МОДЕЛЬ ФУНКЦИОНИРОВАНИЯ ЗАЩИЩЕННОЙ ТЕХНОЛОГИИ ФАЙЛОВОГО ОБМЕНА

Лебедкина Т.В.[1], Соколовский С.П.[2]

Цель исследования: *разработка модели, позволяющей оценить защищенность информационной системы файлового обмена, обеспечить оперативность обслуживания максимального количества запросов санкционированных клиентов с одновременным снижением качества обслуживания запросов от средств злоумышленника.*

Используемые методы: *формализация сервисных процессов в виде марковских случайных процессов, а также численные методы.*

Результат исследования: *разработана критериальная оценочная база эффективности функционирования информационной системы файлового обмена. Решена задача динамического управления ресурсными возможностями информационной системы файлового обмена за счет управления параметрами передачи данных. Проведена оценка асимптотической устойчивости и робастности модели относительно возмущений значений исходных параметров с целью повышения адекватности модели при выборе режимов управления процессом передачи данных. Получены вероятностные и временные характеристики процесса функционирования информационной системы файлового обмена в условиях несанкционированных воздействий при различных ситуациях взаимодействия сторон конфликта, а также при управлении вычислительным и временным ресурсом средств сетевой разведки злоумышленника. Обоснованы оптимальные режимы функционирования информационной системы файлового обмена, обеспечивающие ее соответствие установленным требованиям безопасности объектов критической информационной инфраструктуры.*

Ключевые слова: *сетевая разведка, сетевые соединения, марковский случайный процесс, асимптотическая устойчивость, робастность.*

DOI:10.21681/2311-3456-2021-5-52-62

Введение

Широкое использование средств информатизации во всех сферах деятельности общества вызвало асимметричное увеличение количества деструктивных воздействий на все составляющие информационной инфраструктуры [1]. Система информационного взаимодействия в любых условиях обстановки должна организовывать своевременный, достоверный и безопасный обмен данными. Процессы информационного обмена внутри сети передачи данных (СПД), включают в себя активное использование информационных систем файлового обмена (ИС ФО) ведомственного назначения на всех уровнях иерархии. В настоящее время информационные потоки формируются через сети связи общего пользования (ССОП) с использованием протоколов информационного взаимодействия, что требует наличия адресной информации в передаваемых пакетах сообщений. В связи с этим существенно возрастают возможности сетевой разведки (СР), по вскрытию состава, структуры и алгоритмов функционирования ИС ФО [2]. В ведомственных ИС ФО безопасность и защита информационного взаимодействия реализуется как набор мер и рекомендаций регуляторов[3,4,5]. В значимых информационных системах объектами, подлежащими защите от угроз безопасности информации[6], являются их архитектура и конфигурация. В ИС ФО должны применяться специально созданные (эмулированные) ложные компоненты или создаваться ложные информационные системы, выступающие в качестве целей для злоумышленника при реализации им компьютерных атак и предназначенные как для обнаружения, регистрации и анализа действий злоумышленника в процессе реализации угроз безопасности информации, так и для предупреждения его вредоносных воздействий. Однако организация защиты ИС ФО с применением традиционных средств защиты, основанных на реализации запрещающих регламентов и дистанцировании со злоумышленником, вынуждают его и далее продолжать или менять стратегию деструктивных воздействий

1 Лебедкина Татьяна Владимировна, преподаватель кафедры защищенных информационных технологий Краснодарского высшего военного орденов Жукова и Октябрьской Революции Краснознаменное училища имени генерала армии С.М. Штеменко, г. Краснодар, Россия. E-mail: alina010570@mail.ru

2 Соколовский Сергей Петрович, кандидат технических наук, доцент Краснодарского высшего военного орденов Жукова и Октябрьской Революции Краснознаменное училища имени генерала армии С.М. Штеменко, г. Краснодар, Россия. E-mail: mtd.krd@mail.ru

3 Приказ ФСТЭК от 15.02.2017 г. № 27

4 Методический документ ФСТЭК «Меры защиты информации в государственных информационных системах» от 11.02.2014 г.

5 Приказ ФСТЭК от 25.12.2017 г. № 239

6 Банк данных угроз безопасности информации ФСТЭК России. URL: https://bdu.fstec.ru/threat

на ИС ФО, что в итоге может привести к исчерпанию ресурса системы защиты и достижению злоумышленником поставленных целей.

Проведенный анализ публикаций в области противодействия сетевой разведке [3-17] показал, что в настоящее время вопросам поиска и разработки новых технических и методических решений по защите ИС ФО от сетевой разведки уделяется недостаточно внимания, что обуславливает актуальность проводимого исследования.

Формализованная постановка задачи на моделирование информационной системы файлового обмена

ИС ФО представляет собой инфокоммуникационную систему, включающую совокупность клиентов, серверов и коммуникационного оборудования, соединенного физическими линиями связи. В процессе функционирования ИС ФО, имеющей в своем составе сервер, инициатор соединения (клиент) формирует запросы к серверу, который обрабатывает их в условиях ограниченного вычислительного ресурса. Ограниченность вычислительного ресурса выражается в том, что сервер способен обработать ограниченное количество пакетов данных за единицу времени при выполнении требований к его доступности для санкционированных клиентов.

Для этого необходимо решать задачу балансировки заявок на обслуживание, что усугубляется воздействием как помех и сбоев, вызванных влиянием на клиентов, сервер и каналы связи, так и деструктивными воздействиями злоумышленников.

Для передачи информации между клиентами и серверами в ИС ФО посредством протоколов взаимодействия устанавливают логическое соединение, под которым понимают инициализацию запросов на обслуживание от клиента к серверу, получение параметров соединения и поддержание соединения между клиентом и сервером до его окончания [3]. Основные услуги по пересылке файлов в ИС ФО обеспечиваются протоколом *FTP* (*File Transfer Protocol*), определенным в *RFC* 959. Схема установления сетевого соединения и использования *FTP* для извлечения списка элементов директории представлена на рис.1.

Содержательная постановка задачи на моделирование функционирования ИС ФО: разработать модель μ ИС ФО S, устанавливающую закономерность изменения множества P_i выходных параметров модели функционирования ИС ФО и множества Q показателей эффективности функционирования ИС ФО от множества C значений входных параметров, множества Z значений внутренних параметров, множества I значений параметров условий функционирования. На значения параметров множеств C, P_i, Z, I наложены условия их допустимости.

Математическая постановка задачи на моделирование функционирования ИС ФО:

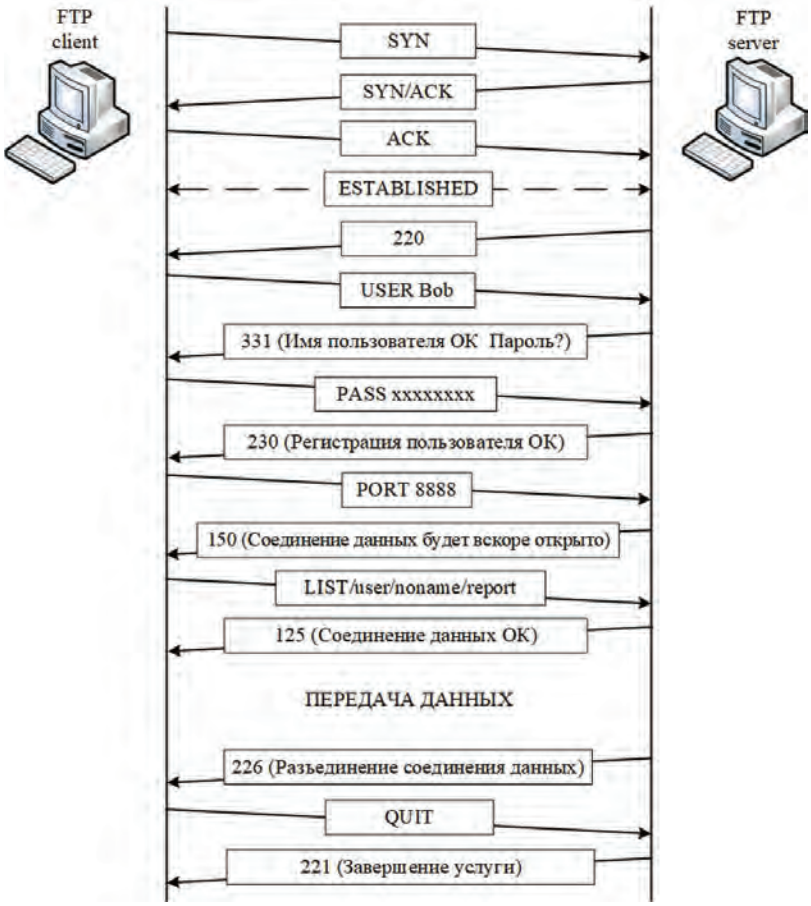

Рис. 1. Схема использования FTP для извлечения списка элементов директории

DOI:10.21681/2311-3456-2021-5-52-62

$$\mu : < S, C, Z, I > \to P_i,$$
$$Q \mid C \subseteq \{ I_{c\max}, t_{зад}, d, g, f \}, \quad (3)$$
$$P_i = \lim_{t \to \infty} P_i(t), \quad I \subseteq \{ FTP / FTP - DATA \}.$$

Формализованная постановка задачи на оптимизацию показателей эффективности ИС ФО:

$$< S, C, Z, I > \to \min P_D^C \mid P_D^C \in \{ P_i \}, i = 1, 2, \ldots, h \quad (4)$$

для минимизации вероятности простоя клиента и сервера;

$$< S, C, Z, I > \to \max P_D^{NI} \mid P_D^{NI} \in \{ P_i \}, i = 1, 2, \ldots, h \quad (5)$$

для максимизации вероятности простоя средства СР.

Модель функционирования информационной системы файлового обмена

Пусть имеется узел ИС ФО – сервер, обеспечивающий функционирование системы S, в том числе и в части системы контроля (оценки) значения показателя простоя. 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 (рис. 2).

Дискретные состояния процесса функционирования ИС ФО следующие: S_1 – состояние, в котором ИС ФО находится в состоянии простоя, не принимает и не передает потоки данных; S_2 – состояние инициализации соединения клиентом, открытие канала управления, авторизация клиентов на FTP сервере; S_3 – состояние установления сетевого соединения и получение клиентом перед ответным откликом от FTP сервера множества промежуточных откликов через заданные интервалы времени их задержки, направления клиенту фрагментированного ответного отклика, направления ложного ответного отклика с сообщением о временной недоступности сервера (ИС ФО находится в состоянии простоя, при превышении допустимого количества попыток авторизации); S_4 – состояние оценки значения показателя простоя ИС ФО; S_5 – состояние, в котором осуществляется передача и прием потоков данных между клиентом и сервером; S_6 – состояние подтверждения сервером приема частей потока данных (квитирование).

Интенсивности потоков событий – заявок, вызывающих переход системы из состояния, имеют следующую интерпретацию: λ_{12} – интенсивность потока событий на авторизацию клиента на сервере ИС ФО; λ_{21} – интенсивность потока событий на отказ в авторизации клиента на сервере, в случае неправильного ввода имени и пароля; λ_{23} – интенсивность потока событий на увеличение времени получения клиентом ответного отклика от сервера в случае превышения количества попыток неудачной авторизации; λ_{25} – интенсивность потока событий на передачу данных (после успешной авторизации); λ_{31} – интенсивность потока событий на разрыв соединения между клиентом и сервером в результате превышения времени ожидания ответного отклика; λ_{34} – интенсивность потока событий на оценку значения показателя простоя клиента; λ_{43} – интенсивность потока событий на увеличение времени простоя клиента (фрагментация ответного отклика, отправка промежуточных откликов, отправка ложного сообщения об ошибке); λ_{45} – интенсивность потока событий на передачу и прием потоков данных между клиентом и сервером после простоя клиента; λ_{56} – интенсивность потока событий на передачу клиентом очередной части потока данных; λ_{63} – интенсивность потока событий на увеличение времени простоя клиента после получения очередной части потока данных; λ_{65} – интенсивность потока событий на подтверждения сервером приема частей потока данных (квитирование); λ_{61} – интенсивность потока событий на закрытие канала управления.

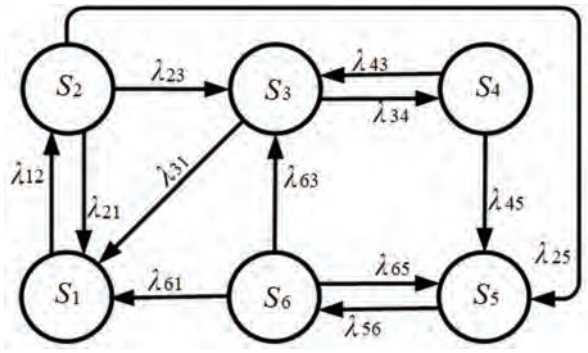

Рис. 2. Граф состояний функционирования ИС ФО

Моменты возможных переходов ИС ФО из состояния в состояние неопределенны, случайны и происходят под действием потоков событий, характеризующиеся их интенсивностями λ, являющимися важной характеристикой потоков событий и характеризующими среднее число событий, приходящееся на единицу времени[7],[8].

Пусть S_1 – начальное состояние моделируемой ИС ФО, в котором она не принимает и не передает потоки данных, то есть состояние покоя, в этом случае сервер, как и клиент находятся в состоянии простоя. После направления клиентом файловому серверу потока заявок на инициализацию соединения с интенсивностью λ_{12} система переходит из состояния S_1 в состояние S_2 в котором осуществляется открытие канала управления для авторизации (ввод имени и пароля). Если на этапе авторизации клиент оказывается санкционированным, то ему предоставляется доступ к информационным ресурсам сервера и система переходит в состояние S_5 под воздействием потока событий с интенсивностью λ_{25}, открывается канал передачи, потоки данных начинают передаваться с интенсивностью потоков событий λ_{56}. В

7 Розанов Ю. А. Случайные процессы. – М.: Наука, 1971. – 286 с.

8 Гнеденко Б. В., Коваленко И. Н. Введение в теорию массового обслуживания. – М.: Наука, 1966. – 431 с

процессе передачи и приема потоков данных от сервера клиентам поступают квитанции (подтверждениями о приеме частей потоков данных), система находится в состоянии S_6. Когда сервер закончил передачу данных и готов прервать соединение, возникает поток событий с интенсивностью λ_{61} на закрытие канала управления, и система переходит в состояние S_1.

В случае, когда клиент на этапе авторизации оказался несанкционированным, возникает поток событий с интенсивностью λ_{21} на отказ в авторизации клиента на сервере. При превышении максимально допустимого количества неудачных попыток авторизации клиента I_{cmax} возникает поток событий с интенсивностью λ_{23} на увеличение времени получения клиентом ответного отклика от сервера, в целях исключения попытки подбора клиентом имени пользователя и пароля методом перебора. Этот поток событий переводит моделируемую систему в состояние S_3, в котором клиент принимает от сервера множество промежуточных откликов, направляемые ему через заданные интервалы времени их задержки, изменяемые адаптивно или же фрагментированный ответный отклик или же ложного ответного отклика с сообщением о временной недоступности сервера (или же возможна комбинация этих методов). Этим обеспечивается замедление подключения злоумышленника к серверу, клиенты выстраиваются сервером в очередь на обработку их заявок, без разрыва с ними управляющего соединения, соединение для передачи данных не открывается. Далее моделируемая система с интенсивностью потоков событий λ_{34} переходит в состояние S_4, где оценивается состояние показателя простоя для злоумышленника. В случае, если значение времени простоя злоумышленника не достигло требуемого значения, то сервер, с интенсивностью потока событий λ_{43} продлевает это время простоя клиента, одним из вышеприведенных методов или их комбинацией, на необходимую величину. Далее, после простоя клиента в течение заданного времени, в целях обеспечения бескомпроматного функционирования средств защиты, возникает поток событий с интенсивностью потока событий λ_{45} на передачу и прием потоков данных между клиентом и сервером, а также поток событий на передачу клиентом очередной части потока данных для завершения передачи с интенсивностью потока событий λ_{56} (задачи системы защиты выполнены в течение времени пока злоумышленник находился в простое). В случае же компрометации средств защиты несанкционированный клиент может самостоятельно разорвать управляющее соединение, и тогда моделируемая система с интенсивностью потока событий λ_{31} переходит в состояние S_1.

Моделируемая ИС ФО может находиться в состояниях S_i с различной вероятностью $p_i(t)$. По размеченному графу состояний (рис. 2) строится математическая модель ее функционирования (6).

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. Задавая численные значения интенсивностей λ_{ij} 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) (6) с постоянными коэффициентами решают численными или аналитическими методами[9].

Аналитическая форма общего решения СЛОДУ Колмогорова с учетом условия нормировки сводится к решению алгебраической задачи на собственные значения.

Для определения существования финальных вероятностей и соответственно стационарного процесса проводится оценка асимптотической устойчивости (свойство эргодичности) исследуемой модели ИС ФО к вариациям исходных данных, через назначение граничных значений интенсивностей в условиях функционирования ИС ФО. Финальные вероятности существуют, если действительные части собственных чисел матрицы интенсивностей потоков событий принимают отрицательные значения. Чем меньше значение действительной части собственных чисел, тем меньше длительность переходного процесса. Определяя зависимости собственных чисел от значений различных интенсивностей потоков событий λ, можно определить интервалы их возможных значений, при которых существуют финальные вероятности состояний исследуемой модели ИС ФО.

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

В рамках оценки корректности модели необходимо оценить устойчивость параметров передачи данных по отношению к возмущениям (погрешностям) исходных данных (интенсивностей потоков событий). В данном случае используется понятие робастной устойчивости модели к возмущению исходных данных. Под робастностью математической модели понимают устойчивость искомых (выходных) параметров модели к погрешности исходных данных. Робастность решения (вектора финальных вероятностей $\{p_j\}$) к изменению входных параметров (интенсивностей потоков событий), как погрешность решения системы линейных алгебраических

9 Верждицкий В. М. Основы численных методов. – М.: Высшая школа, 2002. – 840 с.

уравнений (СЛАУ) Колмогорова при соответствующей погрешности исходных данных, позволяет оценить число обусловленности *cond(B)* матрицы интенсивностей потоков событий *B*.

Оценим устойчивость модели к вариациям исходных данных, задавая граничные значения в стратегиях взаимодействующих сторон, при этом рассмотрим следующие варианты стратегий:

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, успевает их обработать 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 ИС ФО, то рассматривается, как влияют интенсивности потоков событий λ_{12} на установление соединения сервером и авторизацию клиента на сервере ИС ФО и λ_{25} на передачу данных после успешной авторизации.

Для поиска допустимого интервала варьирования значений интенсивностей зададим λ_{12}=*x* и λ_{25}=*y*, при которых процесс эргодичен, определим зависимости действительной части собственных чисел k_1 – k_5 матрицы *B* от данных интенсивностей. Количество собственных чисел матрицы *B* определяется размерностью матрицы *B*.

Результаты вычисления зависимости действительной части собственных чисел матрицы *B* от значений интенсивностей λ_{12}=*x* и λ_{25}=*y*, $x \in [0,100]$, $y \in [0,100]$ представлены в графическом виде на рисунке 3, ($k_1 = -361;\ k_2 = -138;\ k_{3..5} = f(x,y)$).

Поскольку в рассматриваемом диапазоне значений действительные части собственных чисел матрицы *B*, характеризующей СЛОДУ Колмогорова, принимают отрицательные значения, то цепь Маркова с непрерывным временем при рассматриваемых значениях интенсивностей потоков событий в ситуации SIT_1 эргодична.

Зависимость p_5 (передача и прием потоков данных между клиентом и сервером (открытие канала передачи данных) и p_6 (подтверждение сервером приема частей потока данных (квитирование)) от значений интенсивностей λ_{12}=*x* и λ_{25}=*y*, $x \in [0,100]$, $y \in [0,100]$, представлена на рис.4.

Применительно к ситуации SIT_1 построим зависимость числа обусловленности матрицы B от варьируемых интенсивностей потоков событий (рис. 5) в форме нормы максимум $\|x\|_\infty$.

Так как значение числа обусловленности *v* не превышает 10 для вариации λ_{12} и λ_{25} в диапазоне (0; 100),

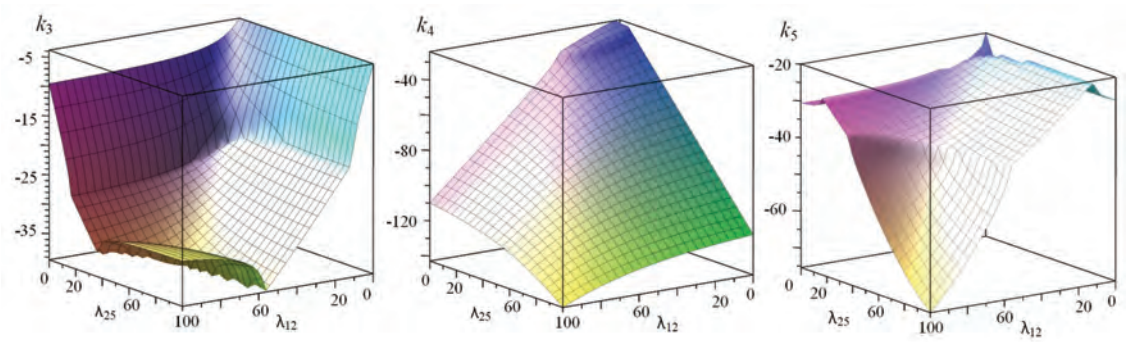

Рис. 3. Зависимости действительной части собственных чисел матрицы B от варьируемых λ_{12} и λ_{25} применительно к SIT_1

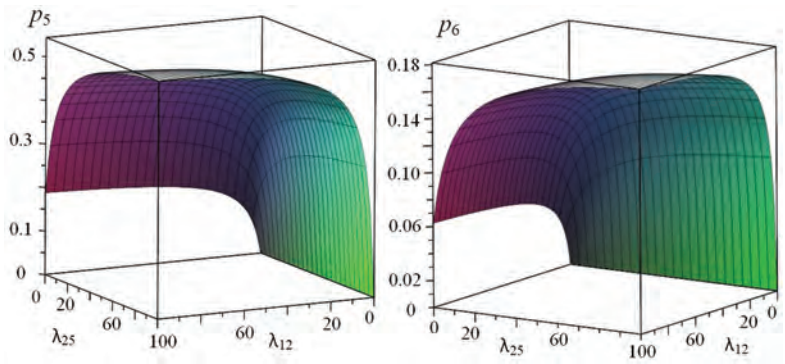

Рис. 4. Зависимость p_5 и p_6 от варьируемых λ_{12} и λ_{25}

то построенная математическая модель марковского процесса в ситуации SIT_1 является робастной.

В качестве численного метода решения системы ЛДУ выбран классический метод четвертого порядка – метод Рунге-Кутты с фиксированным шагом интегрирования. Решение численным методом дает оценку не только финальных вероятностей, но и переходных процессов. Однако при выборе конкретного значения λ_{ij} возникает вопрос обоснованности выбора. Выбранное значение λ_{ij} должно принадлежать диапазону, соответствующему эргодичности и устойчивости случайного процесса при различных значениях входных параметров.

Графики зависимостей вероятностей состояний исследуемого процесса от времени для ситуации SIT_1 представлены на рисунке 6.

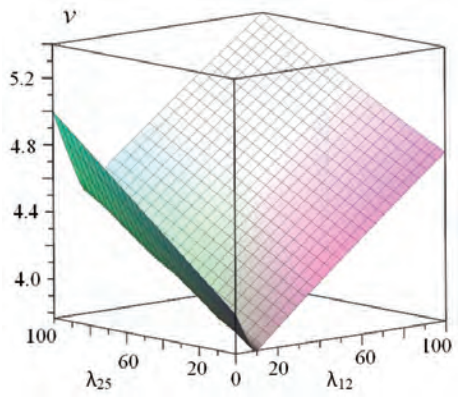

Рис. 5. Зависимость числа обусловленности матрицы B в форме нормы максимум от варьируемых λ_{12} и λ_{25} применительно к SIT_1

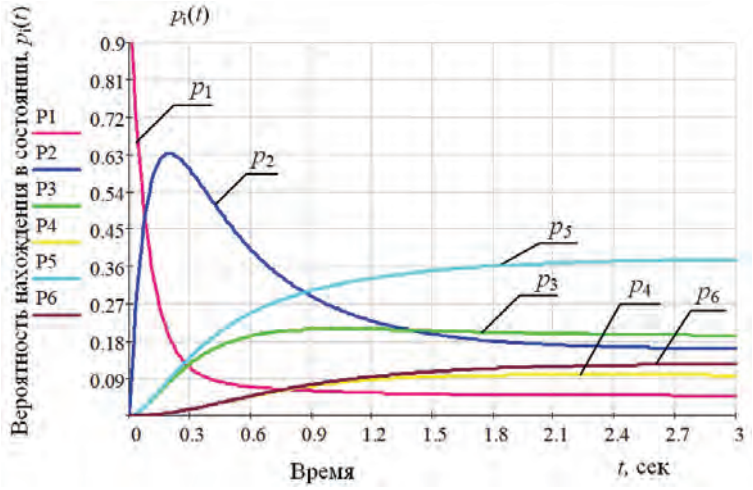

Рис. 6. Результаты расчета зависимости вероятностей состояний от времени для значений интенсивностей событий соответствующие ситуации SIT_1

Для ситуации SIT_1 из графика (рис. 6) видно, что в начале ИС ФО находится в переходном режиме функционирования, где наблюдается всплеск значения вероятности состояния $p_2(t)$, что соответствует нахождению ИС ФО в состоянии инициализации соединения клиентами и начале передачи данных. Далее в ИС устанавливается стационарный режим, когда ИС ФО случайным образом меняет свои состояния и ее вероятности $p_1(t)$, $p_2(t)$, …, $p_6(t)$ уже не зависят от времени и равны финальным (предельным) вероятностям. Вероятность $p_5(t)$ - передача и прием потоков данных между клиентом и сервером (открытие канала передачи данных) имеет максимальное значение 0,381.

Ситуация SIT_2 – соединение клиентов с сервером осуществляется, с замедлением передачи потока данных между клиентом и сервером ИС ФО. Сервер, получив значительное множество заявок на соединение от клиентов, выстраивает их в очередь и далее последовательно обрабатывает. Средства СР обнаружены штатными средствами защиты. Сервер разрывает в одностороннем порядке соединение с клиентом в случае неуспешной авторизации. 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, тогда пусть $\lambda_{12}= x$, $\lambda_{23}= y$.

Результаты вычисления зависимости действительной части собственных чисел матрицы *B* от значений интенсивностей $\lambda_{12}=x$ и $\lambda_{23}=y$, $x \in [0, 500]$, $y \in [0, 500]$ представлены в графическом виде на рисунке 7 ($k_{1..5} = f(x, y)$).

Поскольку в рассматриваемом диапазоне значений действительные части собственных чисел матри-

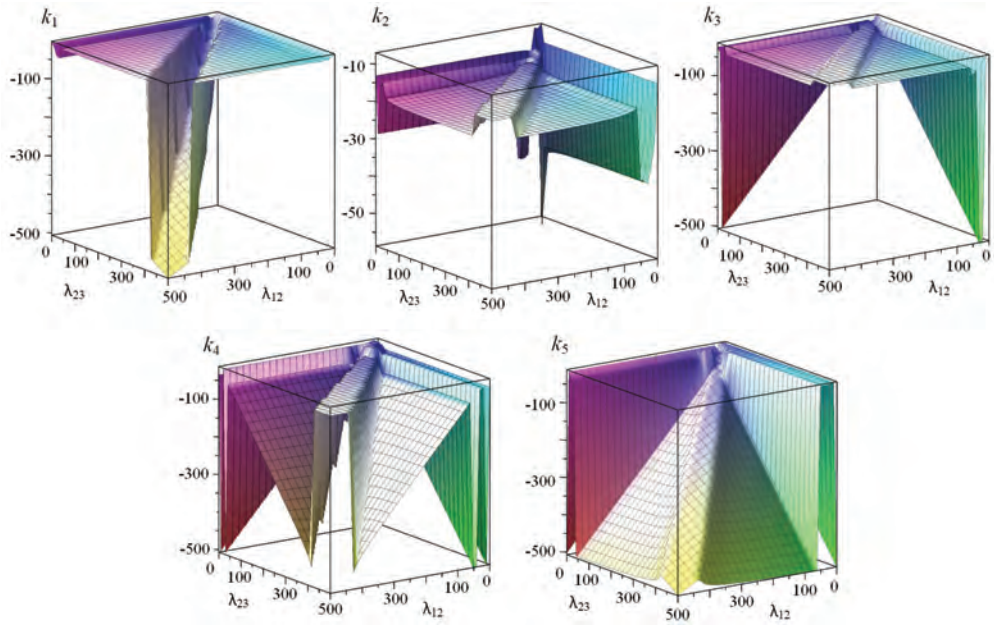

Рис. 7. Зависимости действительной части собственных чисел матрицы B от варьируемых λ_{12} и λ_{23} применительно к SIT_2

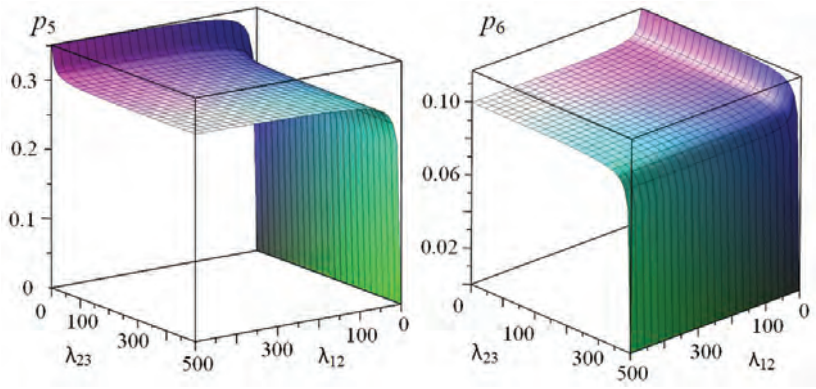

Рис. 8. Зависимость p_5 и p_6 от варьируемых λ_{12} и λ_{23}

цы *B*, характеризующей СЛОДУ Колмогорова, принимают отрицательные значения, то цепь Маркова с непрерывным временем при рассматриваемых значениях интенсивностей потоков событий в ситуации SIT_2 эргодична.

Зависимость p_5 (подтверждение сервером приема частей потока данных (квитирование) и p_6 (передача и прием потоков данных между клиентом и сервером) от значений интенсивностей $\lambda_{12}=x$ и $\lambda_{23}=y$, $x \in [0, 500]$, $y \in [0, 500]$, представлена на рисунке 8.

Применительно к ситуации SIT_2 построим зависимость числа обусловленности матрицы *B* от варьируемых интенсивностей потоков событий (рис. 9) в форме нормы максимум $\|x\|\_\infty$.

Так как значение числа обусловленности *v* превышает 50 для вариации λ_{12} и λ_{23} в диапазоне (0; 500), то построенная математическая модель марковского процесса в ситуации SIT_2 является слабо робастной в этом диапазоне.

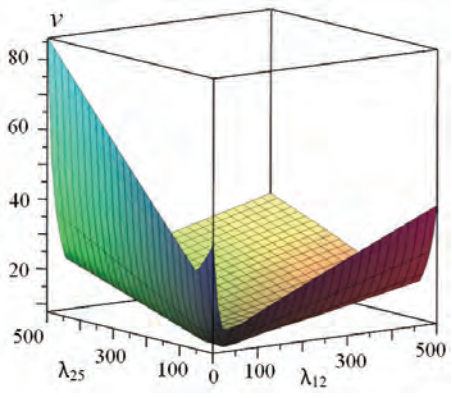

Рис. 9. Зависимость числа обусловленности матрицы B в форме нормы максимум от варьируемых λ_{12} и λ_{23} применительно к SIT_2

УДК 004.772

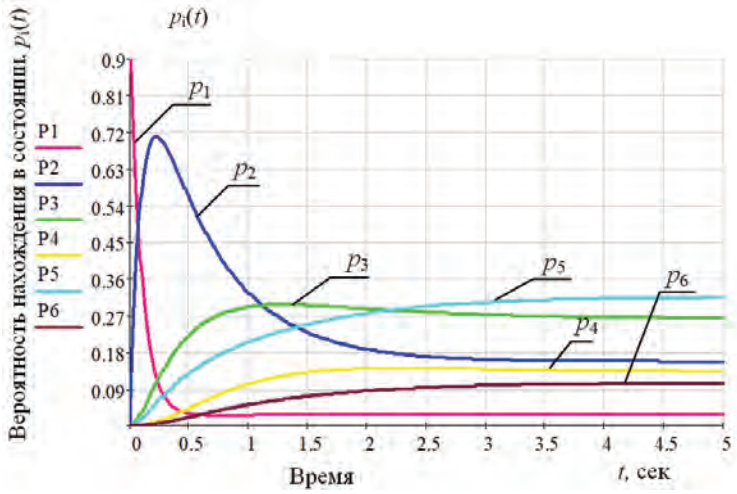

Рис. 10. Результаты расчета зависимости вероятностей состояний от времени для значений интенсивностей событий соответствующие ситуации SIT_2

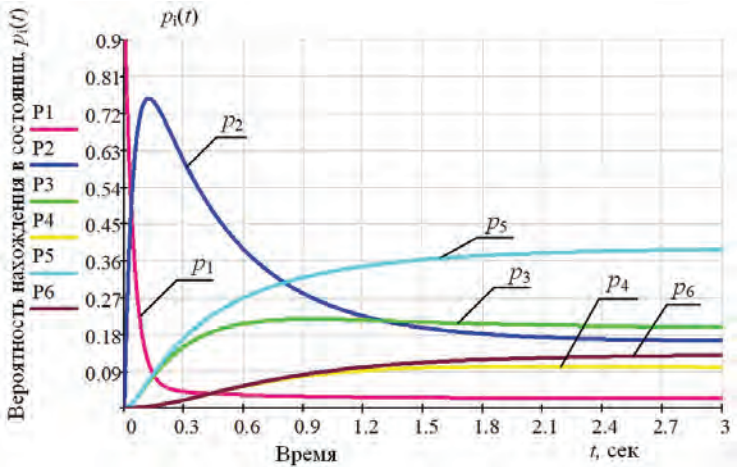

Рис. 11. Зависимости вероятностей состояний от времени для заданных значений интенсивностей потока событий (λ_{12}=2100)

Для получения оценки переходных процессов в ситуации SIT_2 перейдем к решению СЛОДУ численным методом. Графики зависимостей вероятностей состояний исследуемого процесса от времени для ситуаций SIT_2 представлены на рисунке 10.

На интервале времени [0; 0,5] 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 клиентами. При $t \to \infty$ в ИС ФО устанавливается стационарный режим, когда ИС ФО случайным образом меняет свои состояния и ее вероятности $p_1(t)$, $p_2(t)$, …, $p_6(t)$ уже не зависят от времени и равны финальным (предельным) вероятностям.

Полученные значения финальных вероятностей $p_1 = 0.027$, $p_2 = 0.158$, $p_3 = 0.263$, $p_4 = 0.132$, $p_5 = 0.316$, $p_6 = 0.105$ показывают, сколько времени ИС ФО в среднем находится в каких состояниях.

Разработанная модель функционирования ИС ФО учитывает влияние и характер воздействия на ИС ФО потоков событий от клиентов с нормальным и высоким количеством заявок от клиентов к серверу, способных перегрузить его. Процесс защиты сервера от перегрузки, в соответствии с данной моделью, сводится к минимизации вероятности (и среднего времени) значения показателя простоя санкционированных клиентов, и, следовательно, минимизации вероятности перегрузки сервера ИС ФО.

Защита ИС ФО предполагает поиск стратегий ее функционирования в зависимости от изменяющихся вариантов взаимодействия клиентов и сервера из-за ограниченности ресурса сервера во времени. Модель позволяет вскрыть зависимости процесса функционирования ИС ФО от потоков воздействий, оценивать оперативность обслуживания клиентов, обоснованно выбирать алгоритмы защиты сервера от перегрузки и оптимально использовать ресурс сервера.

DOI:10.21681/2311-3456-2021-5-52-62

Увеличение интенсивностей заявок, как со стороны сервера, так и со стороны клиентов соответствует изменению ситуаций взаимодействующих сторон. С увеличением λ_{12} (на рис. 11 до 2100) ИС ФО находится в затрудненном режиме работы, вероятность ее нахождения в состоянии S_1 равна p_1=0.096. В то же время вероятность перехода системы в состояние S_2 будет максимальной и равной p_2=0.755, для заданных значений интенсивностей в ситуации SIT_1.

Снизить нагрузку на данное состояние сервера возможно путем увеличения его ресурса за счет создания очереди заявок между клиентами и сервером, а также отбрасыванием заявок на соединение от клиентов превышающих количество попыток авторизации.

Выводы

Для оценки качества системы защиты и эффективности противодействия СР в процессе установления соединений ИС ФО разработана критериальная оценочная база эффективности функционирования ИС ФО. Показано, что наиболее важным и привлекательным элементом для СР ресурсом является серверное ПО. Это связано с круглосуточным режимом работы серверов и их критической важностью для ИС ФО.

Научная новизна представленной модели заключается в применении математического аппарата теории марковских случайных процессов и решении уравнений Колмогорова для исследования и решения задачи динамического управления ресурсными возможностями ИС ФО, за счет управления параметрами передачи данных, а также в оценке асимптотической устойчивости и робастности модели относительно возмущений значений исходных параметров с целью повышения адекватности модели при выборе режимов управления процессом передачи данных.

Практическая значимость разработанной модели заключается в нахождении вероятностных и временных характеристик, описывающих процесс функционирования ИС ФО при различных ситуациях передачи данных, решении задачи оптимального управления процессом передачи данных, за счет направления злоумышленнику множества промежуточных откликов, через заданные интервалы времени их задержки изменяемые адаптивно, или фрагментированного ответного отклика или же ложного ответного отклика с сообщением о временной недоступности сервера, что обеспечивает управление вычислительным и временным ресурсом средств сетевой разведки, а также снижение возможностей компрометации средств защиты. При этом выбор ситуаций обусловлен особенностями процессов установления сетевых соединений и передачи данных по FTP.

Литература

1. Максимов Р.В., Соколовский С.П., Шарифуллин С.Р., Чернолес В.П. Инновационные информационные технологии в контексте обеспечения национальной безопасности государства // Инновации. 2018. № 3 (233). С. 28–35.
2. Иванов И.И., Максимов Р.В. Этюды технологии маскирования функционально-логической структуры информационных систем / И.И. Иванов, Р.В. Максимов // Инновационная деятельность в Вооруженных Силах Российской Федерации: сб. тр. участников всеармейской научно-практической конференции. – Санкт-Петербург, 2017. С. 147-154.
3. 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.
4. Ворончихин И.С., Иванов И.И., Максимов Р.В., Соколовский С.П. Маскирование структуры распределённых информационных систем в киберпространстве // Вопросы кибербезопасности. 2019. № 6 (34). С. 92-101. DOI: 10.21681/2311-3456-2019-6-92-101.
5. Марков А.С. Техническая защита информации. М. АИСНТ. 2020. 234 с.
6. Способ выбора безопасного маршрута в сети связи (варианты). Пат. 2331158 Рос. Федерация, МПК G06F / Кожевников Д.А., Максимов Р.В., Павловский А.В., Юрьев Д.Ю.; заявитель и патентообладатель Военная академия связи (RU). – № 2007103774; заявл. 31.01.2007; опубл. 10.08.2008. Бюл. № 22.
7. Максимов Р.В., Савинов Е.А. Оценка живучести распределенных интегрированных информационных систем / Р.В. Максимов, Е.А. Савинов // Информационные технологии и нанотехнологии (ИТНТ-2016) : сб. тр. участников Международной конференции и молодёжной школы. Самарский государственный аэрокосмический университет имени академика С.П. Королёва (национальный исследовательский университет)»; Институт систем обработки изображений РАН. Самара, 2016. С. 431- 438.
8. Устройство поиска информации Пат. 2219577 Рос. Федерация, МПК G06F / Ксёнз Е.С., Липатников В.А., Максимов Р.В., Стародубцев Ю.И., Федяков Е.Г., Хлыбов Д.Л.; заявитель и патентообладатель Военная академия связи (RU). № 2002111059; заявл. 24.04.2002; опубл. 20.12.2003. Бюл. № 12.
9. Максимов Р.В. Модель случайных помех интегрированным системам ведомственной связи // Научно-технические ведомости Санкт-Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. 2008. № 3 (60). С. 151-155.
10. 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.
11. Varenitca V. V., Markov A. S., Savchenko V. V. Recommended Practices for the Analysis of Web Application Vulnerabilities. // CEUR Workshop Proceedings. Volume 2603. 2019, pp. 75-78.
12. Chee Keong NG, Lei Pan, Dr. Yang Xiang. Honeypot Frameworks and Their Applications: A New Framework. In SpringerBriefs on Cyber Security Systems and Networks. Springer, Singapore. 2018. DOI: 10.1007/978-981-10-7739-5.

13. Wang, Y., Guo, Y., Zhang, L. et al. SWIM: An Effective Method to Perceive Cyberspace Situation from Honeynet. Arabian Journal for Science and Engineering. 2018. Vol. 43. P. 6863. DOI: 10.1007/s13369-017-2904-5.
14. 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.
15. Bilinski M., Gabrys R., Mauger J. Optimal Placement of Honeypots for Network Defense. In: Bushnell L., Poovendran R., Başar T. (eds) Decision and Game Theory for Security. GameSec 2018. Lecture Notes in Computer Science, vol 11199. Springer, Cham. 2018. DOI: https://doi.org/10.1007/978-3-030-01554-1_7.
16. 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.
17. Способ защиты вычислительных сетей. Пат. 2680038 Рос. Федерация, МПК G06F / Максимов Р.В., Орехов Д.Н., Соколовский С.П., Гаврилов А.Л. и др.; заявитель и патентообладатель Краснодарское высшее военное училище (RU). – № 2696330; заявл. 31.07.2018; опубл. 01.08.2019, Бюл. № 22.

MODEL OF SECURE FILE EXCHANGE INFORMATION TECHNOLOGY OPERATION

***Lebedkina T.V.*[10], *Sokolovsky S.P.*[11]**

The purpose of this work: *to develop a model that allows to assess the security of the information system of file exchange, to ensure the efficiency of servicing the maximum number of requests of authorized customers with a simultaneous decrease in the quality of service of requests from the attacker's means.*

Methods used: *formalization of service processes in the form of Markov random processes, as well as numerical methods.*

The result of the study: *a criterion evaluation base for the effectiveness of the functioning of the information system of file exchange has been developed. The problem of dynamic management of the resource capabilities of the information system of file exchange by managing the parameters of data transmission has been solved. An assessment of the asymptotic stability and robustness of the model relative to the perturbations of the values of the initial parameters is solved in order to increase the adequacy of the model when choosing control modes for the data transmission process. Probabilistic and temporal characteristics and the process of functioning of the information system of file exchange in the conditions of unauthorized influences in various situations of interaction of the parties to the conflict, as well as in the managementand computational and time resource of the means of network intelligence of the attacker are obtained. The optimal modes of functioning of information systemsand file exchange, ensuring its compliance withthe established security requirements of critical information infrastructure objects, aresubstantiated.*

Keywords: *network intelligence, network connections, Markov random process, asymptotic stability, robustness.*

References

1. Maksimov R.V., Sokolovsky S.P., Sharifullin S.R., Chernoles V.P. Innovacionny`e informacionny`e texnologii v kontekste obespecheniya nacional`noj bezopasnosti gosudarstva // Innovacii. 2018. № 3 (233). S. 28-35.
2. Ivanov I.I., Maksimov R.V. Etyudy tekhnologii maskirovaniya funkcional'no-logicheskoj struktury informacionnyh sistem / I.I. Ivanov, R.V. Maksimov // Innovacionnaya deyatel'nost' v Vooruzhennyh Silah Rossijskoj Federacii : sb. tr. uchastnikov vsearmejskoj nauchno-prakticheskoj konferencii. – Sankt-Peterburg, 2017. S. 147-154.
3. Maksimov R.V., Orexov D.N., Sokolovskij S.P. Model` i algoritm funkcionirovaniya klient-servernoj informacionnoj sistemy` v usloviyax setevoj razvedki // Sistemy` upravleniya, svyazi i bezopasnosti. 2019. № 4. C. 50-99.
4. Voronchixin I.S., Ivanov I.I., Maksimov R.V., Sokolovskij S.P. Maskirovanie struktury` raspredelyonny`x informacionny`x sistem v kiberprostranstve // Voprosy` kiberbezopasnosti. 2019. № 6 (34). C. 92-101.
5. Markov A.S. Tekhnicheskaya zashchita informacii. Moscow. AISNT. 2020. 234 p.

10 Tatyana Lebedkina, lecturer of the Department of Protected Information Technologies, Krasnodar Higher Military Orders of Zhukov and the October Revolution Red Banner School named after General of the Army S.M. Shtemenko, Krasnodar, Russia. E-mail: alina010570@mail.ru

11 Sergey Sokolovsky, Ph.D., Associate Professor, Krasnodar Higher Military Orders of Zhukov and the October Revolution Red Banner School named after General of the Army S.M. Shtemenko, Krasnodar, Russia. E-mail: mtd.krd@mail.ru

6. Sposob vybora bezopasnogo marshruta v seti svyazi (varianty). Pat. 2331158 Ros. Federaciya, MPK G06F / Kozhevnikov D.A., Maksimov R.V., Pavlovskij A.V., Yur'ev D.Yu.; zayavitel' i patentoobladatel' Voennaya akademiya svyazi (RU). – № 2007103774; zayavl. 31.01.2007; opubl 10.08.2008. Byul. № 22.
7. Maksimov R.V., Savinov E.A. Ocenka zhivuchesti raspredelennyh integrirovannyh informacionnyh sistem / R.V. Maksimov, E.A. Savinov // Informacionnye tekhnologii i nanotekhnologii (ITNT-2016) : sb. tr. uchastnikov Mezhdunarodnoj konferencii i molodyozhnoj shkoly. Samarskij gosudarstvennyj aerokosmicheskij universitet imeni akademika S.P. Korolyova (nacional'nyj issledovatel'skij universitet)»; Institut sistem obrabotki izobrazhenij RAN. – Samara, 2016. S. 431-438.
8. Ustrojstvo poiska informacii Pat. 2219577 Ros. Federaciya, MPK G06F / Ksyonz E.S., Lipatnikov V.A., Maksimov R.V., Starodubcev Yu.I., Fedyakov E.G., Hlybov D.L.; zayavitel' i patentoobladatel' Voennaya akademiya svyazi (RU). – № 2002111059; zayavl. 24.04.2002; opubl 20.12.2003. Byul. № 12.
9. Maksimov R.V. Model' sluchajnyh pomekh integrirovannym sistemam vedomstvennoj svyazi / R.V. Maksimov // Nauchno-tekhnicheskie vedomosti Sankt-Peterburgskogo gosudarstvennogo politekhnicheskogo universiteta. Informatika. Telekommunikacii. Upravlenie. 2008. № 3 (60). S. 151-155.
10. Gorbachev A. A., Sokolovsky S. P., Usatikov S. V. Model` funkcionirovaniya i algoritm proaktivnoj zashhity` servisa e`lektronnoj pochty` ot setevoj razvedki // Sistemy` upravleniya, svyazi i bezopasnosti. 2021. № 3. S. 60-109. DOI: 10.24412/2410-9916-2021-3-60-109.
11. Varenitca V. V., Markov A. S., Savchenko V. V. Recommended Practices for the Analysis of Web Application Vulnerabilities. 10th Anniversary International Scientific and Technical Conference on Secure Information Technologies, BIT 2019 CEUR Workshop Proceedings. Volume 2603. Moscow, 2019, pp. 75-78.
12. Chee Keong NG, Lei Pan, Dr. Yang Xiang. Honeypot Frameworks and Their Applications: A New Framework. In SpringerBriefs on Cyber Security Systems and Networks. Springer, Singapore. 2018. DOI: 10.1007/978-981-10-7739-5.
13. Wang, Y., Guo, Y., Zhang, L. et al. SWIM: An Effective Method to Perceive Cyberspace Situation from Honeynet. Arabian Journal for Science and Engineering. 2018. Vol. 43. P. 6863. DOI: 10.1007/s13369-017-2904-5.
14. 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.
15. Bilinski M., Gabrys R., Mauger J. Optimal Placement of Honeypots for Network Defense. In: Bushnell L., Poovendran R., Başar T. (eds) Decision and Game Theory for Security. GameSec 2018. Lecture Notes in Computer Science, vol 11199. Springer, Cham. 2018. DOI: https://doi.org/10.1007/978-3-030-01554-1_7.
16. 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.
17. Sposob zashchity vychislitel'nyh setej. Pat. 2680038 Ros. Federaciya, MPK G06F / Maksimov R.V., Orekhov D.N., Sokolovskij S.P., Gavrilov A.L. i dr.; zayavitel' i patentoobladatel' Krasnodarskoe vysshee voennoe uchilishche (RU). – № 2696330; zayavl. 31.07.2018; opubl. 01.08.2019, Byul. № 22.