторон.

Ситуация SIT_1 — соединение клиентов с сервером осуществляется, без замедления передачи потока данных между клиентом и сервером ИС ФО (успешная авторизация) сервер, получая заявки на соединение от клиентов, выстраивает их в очередь и далее последовательно обрабатывает без задержки. Средства СР не обнаружены, система работает в штатном режиме. Поскольку в данном случае клиентам предоставляется доступ к информационным ресурсам сервера с минимизацией простоя работы ИСФО, то рассматривается, как влияют заявки λ_{12} — на установление соединения сервером и авторизацию клиента на сервере ИС ФО и λ_{25} — на передачу данных после успешной авторизации.

Ситуация SIT_2 — соединение клиентов с сервером осуществляется с замедлением передачи частей потока данных между клиентом и сервером ИС ФО, в этом случае соединение средства СР с сервером осуществляется следующим образом — сервер, получив значительное количество заявок на соединение от средства СР, имитирует канал связи с плохим качеством за счет направления клиенту, не прошедшему успешную авторизацию, фрагментированного ответного отклика с ложным сообщением о временной ошибке, фрагменты которого направляются через малые интервалы времени задержки, после множества промежуточных откликов. Поскольку в данном случае клиентам предоставляется доступ к информационным ресурсам сервера, с учетом простоя работы ИС ФО, то рассматривается, как влияют заявки λ_{12} — на авторизацию клиента на сервере ИС ФО и λ_{23} — на увеличение времени получения клиентом ответного отклика от сервера в случае превышения попыток успешной авторизации.

Производится расчет зависимости вероятностей состояний от времени для значений интенсивностей событий соответствующие ситуациям (SIT_1, SIT_2).

Для ситуации SIT_1 из графика (рис. 3) можно сделать вывод, что в начале ИС ФО находится в состоянии инициализации соединения с клиентами и в начале передачи данных. Вероятность $p_5(t)$ — передача и прием потоков данных между клиентом и сервером (открытие канала передачи данных) имеет максимальное значение 0,381.

Графики зависимостей вероятностей состояний исследуемого процесса для ситуации SIT_2 представлены на рис. 4. На графике видно, что на начальном этапе ИС ФО находится в переходном режиме функционирования, где наблюдается всплеск значений вероятности состояния $p_2(t)$, что соответствует нахождению ИС ФО в состоянии инициализации соединения с клиентами и средствами СР. Далее в ИС устанавливается стационарный режим и вероятность удержания несанкционированных клиентов в простое $p_3(t)$ принимает максимальное значение 0,304.

Научная новизна алгоритма заключается в применении математического аппарата теории марковских случайных процессов и решении уравнений Колмогорова, для динамического управления ресурсными возможностями средств СР при установлении и поддержании сетевых соединений ИС ФО в условиях СР.

Практическая значимость заключается в решении задачи динамической конфигурации па-

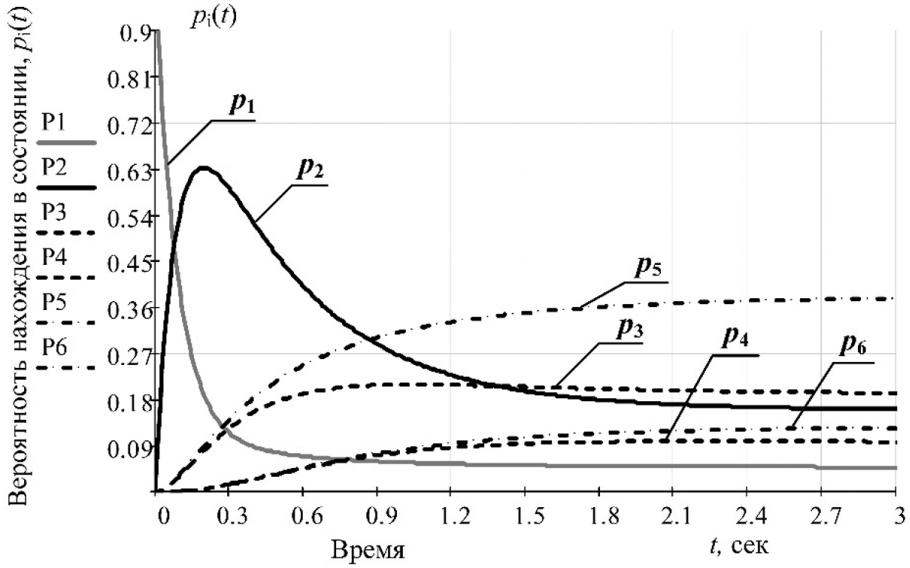

Рис. 3. Результаты расчета зависимости вероятностей состояний от времени для значений интенсивностей событий соответствующие ситуации SIT_1

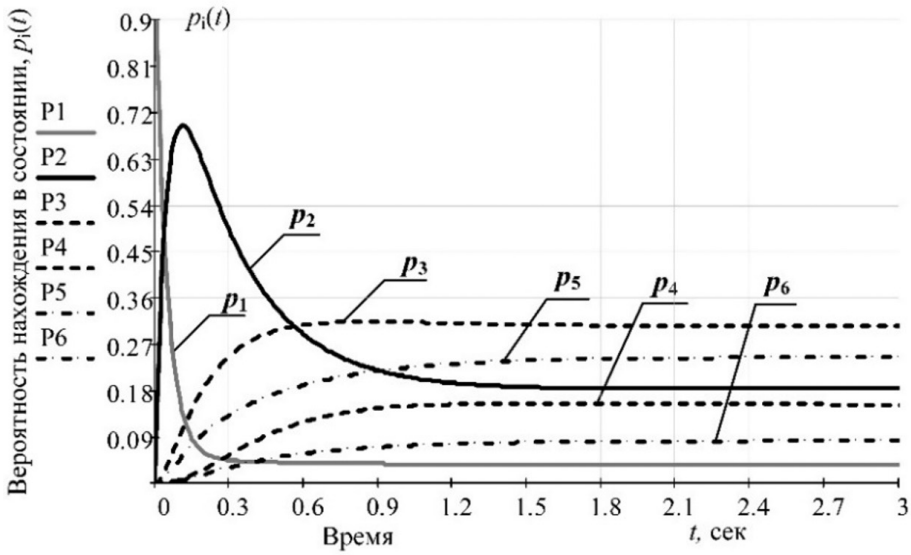

Рис. 4. Результаты расчета зависимости вероятностей состояний от времени для значений интенсивностей событий соответствующие ситуации SIT_2

раметров сетевых соединений ИС ФО, обеспечивающей дискриминацию трафика средств СР, скрытие факта использования средств защиты и идентификации их характеристик.

Вывод

Разработанный алгоритм позволяет повысить результативность защиты, по сравнению с аналогами, за счет снижения возможностей злоумышленника по подбору имен и паролей санкционированных клиентов ИС ФО. Это достигается имитацией канала связи с плохим качеством, обеспечивающей значительное увеличение времени для проведения атак с подбором пароля, за счет направления средству СР, фрагментированного ответного отклика с ложным сообщением о временной ошибке, фрагменты которого направляются через малые интервалы времени задержки, после множества промежуточных откликов. Снижение возможностей злоумышленника по компрометации средств

защиты вычислительных сетей и их обходу достигается за счет отсутствия блокирования соединений со средствами СР.

Литература

1. Соколовский С.П., Орехов Д.Н. Концептуализация проблемы проактивной защиты интегрированных информационных систем // Научные чтения имени профессора Н.Е. Жуковского: сб. научн. стат. VIII Междунар. науч. метод. конф. — Краснодар. 2018. С. 47–52.

2. Соколовский С.П., Гаврилов А.Л., Орехов Д.Н. Способы снижения информативности демаскирующих признаков средств проактивной защиты вычислительных сетей // Научные труды Кубанского государственного технологического университета. 2018. № 3. С. 211–220.

3. Горбачев А.А., Соколовский С.П., Усатиков С.В. Модель функционирования и алгоритм проактивной защиты сервиса электронной почты от сетевой разведки // Системы управления, связи и безопасности. 2021. № 3. С. 60–109. DOI: 10.24412/2410-9916-2021-3-60-109.

4. Максимов Р.В., Орехов Д.Н, Соколовский С.П. Модель и алгоритм функционирования клиент-серверной информационной системы в условиях сетевой разведки // Системы управления, связи и безопасности. 2019. № 4. С. 50–99.

5. Request for comments 959 [Электронный ресурс]. Режим доступа: https://tools.ietf.org/html/rfc959 (дата обращения: 22.07.2021).

6. Request for comments 2577 [Электронный ресурс]. Режим доступа: https://tools.ietf.org/html/rfc2577 (дата обращения: 24.07.2021).

7. Iskolnyy B.B., Maximov R.V., Sharifullin S.R. Survivability Assessment of Distributed Information and Telecommunication Networks // Selected Papers of the VIII All-Russian Conference with International Participation «Secure Information Technologies» (BIT 2017). Bauman Moscow Technical University. December 6–7, 2017. — Moscow, Russia. P. 59–65.

8. Maximov R.V., Ivanov I.I., Sharifullin S.R. Network Topology Masking in Distributed Information Systems // Selected Papers of the VIII All-Russian Conference with International Participation «Secure Information Technologies» (BIT 2017). Bauman Moscow Technical University. December 6-7, 2017. — Moscow, Russia. P. 83–87.

References

1. Sokolovsky S.P., Orehov D.N. Conceptualization of the problem of proactive protection of integrated information systems // Scientific readings named after Professor N.E. Zhukovsky: sat. stat. VIII International Scientific Journal. method. conf. — Krosnadar. 2018. P. 47–52.

2. Sokolovskij S.P., Gavrilov A.L., Orehov D.N. Ways to reduce the information content of unmasking features of proactive protection means for computer networks // Scientific works of the Kuban State Technological University. 2018. № 3. P. 211–220.

3. Gorbachev A.A., Sokolovskij S.P., Usatikov S.V. Functioning model and algorithm for proactive protection of the e-mail service from network intelligence // Control, communication and security systems. 2021. № 3. P. 60–109. DOI: 10.24412/2410-9916-2021-3-60-109.

4. Maximov R.V., Orehov D.N., Sokolovskij S.P. Model and algorithm of functioning of the client-server information system in the conditions of network intelligence // Control, communication and security systems. 2019. № 4. P. 50–99.

5. Request for comments 959 [Electronic resource]. Access mode: https://tools.ietf.org/html/rfc959.

6. Request for comments 2577 [Electronic resource]. Access mode: https://tools.ietf.org/html/rfc2577.

7. Iskolnyy B.B., Maximov R.V., Sharifullin S.R. Survivability Assessment of Distributed Information and Telecommunication Networks. Selected Papers of the VIII All-Russian Conference with International Participation «Secure Information Technologies». — Moscow. 2017. P. 59–65.

8. Maximov R.V., Ivanov I.I., Sharifullin S.R. Network Topology Masking in Distributed Information Systems. Selected Papers of the VIII All-Russian Conference with International Participation «Secure Information Technologies». — Moscow. 2017. P. 83–87.