Модель системы анализа защищенности информации в автоматизированных системах

Корсунский А.С.
кандидат технических наук

Масленникова Т.Н.
кандидат технических наук, Федеральный научно–производственный центр ОАО «НПО «Марс»

Ерышов В.Г.
кандидат технических наук, Военная академия связи имени С.М. Буденного

Аннотация

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

Ключевые слова: анализ защищённости; эффективность системы; автоматизированная система; конфиденциальная информация; информационная безопасность.

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 обеспечении требуемого уровня защищенности конфиденциальной информации как циркулирующей в АС, информационных вычислительных сетях (ИВС), локальных вычислительных сетях (ЛВС), так и о них. 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 [1].

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

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. Анализ показывает, что трудно найти систему ЗИ, удовлетворяющую всем требованиям, но выбрать наиболее эффективную можно[2-4] .

Описательная модель САЗИ в АС включает в себя автоматизированную систему, 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 рис. 1. Система ЗИ проводит мониторинг и отслеживает работу АРМ, принимает решения при обнаружении нарушения. Система работает с двумя сегментами: абонентским пунктом и АС.

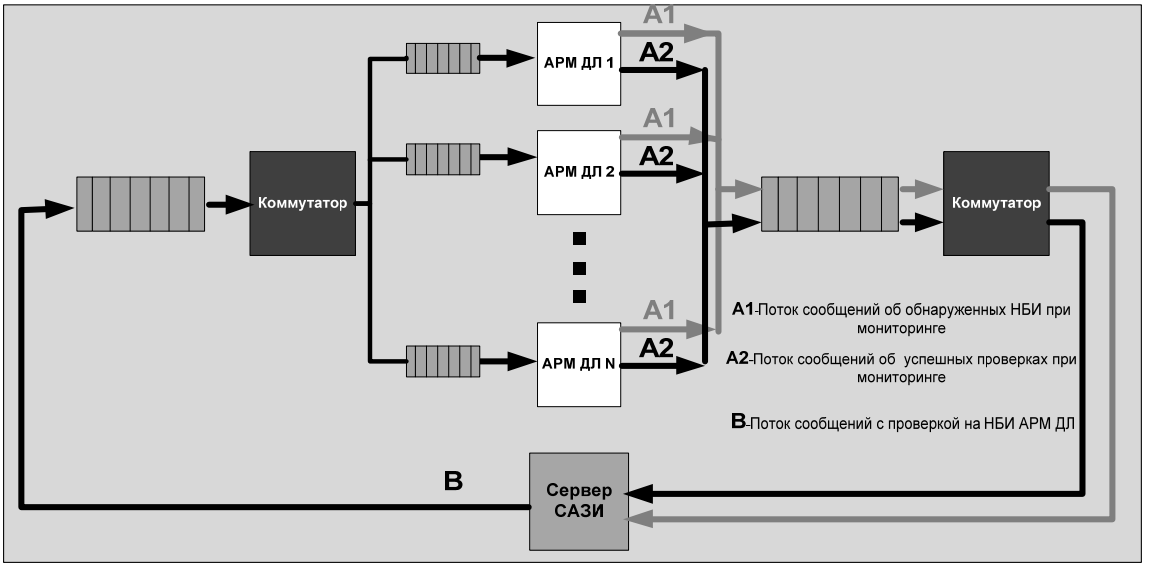

Рис. 1. Структурная схема модели

С сервера САЗИ идут потоки с сообщениями с проверкой АРМ на нарушения безопасности информации (НБИ) (поток В). На АРМ происходит проверка на нарушения, и результаты проверок при мониторинге возвращаются на сервер САЗ. 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.

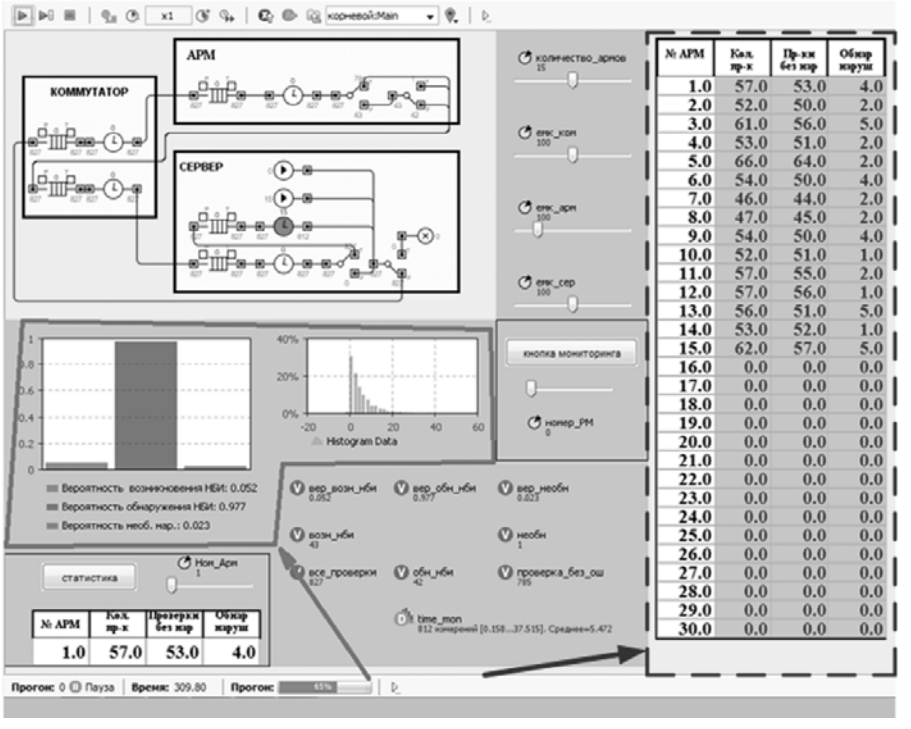

Рис. 2. События в виде таблицы и диаграммы вероятностей

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

– имитация работы АРМ ДЛ;

– имитация обслуживания коммутатором;

– имитация работы сервера системы ЗИ.

Все расчеты вероятностей и подсчеты событий в модели записываются в переменные, представленные на экранной форме рис. 2 (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 рис. 2 (выделено пунктирной линией).

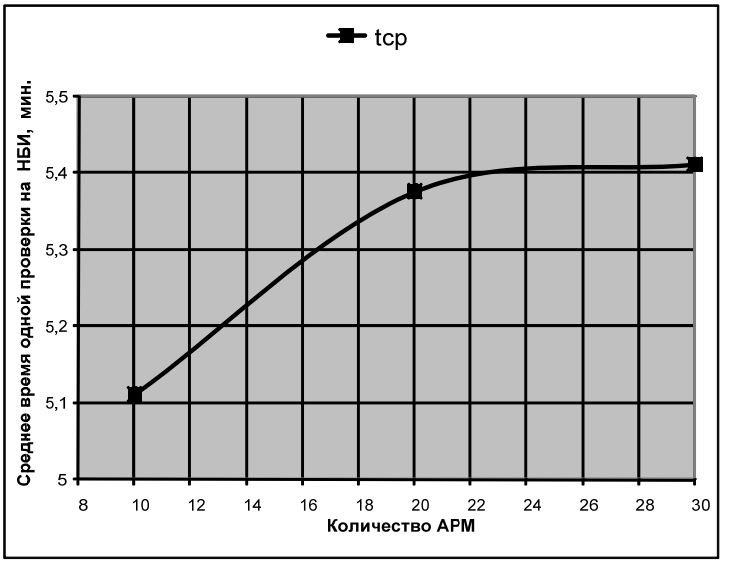

Рис. 3. Зависимость среднего времени проверок от АРМ

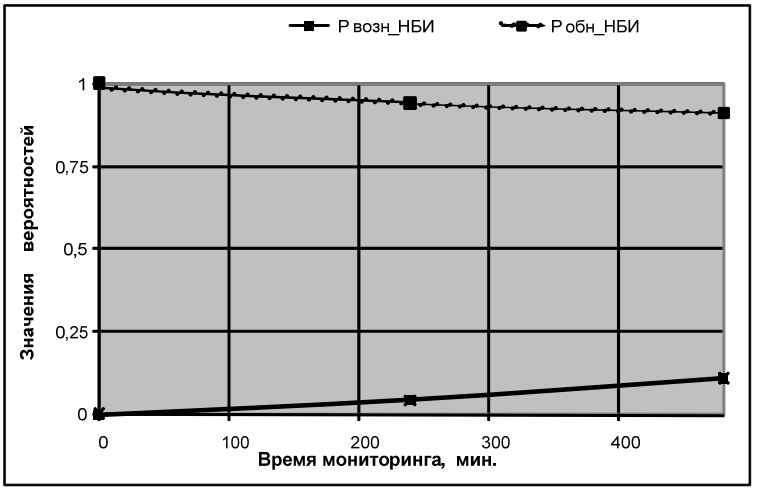

Рис. 4. Зависимость вероятностей от времени мониторинга

По графикам на рис. 3-4 видно, 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 [5].

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.

Заключение

Таким образом, разработанная имитационная модель САЗИ в АС, обрабатывающих конфиденциальную информацию, описанная при помощи инструмента имитационного моделирования AnyLogic 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.

Литература

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.

5. Корсунский А.С., Масленникова Т.Н., Ерышов В.Г. Имитационная модель системы анализа защищенности информации в автоматизированных системах// Автоматизация процессов управления. 2013. № 2 (32). С. 31–36.

Для цитирования:
Корсунский А.С., Масленникова Т.Н., Ерышов В.Г. Модель системы анализа защищенности информации в автоматизированных системах // i-methods. 2015. Т. 7. № 4. С. 30–34.

Model system analysis of information security in automated systems

Korsun A.S.
candidate of technical Sciences
Maslennikova, T.N.
candidate of technical science, Federal research and production center of JSC "NPO "Mars"
Erychov V.G.
candidate of technical Sciences, Military Academy of communications named after S. M. Budenny

Abstract
The article describes a simulation model for system security analysis information.
In the automated systems for various purposes that handle sensitive information. The resulting modeling dependencies can serve later as the basis for analysis of existing and synthesis of new system security analysis information.

Keywords: vulnerability analysis; efficiency of the system; the automated system; confidential information; information security.

References
1. Lipatnikov, V. A., Malyutin V. A., Starodubtsev, Y. I. Information security in the telecommunication systems. SPb.: VUS. 2002. 476 p.
2. Lukatsky A. V. attack Detection. 2-e Izd., Rev. and supplementary SPb. : BHV-Petersburg. 2003. 608 S.
3. Winter M. V. Construction A. Construction N. And. The security of global network technologies. 2-e Izd. SPb.: BHV-Petersburg. 2003. 368 p.
4. Olifer V. G., Olifer N. And. Computer network. Principles, technologies, protocols: textbook for universities. 2-e Izd. SPb.: Peter. 2003. 864 p.
5. Korsun A. S., Maslennikova T. N., Erasov V. G. a Simulation model for system analysis of information security in automated systems// automation of control processes. 2013. No. 2 (32). S. 31–36.

For citation:
Korsun A.S. Maslennikova T.N. Erychov V.G. Model system analysis of information security in automated systems // i-methods. 2015. T. 7. No. 4. Pp. 30–34.