УДК 621.377

А.С. Корсунский, Т.Н. Масленникова, В.Г. Ерышов

ИМИТАЦИОННАЯ МОДЕЛЬ СИСТЕМЫ АНАЛИЗА ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

Корсунский Андрей Сергеевич, *кандидат технических наук, окончил факультет радиосвязи Ульяновского филиала Военного университета связи, адъюнктуру Военной академии связи им. С.М. Буденного. Главный специалист ФНПЦ ОАО «НПО «Марс». Имеет статьи и изобретения в области радиоэлектронной защиты, безопасности связи и информации, а также передачи информации по беспроводным каналам связи информационно-телекоммуникационных систем. [e-mail: aksspb@mail.ru].*

Масленникова Татьяна Николаевна, *кандидат технических наук, окончила радиотехнический факультет Ульяновского политехнического института. Начальник научно-исследовательской лаборатории ФНПЦ ОАО «НПО «Марс». Имеет труды и публикации в области информационного обеспечения автоматизированных систем специального назначения. [e-mail: mars@mv.ru].*

Ерышов Вадим Георгиевич, *кандидат технических наук, окончил Военную академию связи им. С.М. Буденного, докторантуру Военной академии связи. Старший преподаватель кафедры «Общепрофессиональные дисциплины» Военной академии связи. Имеет учебные пособия, статьи и изобретения в области обеспечения электромагнитной совместимости радиоэлектронных средств военного назначения, контроля безопасности связи и информации, а также контроля защищенности информации от ее утечки по техническим каналам. [e-mail: eryshov@mail.ru].*

Аннотация

В статье рассмотрена имитационная модель системы анализа защищенности информации (САЗИ) в автоматизированных системах (АС), обрабатывающих конфиденциальную информацию. Полученные в результате моделирования зависимости могут служить в дальнейшем основой для анализа существующих и синтеза новых САЗИ.

Ключевые слова: система анализа защищенности информации, автоматизированная система, система массового обслуживания, сканер уязвимостей, имитационная модель.

Andrei Sergeevich Korsunsky, *Candidate of Engineering; graduated from the Faculty of Radio-Communications at Ulyanovsk branch of the Military Communications University; finished his post-graduate studies at the Military Communications Academy named after S. Budenny; Chief Specialist at FRPC OJSC 'RPA 'Mars'; author of articles and inventions in the field of radio-electronics protection, communications and information security as well as information transport through wireless channels. e-mail: aksspb@mail.ru.*

Tatiana Nikolaevna Maslennikova, *Candidate of Engineering; graduated from the Faculty of Radio-Engineering of Ulyanovsk Polytechnic Institute; Head of a research-and-development laboratory at FRPC OJSC 'RPA 'Mars'; author of papers and publications in the field of information support of special-purpose computer-aided systems. e-mail: mars@mv.ru.*

Vadim Georgievich Eryshov, *Candidate of Engineering; graduated from Military Communications Academy named after S. Budenny; finished his doctoral studies at the Military Communications Academy; Senior Teacher at the Department of Academic Vocational Disciplines of the Military Communications Academy; author of text-books, articles, and inventions in the field of electromagnetic compatibility of military-purpose radio-electronics facilities, monitoring of communications, and information security as well as monitoring of information security against its leakage through technical channels. e-mail: eryshov@mail.ru.*

Abstract

The article deals with a simulation model of an information security analysis system in computer-aided systems processing the confidential information. Hereafter, the dependences obtained while modeling can form a basis for the analysis of the existing information security analysis systems and for synthesis of new ones.

Key words: information security analysis system, computer-aided system, queuing system, exposure scanner, simulation model.

Введение

В наши дни на современном этапе развития высокотехнологичных отраслей промышленности, информационных технологий наблюдается резкое обострение проблем обеспечения информационной безопасности (ИБ). Все более обостряются противоречия в вопросах обеспечения требуемого уровня защищенности конфиденциальной информации как циркулирующей в АС, информационных вычислительных сетях (ИВС), локальных вычислительных сетях (ЛВС), так и о них. Данные противоречия проявляются, с одной стороны, в обеспечении требуемого уровня безопасности информации, а с другой – бурным развитием и широким внедрением во все сферы деятельности информационных технологий и различного программного обеспечения, всеобщей цифровизацией, в том числе вхождением закрытых ведомственных ИВС в сети связи общего пользования (ССОП), активизацией деятельности промышленного шпионажа, в том числе компьютерного.

Наиболее важную роль для нарушителей ИБ имеет достоверная разведывательная информация (коммерческая тайна, сведения о технологиях, партнерах, продуктах производства и т. д.), получаемая по различным каналам. В этих условиях закономерным является стремление нарушителей обеспечить получение достоверной конфиденциальной информации, в том числе по открытым каналам связи и через сети общего пользования. Немаловажную роль в утечке, разглашении конфиденциальной информации может играть также и внутренний нарушитель безопасности информации – легальный пользователь, администратор АС (ЛВС), зачастую наделенный неограниченными привилегированными правами, который как непреднамеренно, так и преднамеренно может допускать нарушение безопасности информации (НБИ), циркулирующей в ЛВС [1].

Промышленная и экономическая разведка, в том числе и компьютерная, обладает большими потенциальными возможностями по добыванию конфиденциальной информации, циркулирующей в АС, ЛВС, обрабатываемой на объектах информатизации.

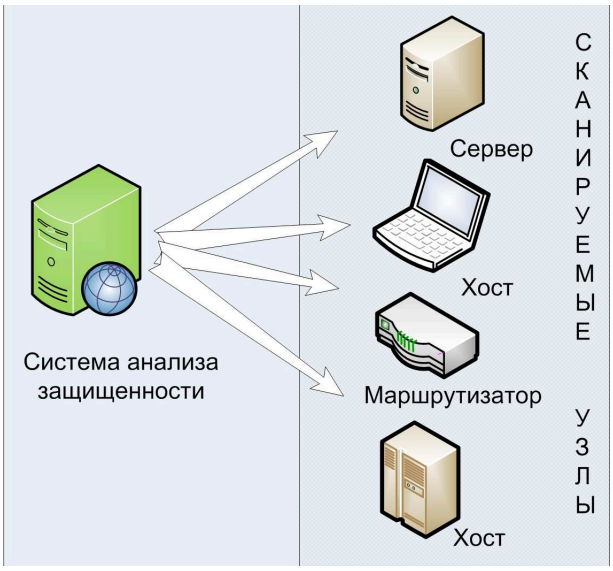


Рис. 1. Архитектура систем анализа защищенности

Исходя из этих условий, актуальным является совершенствование системы защиты информации, которая предполагает создание защитных барьеров (препятствий) для любого несанкционированного вмешательства в процесс функционирования системы, а также для попыток хищения, модификации, ознакомления, разрушения и выведения из строя структурно-функциональных элементов и узлов оборудования, программного и специального программного обеспечения, данных и носителей информации.

Именно поэтому возникает необходимость повышения эффективности САЗИ в АС, обрабатывающих конфиденциальную информацию. Одной из важнейших подсистем системы защиты информации (ЗИ) является САЗИ, предназначенная для защиты от уязвимости ресурсов АС и выработки рекомендаций по их устранению.

Существующие средства и системы анализа защищенности информации в автоматизированных системах

Для анализа защищенности информации и поиска уязвимостей в АС, обрабатывающих конфиденциальную информацию, применяются сканеры уязвимостей.

Сканеры уязвимостей – это программные или аппаратные средства, служащие для осуществления диагностики и мониторинга сетевых компьютеров, позволяющие сканировать сети, компьютеры и приложения на предмет обнаружения возможных проблем в системе безопасности, оценивать и устранять уязвимости.

Сканеры дают возможность проверить различные приложения в системе на предмет наличия «дыр», которыми могут воспользоваться злоумышленники. Также могут быть использованы низкоуровневые средства, такие как сканер портов, для выявления и анализа возможных приложений и протоколов, выполняемых в системе [2–4].

Работу сканера уязвимостей можно разбить на 4 шага:

- обнаружение активных IP-адресов, открытых портов, запущенных операционных систем и приложений;
- составление отчета о безопасности (необязательный шаг);
- определение уровня возможного вмешательства в операционную систему или приложения (может повлечь сбой);
- возможность на заключительном этапе воспользоваться уязвимостью, вызвав сбой операционной системы или приложения.

Существующие сканеры могут быть вредоносными или «дружественными». Последние обычно останавливаются в своих действиях на шаге 2 или 3, но никогда не доходят до шага 4.

Среди сканеров уязвимостей можно выделить:

- сканеры портов;
- сканеры, исследующие топологию компьютерной сети;
- сканеры, исследующие уязвимости сетевых сервисов;
- сетевые черви;
- CGI-сканеры («дружественные» – помогают найти уязвимые скрипты).

В настоящее время на рынке представлен ряд сертифицированных Федеральной службой по техническому и экспортному контролю (ФСТЭК) России программных средств анализа защищенности информации в АС. Например, такие средства, как XSpider 7.7, Internet Scanner, Nessus 4.0, «Ревизор сети», «Сканер-ВС».

Архитектура систем анализа защищенности представлена на рисунке 1.

На основе анализа принципов работы данных систем можно выделить следующие функции САЗИ:

- определение состава программно-аппаратного обеспечения ЛВС;
- анализ и контроль настроек узлов ЛВС;
- выявление уязвимостей серверов и рабочих станций ЛВС;
- анализ защищенности маршрутизаторов и коммутаторов ЛВС;
- формирование перечня рекомендаций администратору безопасности по устранению выявленных уязвимостей;
- возможность подключения новых модулей проверок;
- оповещение администратора безопасности о выявленных уязвимостях;
- генерация отчетов по результатам работы системы с различной степенью детализации.

При этом эти функции определяют набор функциональных требований к САЗИ, таких как:

- всесторонние проверки;
- представление результатов с различной степенью детализации;
- дружественный интерфейс и простота управления;
- многоплатформенность;
- пополнение базы данных уязвимостей;
- поддержка различных политик безопасности;
- функционирование по расписанию;
- наличие базы истории проверок;
- наличие документации, системы подсказок, описания всех обнаруживаемых уязвимостей и способов их устранения;
- наличие механизмов разграничения доступа к своим компонентам и собранным данным;
- наличие сертификата соответствия требованиям ФСТЭК РФ.

Описательная модель САЗИ в АС

Одной из актуальных задач для оценки эффективности САЗИ и разработки требований к таким системам является построение имитационной модели с целью выявления вероятностно-временных зависимостей событий и состояний.

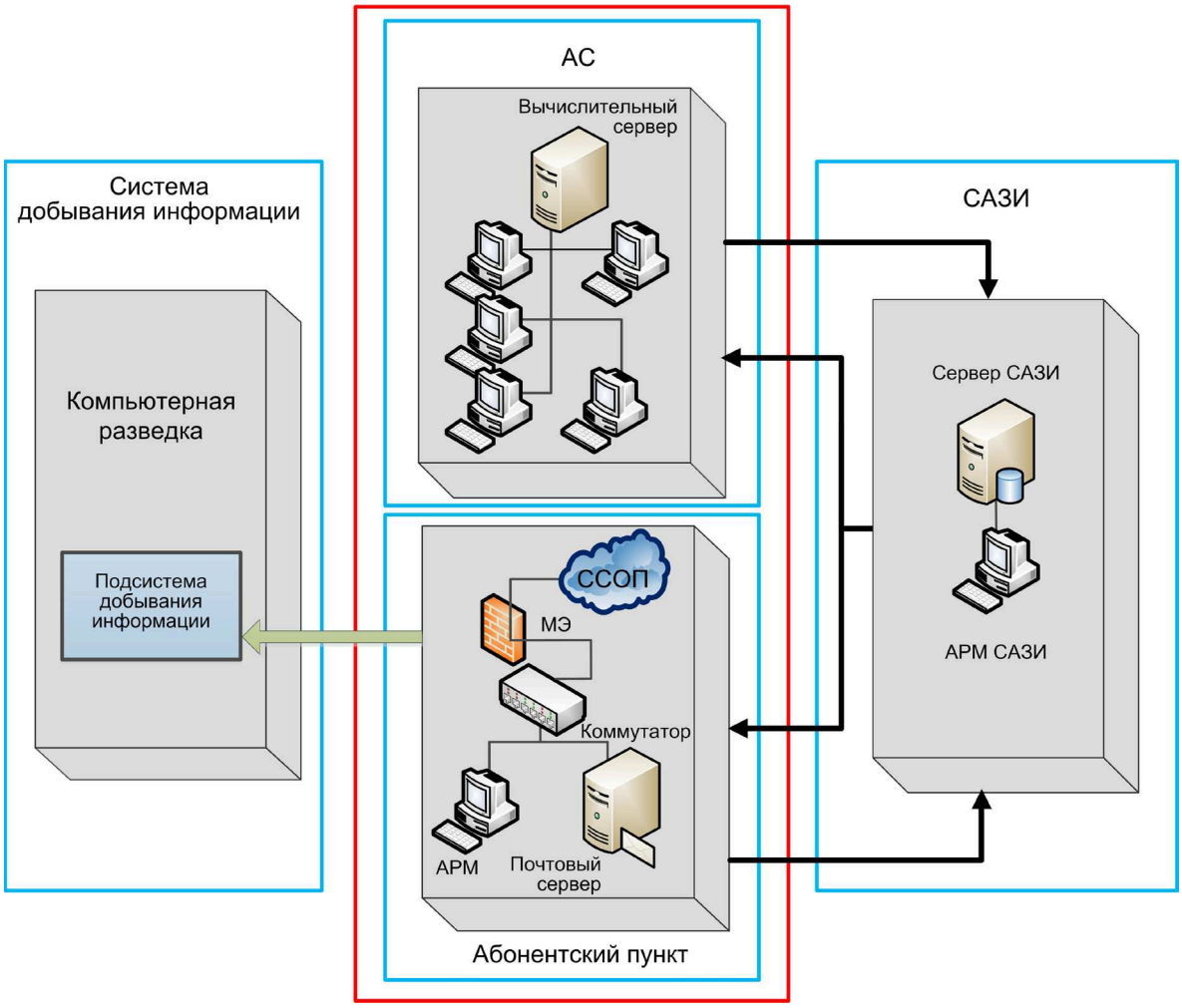


Рис. 2. Описательная модель САЗИ

Анализ показывает, что трудно найти систему ЗИ, удовлетворяющую всем требованиям, но выбрать наиболее эффективную можно.

Описательная модель САЗИ в АС показана на рисунке 2. Она включает в себя АС, абонентский пункт, САЗИ, систему добывания информации, состоящую из подсистемы компьютерной разведки.

Объект САЗИ содержит сервер САЗИ и автоматизированное рабочее место (АРМ) САЗИ: ПЭВМ, которая осуществляет анализ системы и следит за ее работой.

АС состоит из вычислительного сервера, АРМ, принтеров, коммутаторов.

В состав абонентского пункта входят: почтовый сервер, АРМ, межсетевой экран (МЭ), принтеры, коммутатор.

Актуальным является вопрос о выборе целесообразной степени автоматизации процессов в АС, целью которой является повышение производительности САЗИ.

Разработка имитационной модели САЗИ

Модель САЗИ в АС представляет собой имитационную модель, реализованную на основе системы имитационного моделирования AnyLogic.

Работу САЗИ можно отследить на структурной схеме модели, изображенной на рисунке 3. Система ЗИ проводит мониторинг и отслеживает работу АРМ, принимает решения при обнаружении нарушения. Система работает с двумя сегментами: абонентским пунктом и АС.

С сервера САЗИ идут потоки с сообщениями с проверкой АРМ на НБИ (поток В). На АРМ происходит проверка на нарушения, и результаты проверок при мониторинге возвращаются на сервер САЗИ. Это сообщения об успешных проверках (поток А2), которые не выявили ошибок, и НБИ (поток А1).

Данная модель служит как для оценки эффективности системы ЗИ, так и для разработки требований для этой системы. Исходными данными для модели являются: количество АРМ должностных лиц (ДЛ) сети, интервал поступления проверок на НБИ при мониторинге, также времена обработки сообщений как на коммутаторах, так и на сервере, и АРМ ДЛ. Если стоит задача оценить эффективность системы, то исходными данными будут служить вышеперечисленные параметры, при введении которых в результате получим вероятностно-временные зависимости событий. В случае обратной задачи, то есть при разработке требований для системы ЗИ, исходными данными будут являться заданные вероятности и времена, по которым будем искать требования для системы, удовлетворяющие этим данным.

Работу модели можно отследить также с помощью разработанного алгоритма на рисунке 4.

Необходимо отметить, что САЗИ представляет собой замкнутую систему массового обслуживания. Модель САЗИ включает три основные части, представленные на рисунке 5:

- имитация работы АРМ ДЛ;
- имитация обслуживания коммутатором;
- имитация работы сервера системы ЗИ.

Сообщения, циркулирующие в системе, в модели представлены заявками и содержат следующие поля:

- b – содержит данные о сообщении с нарушением, если b=2, то сообщение хранит информацию о НБИ на соответствующем АРМ;
- C – содержит номер АРМ, от которого или на который поступает сообщение;
- d – содержит данные, которые говорят, что это сообщение с проверкой на НБИ на АРМ ДЛ;
- time_v – содержит время поступления сообщения в сеть.

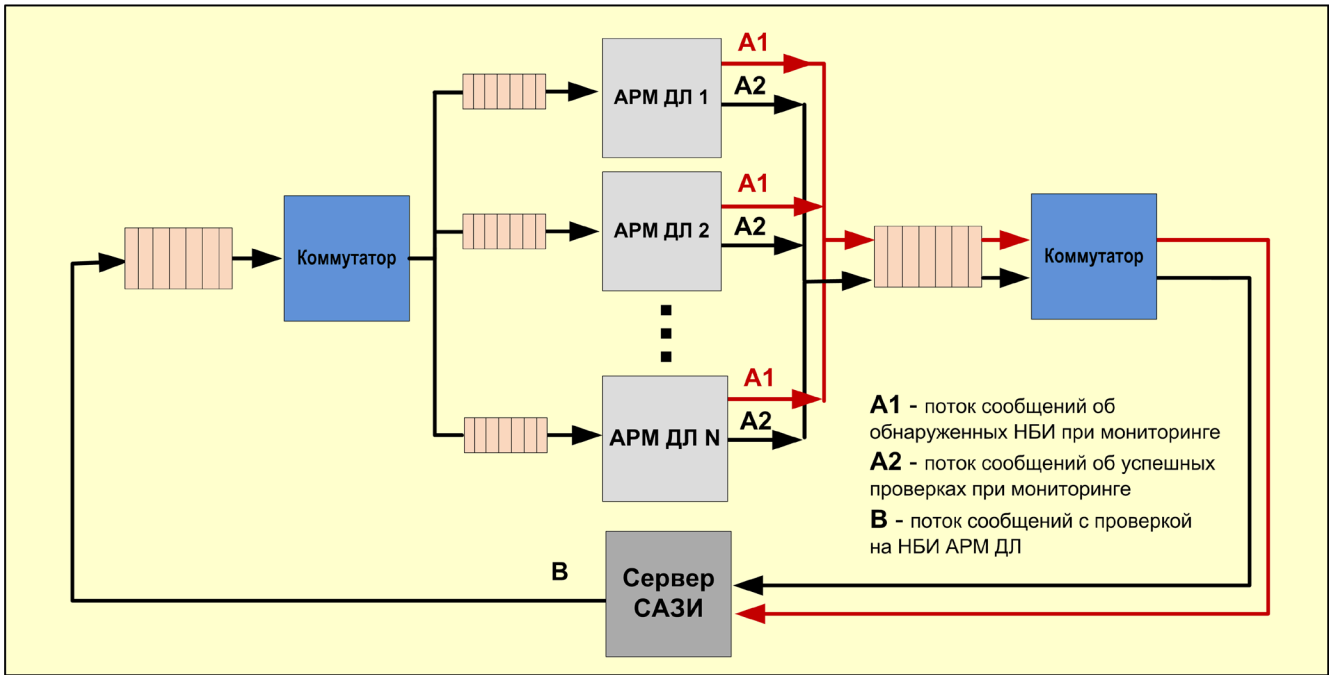


Рис. 3. Структурная схема модели

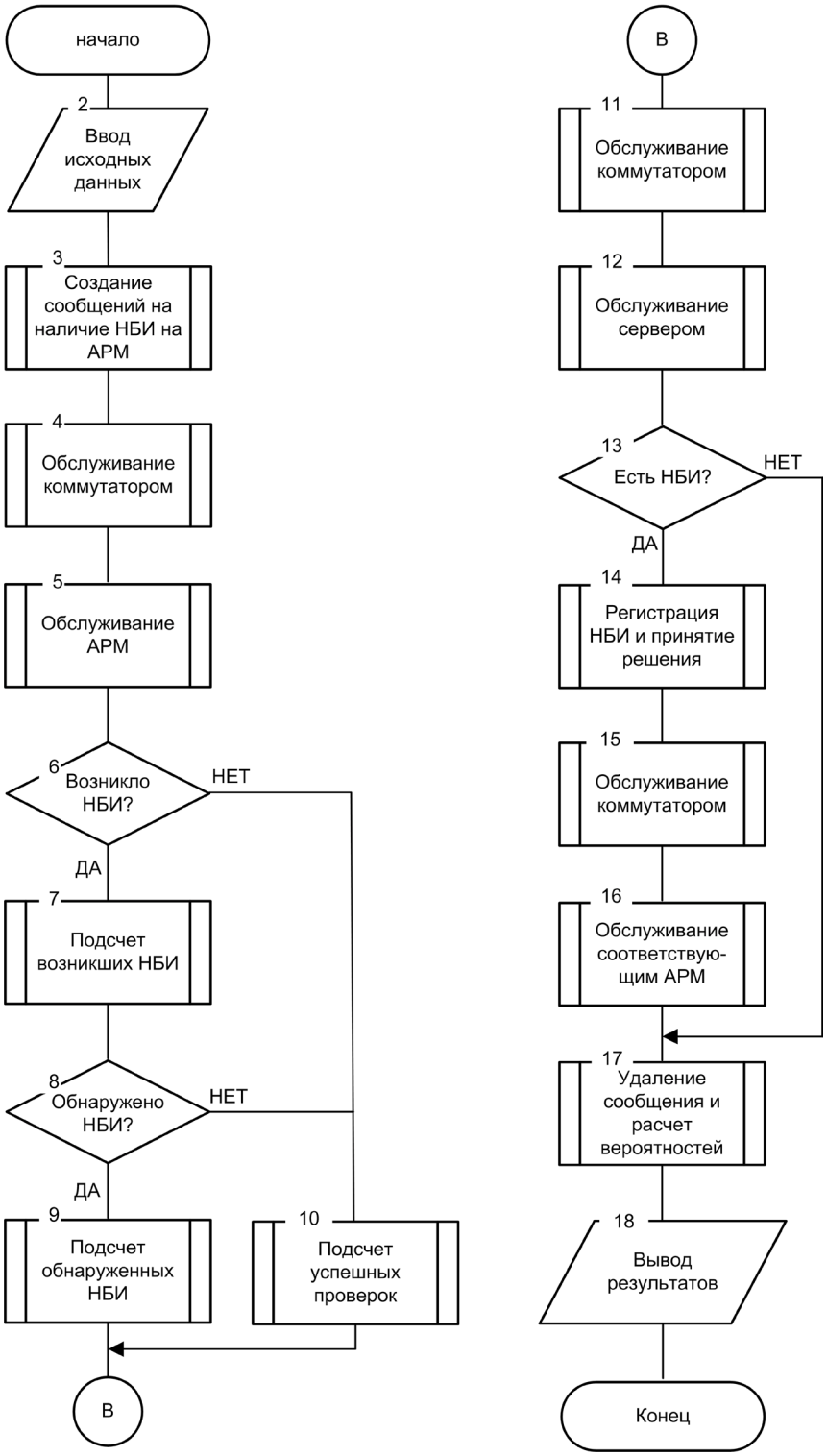


Рис. 4. Алгоритм работы модели

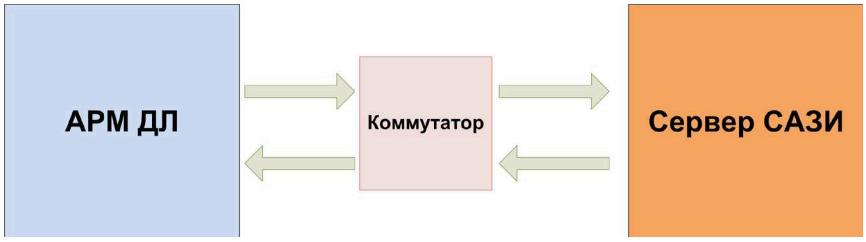


Рис. 5. Концептуальная схема модели САЗИ

Кроме параметров заявок, в модели существуют параметры, не включаемые в поле заявок:

- количество_армов – количество АРМ, контролируемых системой ЗИ;
- емк_ком – емкость коммутатора;
- емк_арм – емкость АРМ;
- емк_сер – емкость сервера;
- Mas[...] – массив целых чисел. Массив содержит число строк по количеству АРМ ДЛ, контролируемых системой ЗИ. В столбцах содержатся данные по каждому АРМ:

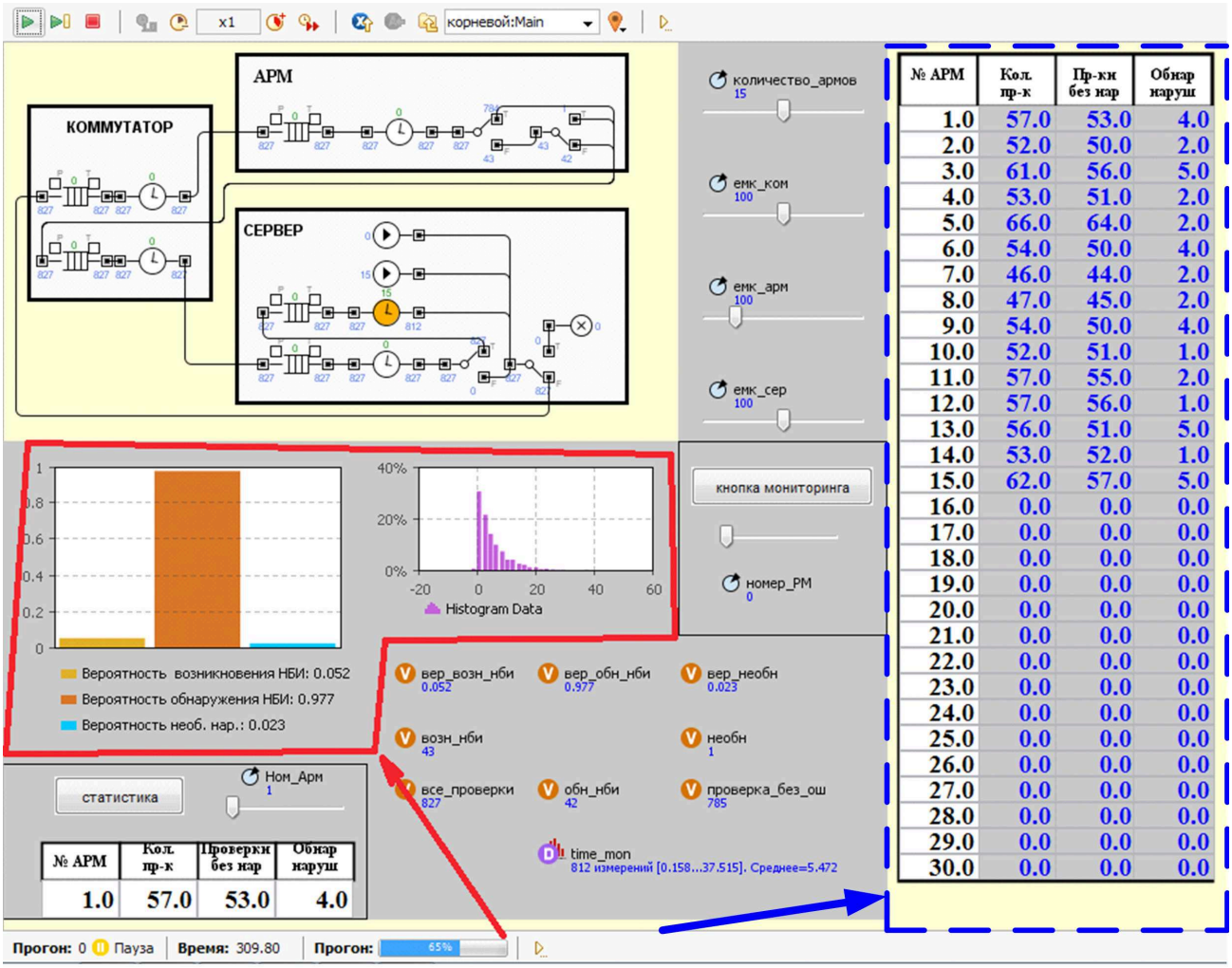
1. Номер АРМ;
2. Количество проверок на НБИ, посланных сервером;
3. Количество успешных проверок;
4. Количество обнаруженных НБИ.

В параметре событие «расчет» рассчитываются вероятности и количество событий в модели:

- вероятность возникновения нарушения:
вер_возн_нар=(возн_нби / все_проверки);
- вероятность необнаружения нарушения:
вер_необн=(необн / возн_нби);
- вероятность обнаружения НБИ на АРМ:
вер_обн_нби=(обн_нби / возн_нби).

Все расчеты вероятностей и подсчеты событий в модели записываются в переменные, представленные на экранной форме рисунка 6 (выделено сплошной линией).

В зависимости от того, какая задача поставлена, оценка эффективности или разработка требований, такие выходные данные и будем искать. Если производится оценка эффективности САЗИ, то выходными данными будут вероятности возникновений и обнаружений нарушений, среднее время мониторинга, количество возникших и обнаруженных нарушений. Все эти данные можно просмотреть с помощью переменных и таблицы в модели. Также вероятности и среднее время мониторинга выводятся на диаграммах, представленных на экранных формах рисунка 6 (выделено пунктирной линией).



№ АРМ	Кол. пр-к	Пр-ки без нар	Обнар наруш
1.0	57.0	53.0	4.0
2.0	52.0	50.0	2.0
3.0	61.0	56.0	5.0
4.0	53.0	51.0	2.0
5.0	66.0	64.0	2.0
6.0	54.0	50.0	4.0
7.0	46.0	44.0	2.0
8.0	47.0	45.0	2.0
9.0	54.0	50.0	4.0
10.0	52.0	51.0	1.0
11.0	57.0	55.0	2.0
12.0	57.0	56.0	1.0
13.0	56.0	51.0	5.0
14.0	53.0	52.0	1.0
15.0	62.0	57.0	5.0
16.0	0.0	0.0	0.0
17.0	0.0	0.0	0.0
18.0	0.0	0.0	0.0
19.0	0.0	0.0	0.0
20.0	0.0	0.0	0.0
21.0	0.0	0.0	0.0
22.0	0.0	0.0	0.0
23.0	0.0	0.0	0.0
24.0	0.0	0.0	0.0
25.0	0.0	0.0	0.0
26.0	0.0	0.0	0.0
27.0	0.0	0.0	0.0
28.0	0.0	0.0	0.0
29.0	0.0	0.0	0.0
30.0	0.0	0.0	0.0

№ АРМ	Кол. пр-к	Проверки без нар	Обнар наруш
1.0	57.0	53.0	4.0

Рис. 6. События в виде таблицы и диаграммы вероятностей

По построенным графикам, представленным на рисунках 7–10, можно пронаблюдать зависимость вероятности возникновения и обнаружения нарушений от количества АРМ и времени всего этапа моделирования, а также проверок на НБИ.

По графикам видно, что с увеличением количества АРМ возрастает количество нарушений, вероятность возникновения НБИ увеличивается, а вероятность обнаружения нарушений уменьшается, но не существенно. Среднее время одной проверки увеличивается при добавлении в сеть очередного АРМ. С ростом времени мониторинга вероятность возникновения НБИ увеличивается, а вероятность обнаружения становится меньше. Для того чтобы увеличить вероятность, нужно изменить интенсивность проверок НБИ.

В случае, если стоит задача разработать требования для САЗИ, исходными данными будут вероятности и количество событий системы, а выходными – количество АРМ, интервалы поступления отчетов пользователей и проверок на НБИ. Эти данные и будут являться требованиями для системы ЗИ.

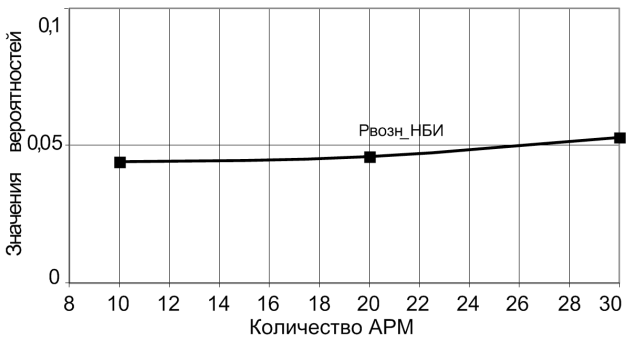


Рис. 7. Зависимость вероятности возникновения НБИ от АРМ

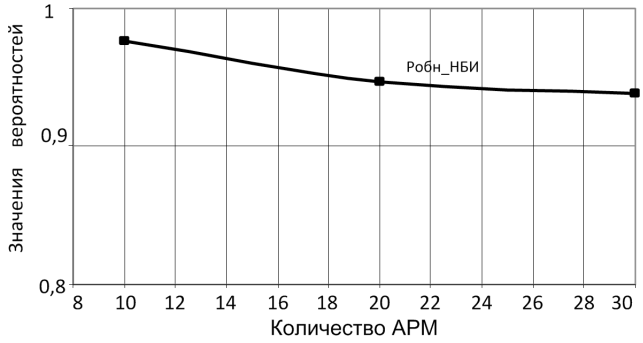


Рис. 8. Зависимость вероятности обнаружения от количества АРМ

Оценка адекватности разработанной математической модели САЗИ в АС

Результаты, полученные в ходе моделирования, дают основание утверждать, что разработанная имитационная модель отражает реальный процесс анализа защищенности информации.

Степень адекватности модели САЗИ в работе оценивается по основным группам показателей, соответствующим основным этапам разработки имитационной модели:

- полноте отображения и точности взаимосвязей основных процессов (экстенсивные показатели);

- глубине и существенности отображения основных факторов (интенсивные показатели);

- достоверности (доказательности) отображения.

В качестве показателя достоверности R используется относительное сокращение среднеквадратической ошибки определения искомого результата, обеспечиваемое применением оцениваемой модели. Для оценки показателя степени достоверности R на основе методов линеаризации и анализа возможных ошибок моделирования получено приближенное $\cong$ выражение, нормированное относительно среднеквадратической ошибки исходных данных:

$$R = 1 - \frac{\sigma}{1 + n_{\text{п}}} - \theta, \qquad (1)$$

где единица характеризует максимальное значение показателя степени достоверности при отсутствии ошибок моделирования; второе слагаемое при $\sigma = 1$ определяет относительную величину ошибки, возникающей из-за ограниченного числа прогонов модели $n_{\text{п}}$ при использовании имитационных моделей; для аналитических моделей эта составляющая погрешности отсутствует, т. е. $\sigma = 0$; третье слагаемое θ – показатель степени неадекватности модели – определяет относительную величину методической ошибки, возникающей из-за неточности учета значимых факторов модели:

$$\theta = \sum_{i=1}^{L} \alpha_i \cdot \beta_i; \qquad \theta \in [0, \infty], \qquad (2)$$

где L – общее количество значимых факторов моделируемого процесса;

α_i – коэффициент значимости i-го фактора:

$$\alpha_i \in [0,1],\ i = \overline{1, L};\ \sum_{i=1}^{L} \alpha_i = 1, \qquad (3)$$

β_i – относительная ошибка учета каждого фактора: $\beta_i \in [0, \infty]$.

Как следует из (1), при $\left(\frac{\sigma}{1 + n_{\text{п}}} + \theta\right) > 1$ величина R принимает отрицательные значения, что свидетельствует о неточности представления моделируемого процесса. Следовательно, для утверждения об адекватности математической модели реальному процессу должно выполняться условие: $R \in [0, 1]$.

При оценке степени достоверности будем учитывать: интенсивность входного потока – λ, интенсивности обслуживания заявок – μ, количество обслуживающих приборов модели – n, т. е. $L = 3$. Положим, что коэффициенты значимости в нашей модели следующие: $\alpha_{\lambda} = 0{,}35$, $\alpha_{\mu} = 0{,}35$, $\alpha_{n} = 0{,}3$.

Относительная ошибка учета каждого фактора:

$$\beta_{\lambda} = \frac{\left| N_{\lambda_{\text{мод}}} - N_{\lambda_{\min}} \right|}{N_{\lambda_{\text{мод}}}}, \qquad (4)$$

где $N_{\lambda_{\text{мод}}}$ – значение входного потока в модели,

$N_{\lambda_{\min}}$ – значение минимального входного потока.

$$\beta_{\lambda} = \frac{\left| 2{,}625 - 1{,}5 \right|}{2{,}625} = 0{,}428.$$

$$\beta_{\mu} = \frac{\left| N_{\mu_{\text{мод}}} - N_{\mu_{\min}} \right|}{N_{\mu_{\text{мод}}}}, \qquad (5)$$

где $N_{\mu_{\text{мод}}}$ – значение выходного потока в модели,

$N_{\mu_{\min}}$ – значение минимального выходного потока.

$$\beta_{\mu} = \frac{\left| 1 - 1 \right|}{1} = 0.$$

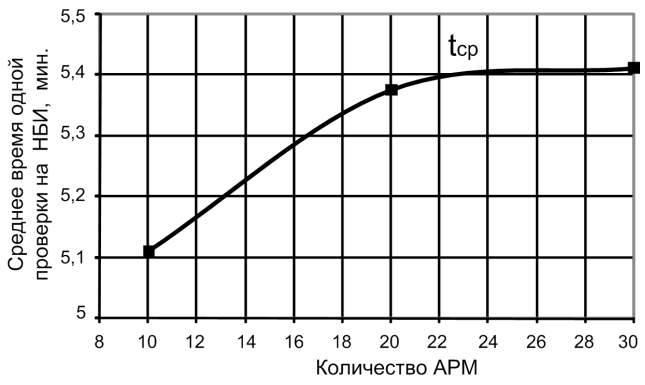


Рис. 9. Зависимость среднего времени проверок от АРМ

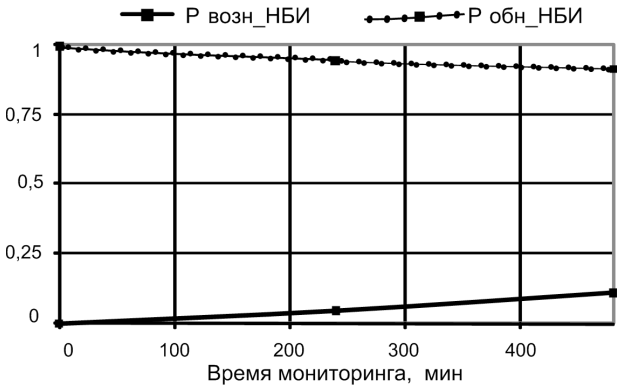


Рис. 10. Зависимость вероятностей от времени мониторинга

$$\beta_n = \frac{|N_{\text{общ}} - n|}{N_{\text{общ}}}, \quad (6)$$

где n – количество обслуживающих приборов в модели,

$N_{\text{общ}}$ – общее количество обслуживающих приборов модели.

$$\beta_n = \frac{|4-2|}{4} = 0,5.$$

Тогда:

$$\theta = 0,428 \cdot 0,35 + 0 \cdot 0,35 + 0,5 \cdot 0,3 = 0,3.$$

То есть $R = 1 - 0 - \theta = 0,7$, что удовлетворяет условию $R \in [0, 1]$, следовательно, можно утверждать, что разработанная имитационная модель адекватно отражает реальный режим функционирования САЗИ.

Выводы

Таким образом, разработанная имитационная модель САЗИ в АС, обрабатывающих конфиденциальную информацию, описанная при помощи инструмента имитационного моделирования AnyLogic, является адекватной, обладает теоретической и практической новизной и дает возможность получать вероятностные и временные зависимости, описывающие состояния исследуемого процесса при варьируемых исходных данных входящих и выходящих событий исследуемого процесса.

Выявленные в предлагаемой модели и полученные в результате проведенного моделирования зависимости послужат в дальнейшем основой для анализа существующих и синтеза новых САЗИ в АС, обрабатывающих конфиденциальную информацию.

СПИСОК ЛИТЕРАТУРЫ

1. Липатников В.А., Малютин В.А., Стародубцев Ю.И. Информационная безопасность телекоммуникационных систем. – СПб. : ВУС, 2002. – 476 с.

2. Лукацкий А.В. Обнаружение атак. – 2-е изд., перераб. и доп. – СПб. : БХВ-Петербург, 2003. – 608 с.

3. Зима В.М. Молдовян А.А., Молдовян Н.А. Безопасность глобальных сетевых технологий. – 2-е изд. – СПб. : БХВ-Петербург, 2003. – 368 с.

4. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы : учебник для вузов. – 2-е изд. – СПб. : Питер, 2003. – 864 с.