УДК 004.056.53 DOI: 10.34759/trd-2020-112-17

Формализация параметров модели адаптивной системы защиты автоматизированной системы управления связью

Филатов В.И.[1*], Бонч-Бруевич А.М.[1], Хохлачев Е.Н.[2***], Борукаева А.О.[1****], Бердиков П.Г.[1*****]**

[1]Московский государственный технический университет им. Н.Э. Баумана, МГТУ им. Н.Э. Баумана, 2-я Бауманская ул., 5, стр. 1, Москва, 105005, Россия

[2]Военная академия Ракетных войск стратегического назначения. имени Петра Великого, ВА РВСН им. Петра Великого, ул. Карбышева, 8, Московская область, Балашиха, Россия

**e-mail: vfil10@mail.ru*

***e-mail: 123andryb@mail.ru*

****e-mail: khokhlach@mail.ru*

*****e-mail: alexbmstu.b@yandex.ru*

******e-mail: palber96@gmail.com*

Статья поступила 24.03.2020

Аннотация

В статье проанализирована теоретическая модель системы защиты автоматизированной системы управления связью (АСУС) от случайных вредоносных воздействий, которые могут быть угрозой для систем управления летательными аппаратами. Определены задачи для реализации системного подхода к решению задачи обеспечения адаптивной защиты АСУС. Рассмотрена имитационная модель для защиты АСУС от вредоносных воздействий, в которой использовались методы теории массового обслуживания. В статье поставлена задача поиска наиболее рациональной организации функционирования АСУС.

Актуальность темы данной работы прежде всего обоснована необходимостью разработать новые методы и способы защиты от вредоносных воздействий на АСУС, используемых для управления летательными аппаратами, например, во избежание перехвата управления.

Ключевые слова: автоматизированная система управления связью, система защиты, вредоносное воздействие, система массового обслуживания, механизм защиты, обслуживающие приборы, имитационное моделирование, теория массового обслуживания.

Согласно официальному подходу [1,2], эффективность системы защиты определяется классом защищенности АСУС. Класс защищенности, в свою очередь, определяет набор механизмов защиты (МЗ), которые должны быть реализованы в АСУС. Такой подход к оценке эффективности защиты информации не позволяет учитывать ни качество самих МЗ, констатируя лишь факт их наличия или отсутствия, ни изменение условий функционирования самой системы защиты. Примерами таких изменений могут служить модификация аппаратной и программной среды, изменение условий информационного взаимодействия объектов и субъектов защиты, числа пользователей системы, возникновение информационных конфликтов в АСУС [3] и т.п.

Количественно защищенность АСУС оценивается, как правило, рядом вероятностных показателей, основным из которых является некий интегральный

показатель [4]. Теоретическая модель системы защиты АСУС от случайных вредоносных воздействий представлена на рисунке 1.

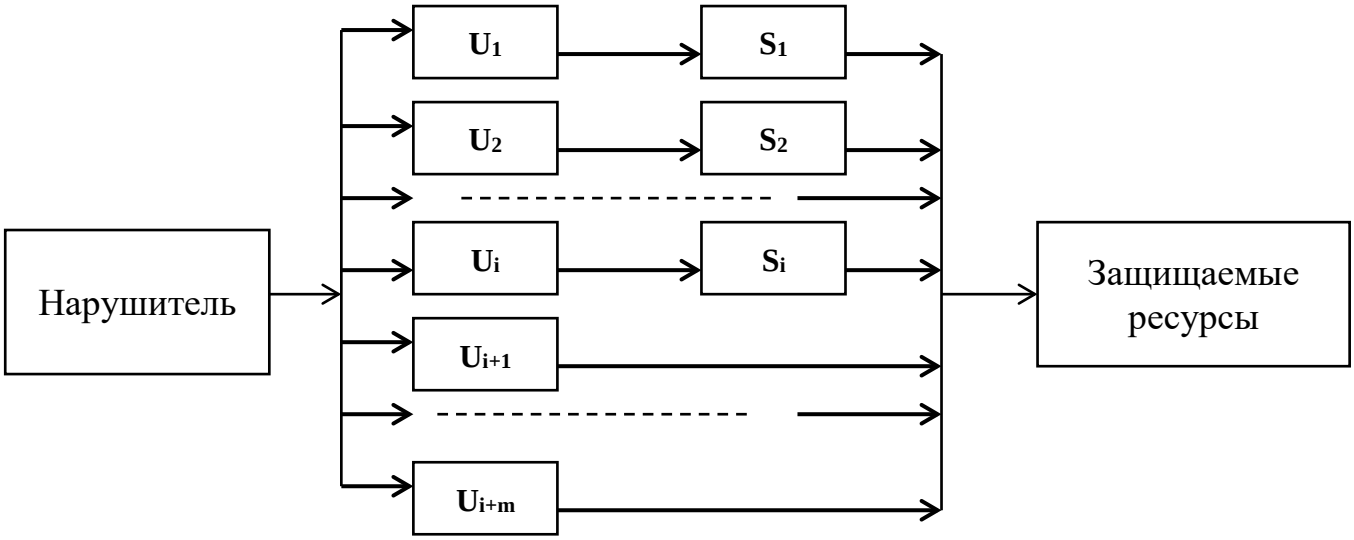

Рисунок 1. Модель системы защиты АСУС

Система защиты представлена здесь в виде сетевой модели, состоящей из некоторого набора средств защиты *Si*. На вход средств защиты поступают потоки вредоносных воздействий, определяемые совокупностью возможных угроз {Ui}. Каждое из средств защиты отвечает за защиту от угрозы определенного типа и использует соответствующий защитный механизм. Его задача состоит в том, чтобы распознать угрозу и предотвратить ущерб от воздействия на АСУС.

В результате функционирования системы защиты исходный поток вредоносных воздействий разрежается, образуя выходной поток. Входные потоки вредоносных воздействий обозначены как Vi(t), i=1,..., n, а потоки нераспознанных (пропущенных) системой защиты – Vi'. Факт неполного закрытия системой защиты всех возможных каналов проявления угроз учитывается отсутствием для m входных потоков средств защиты. Потоки запросов вредоносных воздействий, поступающие

по i-м каналам, разрежаются с вероятностями pi(y), которые зависят от используемого способа обнаружения и блокирования.

На выходе системы защиты образуется выходной поток, являющийся объединением выходных потоков i-средств защиты и потока данных о вредоносных воздействиях, приходящих по m неконтролируемым каналам.

Каждое устройство (механизм) защиты характеризуется вероятностью пропуска вредоносных воздействий – q и, соответственно, вероятностью обеспечения защиты (отражения вредоносных воздействий) p = 1-q.

Воздействия характеризуются вектором интенсивностей $\lambda = \{ \lambda 1, \lambda 2, \ldots \lambda i+m\}$ попыток реализации соответствующих вредоносных воздействий U1…Ui+m.

Очевидно, что для реализации системного подхода к решению задачи обеспечения адаптивной защиты АСУС необходимо комплексное использование методов моделирования систем и процессов информационной и технической защиты каналов. Целями такого моделирования являются поиск оптимальных решений управления МЗ, оценки эффективности использования средств и методов защиты и т.п.

Модель представляет логическое или математическое описание компонентов и функций, отображающих существенные свойства моделируемого объекта или процесса.

Моделирование системы защиты заключается в построении некоторого ее образца, адекватного с точностью до целей моделирования исследуемой системы, и

получения с помощью построенной модели необходимых характеристик реальной системы.

Для реализации комплексного подхода к моделированию системы защиты рассмотрим пример построения имитационной модели по защите АСУС от вредоносных воздействий.

Учитывая схожесть рассматриваемой математической модели с моделями систем массового обслуживания (СМО) и тот факт, что при разработке модели использовались методы теории массового обслуживания [5], представляется целесообразным использовать при построении имитационной модели средства моделирования СМО.

Для описания моделей СМО разработаны специальные языки и системы защиты имитационного моделирования для ЭВМ. Примером общецелевых языков служит широко распространенный язык C#. Кроме того, известно несколько систем имитационного моделирования – GPSS World, System Modeler, AnyLogic.

Как правило, имитационная модель, построенная при помощи подобных средств, состоит из сети блоков, представляющих необходимые действия или задержки транзактов, которые последовательно проходят через блоки. Транзакты представляют собой определенный блок сообщений, которые являются абстрактными подвижными элементами и которые могут моделировать различные объекты реального мира: сообщения, программы, технические средства, людей и т.п. Перемещаясь между блоками модели, транзакты вызывают (и испытывают) различные действия.

Например, блок GENERATE в системе GPSS World [6] создает новые транзакты, воспроизводя рекуррентный поток заявок с требуемым распределением интервалов между ними. Системы защиты имитационного моделирования предоставляют для разработки моделей ряд функциональных блоков, позволяющих имитировать работу обслуживающих приборов, очередей, создание и уничтожение транзактов, условные ветвления и изменения маршрутов прохождения транзактами блоков модели. Транзакты перемещаются в системных времени и пространстве, переходя от одного блока модели к другому. Транзакты возникают и уничтожаются, могут расщепляться и сливаться. Входя в блок, транзакт вызывает определяемую типом блока подпрограмму, которая обрабатывает соответствующее событие. Далее транзакт в общем случае пытается войти в следующий блок. Продвижение продолжается до тех пор, пока очередной блок не удалит транзакт из модели.

Для сбора итоговой статистики используются таймер модельного времени, стандартные атрибуты блоков и параметры транзактов, а также определяемые пользователем переменные, выражения и функции.

В математических моделях сложных объектов, представленных в виде систем массового обслуживания, фигурируют средства обслуживания, называемые обслуживающими приборами (ОП) [19, 21, 22]. Так, в рассматриваемой модели в качестве ОП выступают МЗ, а в качестве транзактов – поступающие запросы о вредоносных воздействиях в АСУС.

Состояние СМО характеризуется состояниями ОП, транзактов и очередей к ОП. Состояние ОП описывается логической переменной, значения которой

интерпретируются как «занят» или «свободен». Переменная, характеризующая состояние транзакта, может иметь значения «обслуживания» или «ожидания». Состояние очереди характеризуется количеством находящихся в ней транзактов.

В целом имитационная модель СМО представляет собой алгоритм, отражающий поведение СМО, то есть изменения состояния СМО во времени при заданных потоках заявок, поступающих на вход системы [7]. Входные потоки заявок определяют внешние параметры СМО. Параметры выходных потоков отражают свойства функционирования системы защиты и являются ее выходными параметрами. В качестве выходных параметров системы защиты можно рассматривать производительность СМО, коэффициенты загрузки оборудования, среднее время обслуживания заявок и т.д.

Имитационное моделирование позволяет исследовать СМО при различных типах входных потоков и интенсивностях поступления заявок на входы, при вариациях параметров ОП. В моделях СМО заявки, приходящие на вход занятого ОП, образуют очереди, отдельные для заявок каждого приоритета. При освобождении ОП на обслуживание принимается заявка из непустой очереди с наиболее высоким приоритетом. К элементам имитационных моделей СМО, кроме ОП, относят также узлы и источники заявок.

Для построения имитационной модели системы защиты при помощи систем имитационного моделирования необходимо соотнести структурные элементы исходной модели с заменяющими их функциональными блоками моделирующих систем [8, 9].

С целью идентификации функциональных блоков имитационной модели представим математическую модель системы защиты, показанную на рисунке 2, в виде концептуальной модели, состоящей из трех основных блоков: «Нарушитель», «СЗИ» и «Защищаемые ресурсы» (рисунок 2).

Рисунок 2. Концептуальная модель системы защиты

«Нарушитель» является первым блоком модели и в общем случае не подвергается входному воздействию. Задача функционирования этого блока – генерация потока (потоков) запросов вредоносных воздействий (транзактов) с заданной интенсивностью λ. Согласно модели нарушителя, разработанной в [3], злоумышленник пытается реализовывать разные угрозы защищенности информации с соответствующими интенсивностями.

Блок «СЗИ» имитирует функционирование системы защиты от вредоносных воздействий (МЗ). Элементы этого блока могут имитировать очереди запросов вредоносных воздействий на входах МЗ, задержки на обслуживание, помехи в каналах передачи данных и команд, выход МЗ из строя (аппаратной части) и т.д. Однако главной задачей функционирования этого блока является отсеивание запросов вредоносных воздействий с определенной (заданной) вероятностью. Разреженный поток запросов вредоносных воздействий на выходе блока «СЗИ» имеет интенсивность μ.

В качестве параметров рассматриваемого процесса используются:

– среднее время функционирования АСУС– $T_п$;

– интенсивность входного потока вредоносных воздействий - λ;

– интенсивность обслуживания потока вредоносных воздействий системой защиты - μ;

– продолжительность ожидания начала обслуживания - $\tau^{ожс}$.

Для соблюдения терминологии, принятой в ТМО, условимся в дальнейшем называть внешние и внутренние пакеты данных о вредоносных воздействиях заявками, а элементы, обеспечивающие защиту информации - приборами обслуживания.

Аналитические методы исследования рассматриваемой здесь системы защиты связаны с исключительно серьезными проблемами, поскольку требуют составления достаточно сложных и громоздких рекуррентных уравнений, общее число которых должно соответствовать количеству все возможных состояний исследуемого процесса. В [10] предлагается другой, более доступный для проведения исследований способ анализа многофазных СМО с приоритетными дисциплинами обслуживания потока заявок. С этой целью вводится так называемая квазирегулярная модель. При этом моделирование каждой фазы процесса осуществляется раздельно с последующим расчетом показателей многофазной СМО через усредненные фазовые показатели. В свою очередь, каждую такую фазу можно рассматривать как многолинейную разомкнутую СМО с многомерным входным потоком требований.

Выбор дисциплины обслуживания произведем, исходя из особенности процесса функционирования системы защиты АСУС от вредоносных воздействий, а также требований по упорядоченности входного потока заявок в соответствии с их приоритетом. Под дисциплиной обслуживания будем понимать правила образования и обработки данных, а под приоритетом – численный показатель, устанавливающий их значимость [13-18]. Специфике АСУС наиболее полно соответствует относительная приоритетная дисциплина без прерывания процесса обслуживания.

Для формализованного представления различных вариантов представления организации защиты АСУС от вредоносных воздействий наилучшим образом подходит символика Кендала-Башарина [9], в которой используются выражения вида A/B/S/q. Они обозначают СМО с S приоритетами обслуживания, количеством приоритетов – q. Индексы A и B обозначают соответственно законы распределения времени между поступлением заявок о вредоносных воздействиях и длительности их обслуживания. В предлагаемой модели будут рассматриваться следующие распределения (вместе с их обозначениями): Г-гамма, R-регулярное, N-нормальное, M-экспоненциальное, E-Эрланга [20].

Общая схема рассматриваемого процесса может быть представлена следующим образом (рисунок 3).

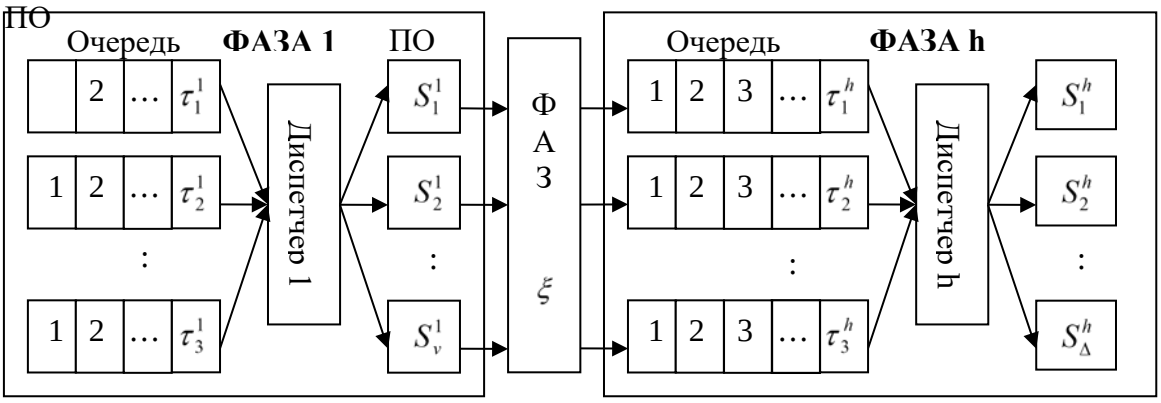

Рисунок 3. Эквивалентная схема многолинейной СМО

В случайные моменты времени в систему поступают заявки, которые в соответствии с установленными для них приоритетами выстраиваются в очередь и обслуживаются S-приборами обслуживания [12]. Количество мест в очереди не одинаково и может изменяться от τ_1 до τ_q. Выбор на обслуживание очередной заявки производит диспетчер в порядке их приоритета так, что из числа находящихся в очереди в освободившийся прибор обслуживания всегда направляется заявка с наименьшим приоритетным номером. Если в прибор обслуживания поступает заявка младшего приоритета, то ее обслуживание будет продолжаться до конца и в том случае, если в систему поступят заявки более высоких приоритетов.

Обозначим через t_j^q - момент поступления в СМО j-й заявки q-го приоритета, $\Delta\tau_j^q = t_j^q - t_{j-1}^q$ - интервал времени между соседними заявками одного приоритета и $\tau_{обсл}^q$ -длительность обслуживания j-й заявки (рисунок 3).

Последовательность случайных величин $\{\Delta\tau_j^q\}$ и $\{\tau_{обсл}^q\}$ будет определять процесс функционирования защиты АСУС в виде СМО. Каждая из этих величин описывается своей функцией распределения вероятностей:

$$A(\Delta\tau_j^q) = P[\Delta\tau_j^q \le \tau_1] \text{ и}$$
$$B(\Delta\tau_{обсл}^q) = P[\Delta\tau_{обсл}^q \le \tau_2],$$

и соответствующей плотностью распределения вероятностей:

$$a(\Delta\tau_j^q) = \frac{dA(\Delta\tau_j^q)}{d\tau} \text{ и}$$
$$b(\Delta\tau_{обсл}^q) = \frac{dB(\Delta\tau_{обсл}^q)}{d\tau},$$

Эти значения являются исходными для расчета основных характеристик СМО, а именно числа заявок, находящихся в системе, загрузки СМО, времени простоя ПО и др.

Среднее время ожидания заявкой q-го приоритета начала обслуживания $-\tau_{ож}^q$ представляет собой промежуток времени с момента появления заявки на входе ПО до момента принятия ее на обслуживание (рисунок 4).

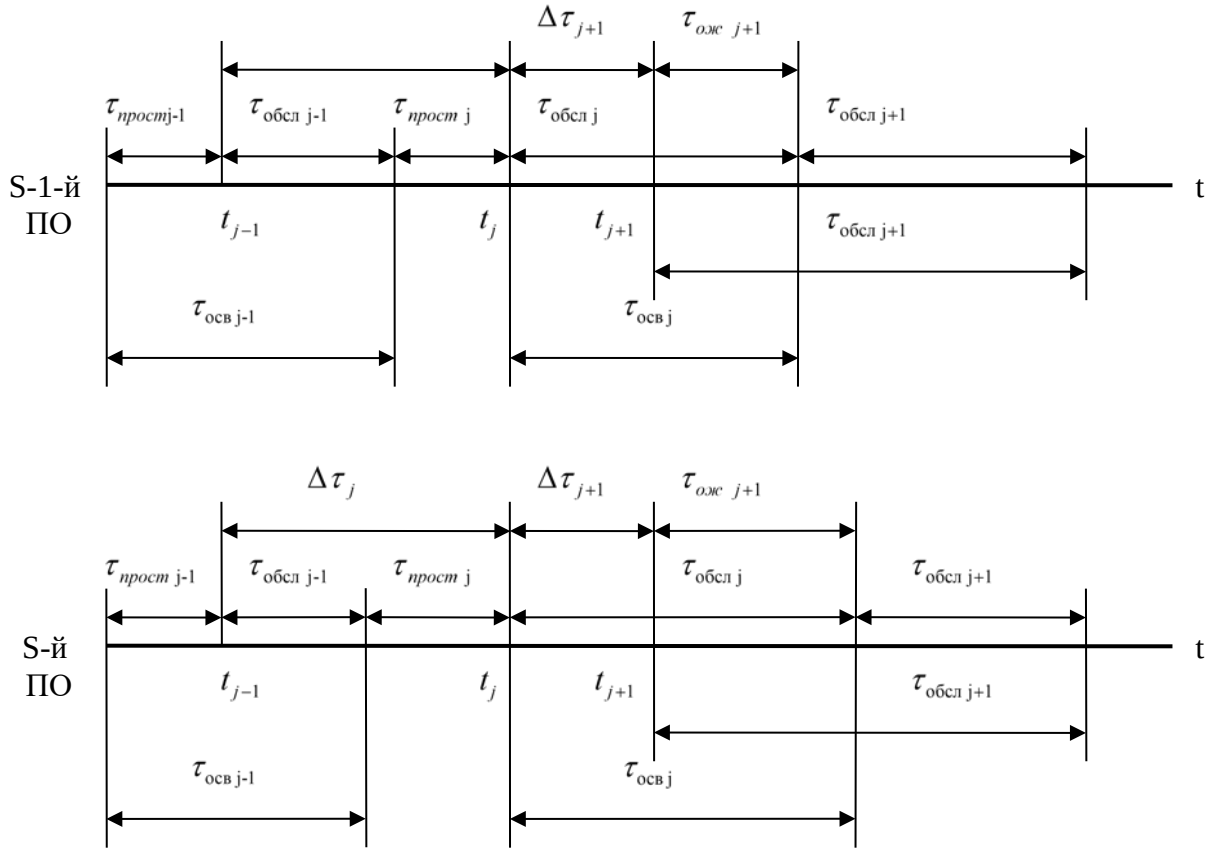

Рисунок 4. Временная диаграмма функционирования адаптивной комплексной системы защиты информации АСУС

Время пребывания заявки в системе $\tau_{пр}^{q}$, а также среднее число заявок, находящихся в системе $\overline{N}_q$, определяется из следующих соотношений:

$$\tau_{пр}^{q} = \tau_{обсл}^{q} + \tau_{ож}^{q}, \quad (1)$$

$$\overline{N}_q = \lambda_q \tau_{пр}^{q}, \quad (2)$$

где λ-интенсивность потока заявок на входе S-го ПО.

Коэффициент загрузки СМО заявками q-го приоритета равен:

$$\rho_q = \frac{\lambda_q \tau_{обсл}}{S} \quad (3)$$

Полная загрузка системы защиты (ρ) представляет собой отрезок времени, в течении которого СМО будет занята обслуживанием всех заявок потока:

$$\rho = \sum_{q=1}^{n} \rho_q \tag{4}$$

Для надежной работы системы защиты АСУС от вредоносных воздействий должна обеспечиваться стационарность процесса ее функционирования. Условие стационарности СМО выполняется, если $0 \le \rho < 1$.

С точки зрения пользователей системы защиты АСУС очень важна своевременность получения результатов на свои запросы. Поэтому, в модели необходимо предусматривать ситуации, связанные с ожиданием ответа на запрос, а также случаи отказа предоставления соответствующих услуг пользователей системы, которые снижают общую эффективность системы защиты АСУС. С этой целью предлагается оценивать такие сбои в работе системы защиты в виде некоторой функции потерь или штрафов за несвоевременное удовлетворение запросов пользователей. В связи с этим, для проведения исследований особенностей поведения СМО в различных режимах ее работы предлагается использовать функцию потерь (штрафов) – W, которая зависит от характеристик входящего потока заявок и параметров АСУС:

$$W = \sum_{q=1}^{n} a_q \lambda_q \tau_{np}^{q}, \tag{5}$$

где:

a_q – штраф за единицу времени пребывания в системе заявки q-го приоритета;

λ_q – интенсивность потока заявок;

n – общее количество всех возможных типов запросов.

Для общей постановки задачи исследований обозначим через $X = (x_1, x_2, ..., x_q, ..., x_n)$ - вектор параметров адаптивной системы защиты АСУС (индекс приоритетов), $q = \overline{1,n}$

$Q = \{q_i\}$, $i = \overline{1,n}$ –вектор параметров управления (индексов приоритетов);

$T(X)$ – продолжительность обслуживания заявок для вектора X;

$T_{доп}$ – допустимая продолжительность обслуживания заявок в АСУС.

Тогда выражение (3.5) можно будет представить в следующем виде:

$$W(X) = a(X)\lambda(X)\tau_{пр}(X), \tag{6}$$

Задачу поиска наиболее рациональной организации функционирования АСУС можно сформулировать следующим образом:

На множестве всех возможных вариантов организации системы защиты АСУС от вредоносных воздействий - Q найти такой вариант ее работы $q^* \in Q$, при котором суммарный штраф за пребывание запросов от вредоносных воздействий в системе - W(X) принимает минимальное значение при условии, что продолжительность их обслуживания не превышает некоторого допустимого значения, т.е.

$$\left.\begin{array}{l} W(X, q^*, T) = \min W(X, q, T) \\ T(q^*) \le T^{доп};\ G \le G^{доп} \end{array}\right\} \tag{7}$$

Для сравнения возможностей различных вариантов организации процессов защиты в АСУС значительно удобнее использовать вместо абсолютного значения функцию штрафов – W относительную величину этого критерия:

$$K^{(i,w)} = W^{(i)} / W^{(w)},$$

Которая дает возможность оценить кратность уменьшения средней величины суммарного штрафа за единицу времени работы системы защиты АСУС при дисциплине обслуживания - w. При фиксированном значении штрафа за пребывание в системе запросов пользователей таким критерием будет выигрыш в эквивалентной производительности от применения i-й дисциплины по сравнению с дисциплиной w, т.е. отношение нагрузок $Э^{(i,w)}$.

$$Э^{(i,w)} = \rho^{(i)} / \rho^{(w)} \quad \text{при} \quad W^{(l)} = W^{(w)}, \tag{8}$$

В таком случае процесс поиска наилучшего варианта организации системы защиты АСУС будет состоять в нахождении таких управляющих параметров приоритетной дисциплины обслуживания, при которых достигается минимум среднего штрафа за пребывание в системе или максимального эквивалентного выигрыша в производительности системы защиты АСУС.

Следует отметить, что множество всех допустимых сочетаний приоритетов описывается множеством $J = (j_1, j_2, ..., j_n)$. Каждая такая подстановка указывает на то, что первый (высший) приоритет предоставляется запросам из потока с номером j_1, второй с номером j_2 и т.д. Причем существование оптимальной

последовательности очевидно, т.к. их общее число конечно и равно n!. Таким образом, задача нахождения оптимального варианта организации адаптивной системы защиты АСУС принципиально может быть решена методом простого перебора всех возможных вариантов. Однако, даже при сравнении небольших значений множества приоритетных групп n применение метода полного перебора нереально. В связи с этим возникает необходимость поиска таких методов решения поставленной задачи, которые позволяют исключить из рассмотрения значительное число неперспективных вариантов. В качестве одного из таких методов предлагается использовать комбинированный алгоритм направленного поиска с наказанием случайностью [13] совместно со статистическими испытаниями. Для практического применения такой сложной комбинации проведения исследований лучше всего подходит метод имитационного моделирования.

Библиографический список

1. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Руководящий документ Гостехкомиссии России от 30.03.1992.

2. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Руководящий документ Гостехкомиссии России от 30.03.1992.

3. Соломатин М.С., Митрофанов Д.В. Модель интеллектуального детектора системы защиты автоматизированной системы управления // Труды МАИ. 2020. № 110. URL: http://trudymai.ru/published.php?ID=112926. DOI: 10.34759/trd-2020-110-16

4. Филатов В.И., Борукаева А.О., Бердиков П.Г. Алгоритм анализа согласованности экспертных оценок параметров аппаратно-программного комплекса автоматизированного рабочего места // Труды МАИ. 2018. № 103. URL: http://trudymai.ru/published.php?ID=100781

5. Бочаров П.П., Печинкин А.В. Теория массового обслуживания. - М.: Изд-во РУДН, 1995. – 529 с.

6. Шрайбер Т.Дж. Моделирование на GPSS. - М.: Машиностроение, 1980. – 592 с.

7. Овчаров Л.А. Прикладные задачи теории массового обслуживания. - М.: Машиностроение, 1969. - 323 с.

8. Клейнрок Л. Теория массового обслуживания. - М.: Машиностроение, 1979. - 432 с.

9. Жожикашвили В.А., Вишневский В.М. Сети массового обслуживания. - М.: Радио и связь, 1988. – 191 с.

10. Балакирский В.Б. Безопасность электронных платежей // Защита информации. «Конфидент». 1996. № 5. С. 47 – 53.

11. Zaitsev M.A., Filatov V.I. and Borukaeva A.O. Analysis of the simulation modeling results of flow of negative impacts on adaptive system to ensure the sustainability of communication system // Journal of Physics: Conference Series, International Conference "High-tech and Innovations in Research and Manufacturing (HIRM-2019)", 6 May 2019, Krasnoyarsk, Russia.

12. Герасименко В.А., Диев С.И., Размахнин М.К. Новые данные о защите информации в автоматизированных системах обработки данных // Зарубежная радиоэлектроника. 1995. № 9. С. 48 – 75.

13. Панин С.Д. Теория принятия решений и распознавания образов. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2017. – 239 с.

14. Грешилов А.А. Математические методы принятия решений. – М.: Изд-во МГТУ им. Н.Э. Баумана, 2006. – 584 с.

15. Вентцель Е.С. Теория вероятностей и её инженерные приложения. – М.: Высшая школа, 2000. – 480 с.

16. Ивченко Г.И., Медведев Ю.И. Введение в математическую статистику. – М.: Изд-во ЛКИ, 2010. – 600 с.

17. Кобзарь А.И. Прикладная математическая статистика. – М.: ФИЗМАТЛИТ, 2006. – 816 с.

18. Орлов А.И. Теория принятия решений. – М.: Изд-во Экзамен, 2005. – 656.

19. Бритвин Н.В., Мешавкин К.В. Анализ алгоритмов управления очередями для улучшения информационного взаимодействия методом сетевого кодирования // Труды МАИ. 2020. № 110. URL: http://trudymai.ru/published.php?ID=112881. DOI: 10.34759/trd-2020-110-14

20. Пантелеев А.В., Лунева С.Ю. Численный метод решения полностью нечетких систем линейных уравнений // Труды МАИ. 2019. № 109. URL: http://trudymai.ru/published.php?ID=111433

21. Голомазов А.В., Смирнов Н.Я., Иосифов П.А. Построение концепции информационной поддержки принятия решений на основе процедур человеко-машинного взаимодействия // Труды МАИ. 2019. № 107. URL: http://trudymai.ru/published.php?ID=107900

22. Голомазов А.В. Метод информационной поддержки принятия решений реализуемый в среде мультиагентной системы // Труды МАИ. 2019. № 106. URL: http://trudymai.ru/published.php?ID=105738

Parameters formalization of adaptive protection system for automated communication control system

Filatov V.I.[1*], Bonch-Bruevich A.M.[1],**

Khokhlachev Y.N.[2*], Borukaeva A.O.[1****], Berdikov P.G.[1*****]**

[1]Bauman Moscow State Technical University, MSTU,

5, bldg. 1, 2-nd Baumanskaya str., Moscow, 105005, Russia

[2]Peter the Great Strategic Missile Troops Academy,

8, Karbysheva str., Moscow region, Balashikha, Russia

**e-mail: vfil10@mail.ru*

***e-mail: 123andryb@mail.ru*

****e-mail: khokhlach@mail.ru*

*****e-mail: alexbmstu.b@yandex.ru*

******e-mail: palber96@gmail.com*

Abstract

he article analyzed the theoretical model of the system for protection of the automated communication control system (ACCS) against accidental hazardous impacts, representing a threat to the aircraft control systems. The tasks for realizing systematic approach to solve the problem of ensuring the ACCS adaptive protection.

The simulation model for the ACCS protection against hazardous impacts, employing the queueing theory, is considered. The article analyzed the properties of simulation modelling systems, namely GPSS World. The article presents also a mathematical model of the protection system and reviews the functions of its components.

The article used Kendal-Basharin representation for formal presentation of various options of the ACCS protection organization against hazardous impacts. Model restrictions,

which represent a function of loss for the untimely users requests compliance were considered

The task of the most rational organization of the ACCS functioning was put forward in the article.

From the performed analytical work the inferences were drawn that it was not rational to use the method of simple sorting of all possible options to obtain the optimal option of the ACCS adaptive protection system. There is a necessity to employ a combined algorithm of the directional search with the penalty of randomness together with static tests.

The topic of this work relevance is stipulated in the first place by the necessity to develop new methods and ways for the ACCS protection from the hazardous impacts, used for the aircraft control, for example, in case of the control interception prevention.

Keywords: automated communications control system, protection system, malware, queue system, protection mechanism, servicing instruments, simulation, queueing theory.

References

1. *Avtomatizirovannye sistemy. Zashchita ot nesanktsionirovannogo dostupa k informatsii. Klassifikatsiya avtomatizirovannykh sistem i trebovaniya po zashchite informatsii. Rukovodyashchii dokument Gostekhkomissii Rossii ot 30.03.1992*. (Automated systems. Protection against unauthorized access to information. Classification of the automated systems and information security requirement. The Guidance document of the State Technological Commission of Russia from 30.03.1992).

2. *Kontseptsiya zashchity sredstv vychislitel'noi tekhniki i avtomatizirovannykh sistem ot nesanktsionirovannogo dostupa k informatsii. Rukovodyashchii dokument Gostekhkomissii Rossii ot 30.03.1992* (The concept of protection aids for computers and automated systems against unauthorized access to information / the Guidance document of State Technological Commission of Russia from 30.03.1992).

3. Solomatin M.S., Mitrofanov D.V. *Trudy MAI*, 2020, no. 110, available at: http://trudymai.ru/eng/published.php?ID=112926. DOI: 10.34759/trd-2020-110-16

4. Filatov V.I., Borukaeva A.O., Berdikov P.G. *Trudy MAI*, 2018, no. 103, available at: http://trudymai.ru/eng/published.php?ID=100781

5. Bocharov P.P., Pechinkin A.V. *Teoriya massovogo obsluzhivaniya* (Queueing theory), Moscow, Izd-vo RUDN, 1995, 529 p.

6. Shraĭber T.Dzh. *Modelirovanie na GPSS* (Modeling with GPSS), Moscow, Mashinostroenie, 1980, 592 p.

7. Ovcharov L.A. *Prikladnye zadachi teorii massovogo obsluzhivaniya* (Applied Problems of Queueing Theory), Moscow, Mashinostroenie, 1969, 323 p.

8. Kleĭnrok L. *Teoriya massovogo obsluzhivaniya* (Queueing theory), Moscow, Mashinostroenie, 1979, 432 p.

9. Zhozhikashvili V.A., Vishnevskiĭ V.M. *Seti massovogo obsluzhivaniya* (Queueing Networks), Moscow, Radio i svyaz', 1988, 191 p.

10. Balakirskii V.B. *Zashchita informatsii. «Konfident»*, 1996, no. 5, pp. 47 – 53.

11. Zaitsev M.A., Filatov V.I. and Borukaeva A.O. Analysis of the simulation modeling results of flow of negative impacts on adaptive system to ensure the sustainability of communication system, *Journal of Physics: Conference Series, International Conference*

"High-tech and Innovations in Research and Manufacturing (HIRM-2019)," 6 May 2019, Krasnoyarsk, Russia.

12. Gerasimenko V.A., Diev S.I., Razmakhnin M.K. *Zarubezhnaya radioelektronika*, 1995, no. 9, pp. 48 – 75.

13. Panin S.D. *Teoriya prinyatiya reshenii i raspoznavaniya obrazov* (Theory of decision – making and pattern recognition), Moscow, Izd-vo MGTU im. N.E. Baumana, 2017, 239 p.

14. Greshilov A.A. *Matematicheskie metody prinyatiya reshenii* (Mathematical methods of decision-making), Moscow, Izd-vo MGTU im. N.E. Baumana, 2006, 584 p.

15. Venttsel' E.S. *Teoriya veroyatnostei i ee inzhenernye prilozheniya* (Law of probability and its engineering applications), Moscow, Vysshaya shkola, 2000, 480 p.

16. Ivchenko G.I., Medvedev Yu.I. *Vvedenie v matematicheskuyu statistiku* (Introduction to mathematical statistics), Moscow, Izd-vo LKI, 2010, 600 p.

17. Kobzar' A.I. *Prikladnaya matematicheskaya statistika* (Applied mathematical statistics), Moscow, FIZMATLIT, 2006, 816 p.

18. Orlov A.I. *Teoriya prinyatiya reshenii* (Decision-making theory), Moscow, Izd-vo Ekzamen, 2005, 656.

19. Britvin N.V., Meshavkin K.V. *Trudy MAI*, 2020, no. 110, available at: http://trudymai.ru/eng/published.php?ID=112881. DOI: 10.34759/trd-2020-110-14

20. Panteleev A.V., Luneva S.Yu. *Trudy MAI,* 2019, no. 109, available at: http://trudymai.ru/eng/published.php?ID=111433

21. Golomazov A.V., Smirnov N.Ya., Iosifov P.A. *Trudy MAI*, 2019, no. 107, available at: http://trudymai.ru/eng/published.php?ID=107900

22. Golomazov A.V. *Trudy MAI*, 2019, no. 106, available at: http://trudymai.ru/eng/published.php?ID=105738