УДК 004.056+ 519.872
DOI: 10.46548/21vek-2020-0951-0009

МОДЕЛЬ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ ДЛЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ НА БАЗЕ ТЕОРИИ МАССОВОГО ОБСЛУЖИВАНИЯ

Прошин Иван Александрович, доктор технических наук, доцент, архитектор
АО «Бэлл интегратор»
(440000, Россия, Пенза, ул. Московская, 27, e-mail: proshin.Ivan@inbox.ru)
Мартышкин Алексей Иванович, кандидат технических наук, доцент,
доцент кафедры «Вычислительные машины и системы»
Истомина Татьяна Викторовна, доктор технических наук, профессор,
ведущий научный сотрудник отдела научных исследований
Пензенский государственный технологический университет
(440039, Россия, Пенза, проезд Байдукова/ул. Гагарина, д. 1а/11, e-mails: alexey314@yandex.ru, istom@mail.ru)

Аннотация. Статья посвящена разработке модели поддержки принятия решений для системы защиты информации на базе теории массового обслуживания, выявление с ее помощью путей улучшения характеристик системы. Рассмотрены ключевые понятия теории массового обслуживания применительно к задаче защиты информации. Предложена общая схема модели, на ее основе разработана модель защиты информации, реализованная в среде AnyLogic. Проведены экспериментальные исследования модели, показавшие, что система защиты регистрирует совершение несанкционированного доступа (НСД) в случае, когда максимальной нагрузке подвергается механизм защиты «Регистрация событий безопасности». Сделан вывод относительно целесообразного порядка обработки заявок с учетом времени их обслуживания, повышающего обоснованность принятия решения о совершении НСД, а также даны рекомендации по уменьшению числа пропущенных событий и повышению производительности системы защиты информации с одновременным увеличением интенсивности обслуживания заявок и сокращения времени их ожидания в очереди.

Ключевые слова: защита информации, несанкционированный доступ, массовое обслуживание, заявка, событие, моделирование, система, теория, локальная вычислительная сеть.

DECISION SUPPORT MODEL FOR INFORMATION SECURITY SYSTEMS BASED ON QUEUING THEORY

Proshin Ivan Aleksandrovich, doctor of technical Sciences, associate Professor, creator
Joint-stock company «Bell integrator»
(440000, Russia, Penza, Moskovskaya street, 27, e-mail: proshin.Ivan@inbox.ru)
Martyshkin Alexey Ivanovich, candidate of technical sciences, docent,
associate Professor of sub-department «Computers and systems»
Istomina Tatyana Viktorovna, doctor of technical Sciences, professor,
leading researcher of the Department of scientific research
Penza state technological University
(440039, Russia, Penza, Baydukov Proyezd / Gagarin Street, 1a/11, e-mails: alexey314@yandex.ru, istom@mail.ru)

Abstract. The article is devoted to the development of a decision support model for the information security system based on the Queuing theory, identifying ways to improve the system characteristics. The key concepts of Queuing theory in relation to the problem of information security are considered. The General scheme of the model is proposed, and the information security model implemented in the AnyLogic environment is developed on its basis. Experimental studies of the model have shown that the security system registers the Commission of unauthorized access (NSD) in the case when the maximum load is exposed to the security mechanism "Registration of security events". The conclusion is made about the expedient order of processing applications, taking into account the time of their service, which increases the validity of making a decision on making an NSD, and recommendations are made to reduce the number of missed events and improve the performance of the information security system, while increasing the intensity of application service and reducing the time they wait in the queue.

Keywords: information security, unauthorized access, mass service, application, event, simulation, system, theory, local area network.

Введение. Система защиты информации (СЗИ) в процессе функционирования обрабатывает множество событий различного уровня сложности, принимая решение о негативности того или иного события на основе заложенных в неё алгоритмов, логики, базы сигнатур и т.д. Все они с течением времени требуют модернизации и совершенствования. Суть исследований согласно теории массового обслуживания (ТМО) заключается в рациональном выборе структуры и процесса обслуживания [1 – 4] и [5 – 8]. Это осуществляется путем анализа потоков требований на обслуживание, поступающих в систему и выходящих из неё, с

учетом продолжительности ожидания и длины очередей. Этим определяется актуальность проводимого в данной работе исследования.

Целью работы является разработка модели принятия решений системой защиты информации на базе ТМО. Решаются следующие задачи:

1) проведение анализа основных злоумышленных воздействий на операционную систему (ОС) компьютерной системы;

2) исследование работы системы защиты информации от несанкционированного доступа с позиций теории массового обслуживания, изучение и представление основных принципов, понятий, характеристик;

3) разработка проекта модели защиты информации, определяющего параметры и условия моделирования;

4) разработка плана и проведение ряда экспериментов с последующим анализом полученных результатов.

Материалы и результаты исследования. СЗИ в процессе функционирования обрабатывает множество событий различного уровня сложности, принимая решение о негативности того или иного события на основе заложенных в неё алгоритмов, логики, базы сигнатур и т.д. Все они с течением времени требуют модернизации и совершенствования ввиду того, что появляются новые злонамеренные приемы несанкционированного доступа. Согласно ГОСТ Р 50922-2006 под системой защиты информации понимается «Совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации» [9]. Это понятие определяет СЗИ в глобальном смысле. Для исследования в рамках данной работы выбрана СЗИ от несанкционированного доступа к данным (НСД). В результате анализа литературных источников [10 – 15] и [16 – 20], посвященных защите данных от НСД, можно сформулировать перечень функций, реализацию которых должна поддерживать типовая СЗИ от НСД. Это аутентификация и идентификация, разграничение доступа пользователей к ПК, регистрация событий безопасности, определение прав доступа к ресурсам, программам, процессам, возможным действиям над информацией, запуск системы защиты на ЭВМ, контроль работоспособности и целостности систем защиты, сигнализация о попытках НСД и др. Очевидно, что процессы, протекающие в СЗИ от НСД, носят случайный характер. Все злонамеренные воздействия на систему генерируют большое число запросов, процессов и событий. Исходя из этого, делаем вывод, что данная система относится к классу систем массового обслуживания (СМО) и ее можно исследовать с точки зрения ТМО. Емко описать принцип работы СМО можно следующим образом: заявки генерируются источником и поступают в СМО случайным образом. Время, затраченное на обслуживание каждой заявки, также случайно. Далее канал обслуживания освобождается и готов к принятию следующей заявки. Каждая СМО, в зависимости от числа каналов и их производительности, обладает некоторой пропускной способностью. Параметр пропускной способности СМО может рассматриваться как абсолютный, либо как относительный.

Общая структура модели. Дана автоматизированная система (АС), представляющая собой электронно-вычислительную машину (ЭВМ), находящуюся в составе локально-вычислительной сети (ЛВС). В АС используется СЗИ от несанкционированного доступа. Функционирование СЗИ в терминах теории массового обслуживания можно представить как взаимодействие с потоками случайных событий – заявок на идентификацию и аутентификацию пользователей, запросы на запуск программ и процессов, использование тех или иных ресурсов, генерация событий в журналах, событий, связанных с необходимостью обеспечения контроля доступа и т.д. Их появление может быть вызвано как действиями обычных легальных пользователей, так и действиями злоумышленников, ошибками и т.д.

В связи с тем, что информационные активы, являющиеся объектом, на который направлены воздействия злоумышленника, размещены на ЭВМ, для упрощения модели будем рассматривать поток событий, среди которых могут быть характеризующие подозрительную активность события, связанные с попытками получения НСД к одной из ЭВМ сети. Т. к. в связи с этим увеличивается количество и случайность генерируемых запросов, это обстоятельство позволяет считать, что моменты появления запросов образуют ординарный рекуррентный поток.

При рассмотрении потоков заявок, поступающих в систему массового обслуживания в качестве случайной величины, будем принимать во внимание время появления заявок в системе [2]. Для описания потоков заявок необходимо задать интервалы времени $\tau_k = t_k - t_k - 1$ между соседними моментами $t_k - 1$ и t_k поступления заявок с порядковыми номерами $(k - 1)$ и k соответственно ($k=1, 2, \ldots; t_0 = 0$ – начальный момент времени).

В качестве основной характеристики потока заявок выступает его интенсивность λ – среднее число заявок, проходящих через некоторую границу за единицу времени. В рамках рассматриваемой модели в качестве приборов обслуживания выступают механизмы защиты, а в качестве заявок – поступающие запросы, заявки на обслуживание, доступ к ресурсам, события в ОС и т.д.

Модель СМО реализует алгоритм, отражающий изменения состояний системы во времени при заданных входных параметрах потоков заявок. Входящие потоки определяют значения внешних параметров СМО. С целью идентификации функциональных блоков модели представим обобщенную схему СМО (рис. 1) в виде общей схемы, состоящей из трех основных блоков: «Пользователь», «СЗИ» и «Активные устройства».

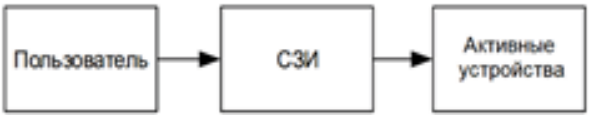


Рисунок 1 – Общая схема модели

Задача функционирования блока «Пользователь» – генерация потока (потоков) запросов с заданной интенсивностью λ. Блок «СЗИ» имитирует работу механизмов защиты: очереди запросов на входах механизмов защиты, задержки на обслуживание и т.д. Блок «Активные устройства» не выполняет никаких самостоятельных функций. Он используется для полноты схемы, т.к. запросы должны направляться на какой-то ресурс, а не в пустоту. СЗИ представляет собой разомкнутую СМО, т.к. поток заявок поступает извне, проходит через каналы, очереди, обработчики запросов и на выходе уничтожается.

В результате анализа перечня функций, реализуемых системой защиты информации, объединения и упрощения некоторых из них таким образом, чтобы они вписывались в рамки ТМО, выделен список следующих механизмов защиты:

- идентификация и аутентификация;
- разграничение доступа пользователей к ресурсам;
- контроль доступа;
- регистрация событий безопасности.

Заявки, поступающие по каналам к вышеуказанным механизмам защиты, включают в себя, например:

- запросы на идентификацию,
- регистрация событий входа/выхода пользователя из системы,
- создание новых учетных записей,
- запуск программ и процессов и т.д.

В рамках данной модели введен параметр *K*, определяемый как отношение пропущенных (необработанных) заявок к общему количеству поступивших в систему заявок. При значении $K = 0,3$ этот параметр представляет собой границу, превышение которой принимается системой защиты как попытка совершения НСД.

Разработка модели системы защиты информации. С учетом особенностей реализации алгоритмов функционирования СМО в среде *AnyLogic* схему модели можно представить так, как это показано на рисунке 2.

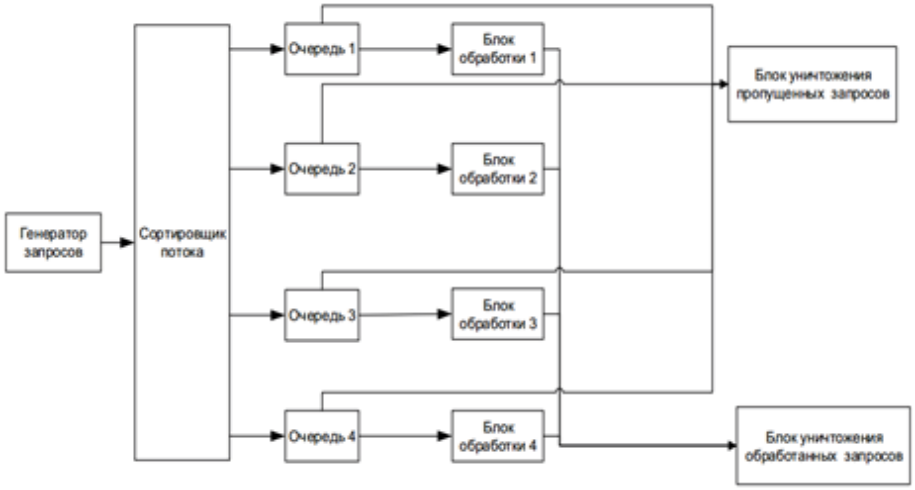


Рисунок 2 – Схема модели СЗИ

Генератор запросов инициирует поток заявок с заданной интенсивностью. Попадая в сортировщик, поток разбивается на четыре потока за счет перенаправления заявок на разные выходы согласно заданным процентным долям. Каждый из потоков направляется в накопитель, представленный блоком «Очередь», и остается в нем в ожидании своей очереди. Необходимо отметить, что заявки выбираются из очереди в соответствии с заданной дисциплиной обслуживания.

Блоку обработки соответствует тот или иной механизм защиты. В этом блоке заявки задерживаются на некоторое время согласно заданным условиям обработки. В рамках рассматриваемой модели – согласно случайному распределению по экспоненциальному закону. А затем следует «Блок уничтожения обработанных заявок».

Также заявки из очереди могут вытесняться в соответствии с заданным условием, а именно из-за перегрузки буфера. То есть, когда заявка приходит, а места в очереди нет, она вытесняется или вытесняет другую заявку в соответствии с заданной дисциплиной обслуживания, установленным приоритетом или заданным условием.

Из каждой очереди такие вытесненные заявки направляются на «Блок уничтожения пропущенных запросов», который аналогично блоку уничтожения обработанных заявок реализуется объектом *Sink*.

Выбор значения параметра вероятности попадания событий из входящего потока на тот или иной выход для последующего помещения в очередь на обслуживание осуществляется согласно заданным процентным долям. Их значения выбираются исходя из результата анализа статистических данных о числе событий, занесенных в журналы ОС. Значение рассчитывается как доля событий, подлежащих обслуживанию определенным механизмом защиты, в общей

сумме всех событий, внесенных в журналы ОС за единицу времени.

К входным параметрам модели, значения которых изменяются в зависимости от условий и сценария эксперимента относятся интенсивность потока заявок и вероятности попадания заявки в определенный поток. Выходные параметры модели, значения которых будут использоваться для дальнейших анализа и обработки, – это: производительность СМО; нагрузка системы; время наблюдения за системой; количество заявок, поступивших в систему за время ее работы; доля пропущенных заявок; доля обработанных заявок.

Проведение экспериментальных исследований. Задача экспериментального исследования заключается в изучении поведения модели СЗИ в условиях изменения интенсивности потока заявок и увеличения нагрузки на отдельные каналы, а также выявлении зависимостей скорости принятия решения о совершении НСД от входных параметров. Необходимо заметить, что принятие решения о совершении НСД происходит, когда отношение количества пропущенных заявок к количеству обработанных заявок превышает 30%. В этом случае работа системы блокируется, и принимается решение о наличии несанкционированных действий.

Эксперимент включает выполнение десяти этапов, в первых пяти из них моделируется работа СЗИ от НСД в условиях, когда в приоритете заявки с минимальным временем обработки. На первом этапе моделируется работа СЗИ от НСД в нормальном режиме. Значения долей распределения заявок по потокам выбираются исходя из результата анализа статистических данных о числе событий, занесенных в журналы ОС, рассчитываются они как доля событий, подлежащих обслуживанию определенным механизмом защиты, в общей сумме всех событий, внесенных в журналы ОС за единицу времени. На последующих (со второго по пятый) этапах моделируется работа СЗИ от НСД в режиме, когда нагрузка увеличивается на каждом механизме защиты поочередно, при этом значение доли в распределении заявок для выбранного механизма защиты увеличивается на 0,3. Для остальных – уменьшается прямо пропорционально их долевому значению, причем таким образом, чтобы их сумма уменьшилась ровно на 0,3.

Анализ полученных данных. Для интерпретации результатов, полученных в ходе экспериментов, ниже представлены графики зависимостей, иллюстрирующие работу модели.

График зависимости загрузки системы от интенсивности генерируемого потока для каждого набора распределения загрузки каналов представлен на рисунке 3. Из графика следует, что система наиболее загружена в случае, когда загрузка первого канала максимальна. Таким образом, большая часть генерируемых событий подлежит обработке первым механизмом защиты «Идентификация и аутентификация». Меньше всего на загрузку системы влияет максимальная загрузка третьего канала, по которому идут запросы к механизму защиты «Контроль доступа».

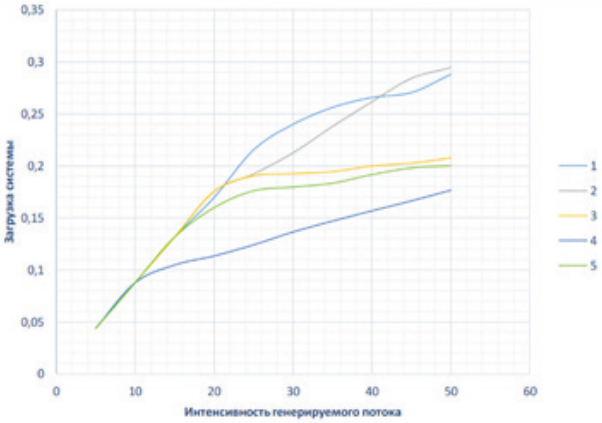


Рисунок 3 – График зависимости загрузки системы от интенсивности генерируемого потока

Это обусловлено тем, что запросов и событий, связанных с проверкой соответствия запрашиваемых и имеющихся разрешений на доступ к тому или иному ресурсу или объекту, обычно гораздо больше, чем запросов к другим механизмам защиты. Потому система устойчива к нагрузкам на этот канал.

Для анализа полученных результатов определялось значение упомянутого выше показателя K:

$$K = \frac{(N - N_0)/N}{T}, \quad (1)$$

где N – количество поступивших систему заявок, No – количество обработанных заявок. T – время работы модели до получения сигнала о принятии решения о совершении вредоносной деятельности.

Необходимо заметить, что данный показатель учитывает также и заявки, ожидающие обработки. Желательным является минимизация количества пропущенных заявок и минимизация длины очередей, однако это сопряжено с увеличением времени работы модели. Действительно, момент достижения установленного отношения пропущенных заявок к обработанным будет отодвигаться, а значение названного показателя стремиться к максимуму. График зависимости значения показателя от интенсивности генерируемого потока при работе системы в нормальном режиме представлен на рисунке 4.

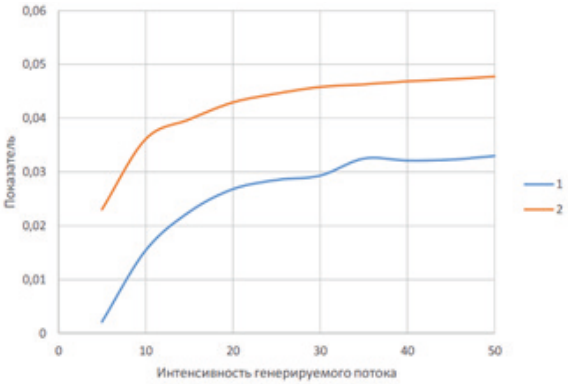
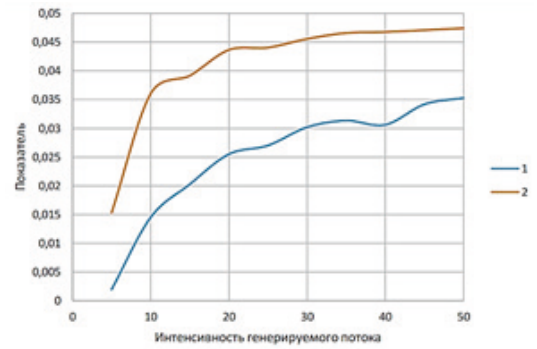
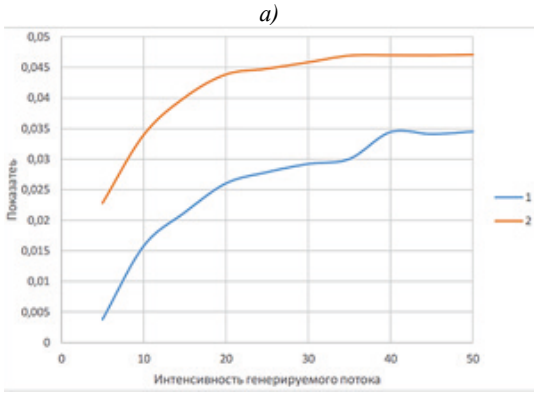


Рисунок 4 – График зависимости значения показателя от интенсивности генерируемого потока

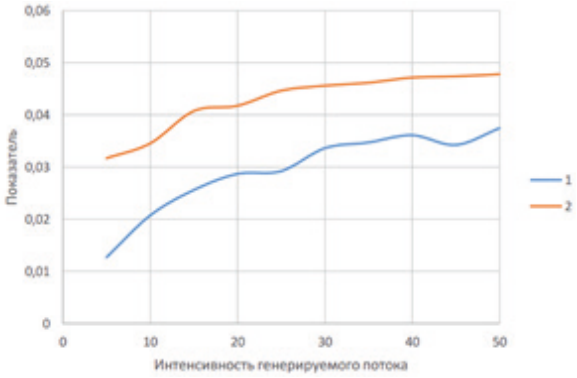


а)

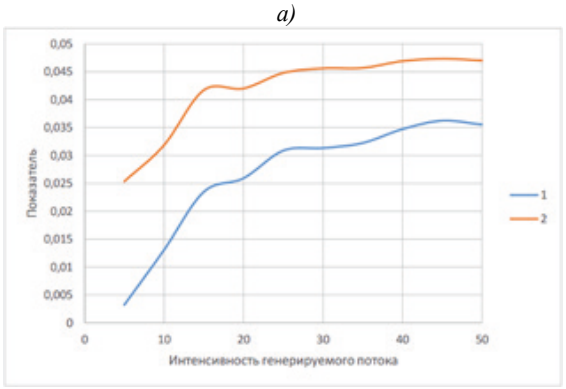


б)

Рисунок 5 – График зависимости значения показателя от интенсивности генерируемого потока. Усиленная нагрузка: на первый механизм защиты (а), на второй механизм защиты (б)



а)



б)

Рисунок 6 – График зависимости значения показателя от интенсивности генерируемого потока. Усиленная нагрузка: на третий механизм защиты (а), на четвертый механизм защиты (б)

Здесь и далее на рисунках 5 – 6 под цифрой 1 представлены зависимости показателя от интенсивности генерируемого потока при условии, когда в приоритете заявки с минимальным временем обработки, под цифрой 2 – зависимости показателя от интенсивности генерируемого потока при условии, когда в приоритете заявки с максимальным временем обработки.

Доли распределения заявок на механизмы защиты имеют следующие значения: $P1 = 0{,}104$; $P2 = 0{,}231$; $P3 = 0{,}473$; $P4 = 0{,}192$. Проанализировав график, можно прийти к выводу, что наилучшим решением является режим работы системы, когда в приоритете заявки с максимальным временем обработки.

На рисунках 5, 6 представлены зависимости значения показателя от интенсивности генерируемого потока, в режиме усиленной нагрузки на один из механизмов защиты.

Для рисунка 5, а: доли распределения заявок на механизмы защиты имеют следующие значения: $P1 = 0{,}404$; $P2 = 0{,}153$; $P3 = 0{,}315$; $P4 = 0{,}128$, для рисунка 5, б – соответственно: $P1 = 0{,}063$; $P2 = 0{,}531$; $P3 = 0{,}288$; $P4 = 0{,}117$.

Для рисунка 6, а: доли распределения заявок на механизмы защиты имеют следующие значения: $P1 = 0{,}045$; $P2 = 0{,}1$; $P3 = 0{,}772$; $P4 = 0{,}083$, а для рисунка 6, б – $P1 = 0{,}065$; $P2 = 0{,}145$; $P3 = 0{,}297$; $P4 = 0{,}492$.

Проанализировав графики на рисунках 5 – 6, сделаем вывод, что для каждого режима работы наилучшим решением является режим работы системы, когда в приоритете заявки с максимальным временем обработки. Однако в случае усиленной нагрузки на четвертый механизм защиты режим работы оказывается неустойчивым, что характеризуется колебаниями кривых. Это говорит о том, что при разработке или модернизации СЗИ от НСД необходимо уделить наибольшее внимание работе именно этого механизма защиты, повышению производительности его работы путем увеличения интенсивности обслуживания заявок, времени ожидания в очереди, что позволит уменьшить число пропущенных событий.

Заключение. В ходе работы проведены следующие исследования и получены следующие основные результаты:

1. Для системы защиты информации от несанкционированного доступа составлен перечень выполняемых функций.

2. Проведен анализ основных злоумышленных воздействий на ОС ЭВМ – сканирование файловой системы, подбор пароля, кража ключевой информации, сборка мусора, превышение полномочий, программные закладки.

3. Определены направления исследования СЗИ от НСД с позиций ТМО, представлены основные понятия, принципы и характеристики в данной предметной области.

4. Предложена схема и разработана модель защиты информации. Путем моделирования проведены экспериментальные исследования с использованием разработанной модели.

5. По результатам проведенных экспериментов сделан вывод о том, что наилучшем режимом работы СЗИ является режим с приоритетом заявки с максимальным временем обработки. Однако в случае усиленной нагрузки на четвертый механизм защиты «Регистрация событий безопасности» режим работы может оказаться неустойчивым.

6. При разработке или модернизации СЗИ от НСД признано целесообразным уделять наибольшее внимание механизму защиты «Регистрация событий безопасности», повышению производительности его работы путем увеличения интенсивности обслуживания заявок и времени ожидания в очереди, что позволит уменьшить число пропущенных событий.

СПИСОК ЛИТЕРАТУРЫ:

1. Алиев Т.И. Основы моделирования дискретных систем. – СПб : СПбГУ ИТМО, 2009. – 363 с.

2. Воронов, С.А. Методика оценки эффективности системы защиты информации вычислительных ресурсов / С.А. Воронов, А.Н. Гладков, В.В. Михалев, А.Н. Павлов // Вестник ПНИПУ. – 2015. – № 13. – С.82 – 90.

3. Ослин Б.Г. Моделирование. Имитационное моделирование СМО. – Томск: Изд-во Томского политехнического университета, 2010. – 128 с.

4. Трахтенгерц Э.А. Компьютерные методы реализации экономических и информационных управленческих решений. В 2-х томах. Том 1. Методы и средства. – М.: СИНТЕГ, 2009, 172 с.

5. Бикташев Р.А., Мартышкин А.И. Программный комплекс для расчета вероятностно-временных характеристик стохастических сетей массового обслуживания / Свидетельство о регистрации программы для ЭВМ.

6. Мартышкин А.И. Исследование подсистем памяти информационных систем с буферизацией транзакций на моделях массового обслуживания / И.И. Сальников, М.Ю. Бабич, М.М. Бутаев, А.И. Мартышкин // International Journal of Applied Engineering Research. 2016. Т. 11. № 19. С. 9846-9849.

7. Мартышкин А.И. Программный комплекс для имитационного моделирования диспетчеров задач многопроцессорных систем с использованием приоритетных сетей массового обслуживания / А.И. Мартышкин, Р.А. Бикташев, Н.Г. Востоков // Фундаментальные исследования. – 2014. – № 11-10. – С. 2155-2159.

8. AnyLogic. [Электронный ресурс]. URL: https://www.anylogic.ru/ (дата обращения: 15.09.2020).

9.ГОСТ Р 50922-2006 Защита информации. Основные термины и определения / Федеральное агентство по техническому регулированию и метрологии.

10. Боев В. Д., Исследование адекватности GPSS World и AnyLogic при моделировании дискретно-событийных процессов: Монография. – СПб.: ВАС, 2011. – 404 с.

11. Григорьев В.А., Карпов А.В. Имитационная модель системы защиты информации // Программные продукты и системы – 2005. – №2. – С.26-30.

12. Иванова Т.С. Модель системы защиты от несанкционированного доступа на базе теории массового обслуживания/ Т. С. Иванова // Вестник магистратуры. – 2017. – № 5-2(68). – С.48-49.

13. Никишова А.В., Иванова Т.С. Система мониторинга событий операционной системы – Актуальные вопросы информационной безопасности регионов в условиях глобализации информационного пространства: материалы III Всероссийской науч.-практ. конф., г. Волгоград, 24-25 апреля 2014г. – В.: ВолГУ, 2014. С.123-126.

14. Хисамов, Ф.Г. Проблемы информационной безопасности и устойчивости современных информационных сообществ – Раздел I. Общие вопросы информационной безопасности // Известия ЮФУ. Технические науки. – 2011. – № 12. – С. 8-13.

15. Чечулин А.А., Котенко И.В., Новикова Е.С., Дойникова Е.В. Моделирование атак и механизмов защиты в системах управления информацией и событиями безопасности / Материалы конференции "Информационные технологии в управлении". 2012. Издательство: Концерн "Центральный научно-исследовательский институт "Электроприбор" (Санкт-Петербург). – С. 735-739.

16. Щеглов А. Ю. Защита компьютерной информации от несанкционированного доступа. – СПб: Издательство Наука и Техника, 2004. – 384 с. – ISBN 5-943871-23-3.

17. Банк данных угроз безопасности информации ФСТЭК, 2017 / [Электронный ресурс]. URL: http://www.bdu.fstec.ru/ubi/vul/ (дата обращения: 15.09.2020).

18. Защита информации в компьютерных системах / [Электронный ресурс]. URL: http://protect.htmlweb.ru/attack.htm (дата обращения: 15.09.2020).

19. Способы защиты от несанкционированного доступа / [Электронный ресурс]. URL: http://infoprotect.net/note/zasccityi_ot_nesankcionirovannogo_dostupa/ (дата обращения: 15.09.2020).

20. ГОСТ Р ИСО/МЭК 18045-2013 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий. Введ. 2014-01-07. М.: Стандартинформ, 2014. – 243 с.

Статья поступила в редакцию 04.11.2020
Статья принята к публикации 11.12.2020