5. Scheglov A.Yu. *Protection of computer information from unauthorized access*. Saint Petersburg: Nauka i Tehnika, 2019, 384 p. (In Russ.)
6. Platonov V.V. *Information security software and hardware*. Moscow: Akademija, 2013, 336 p. (In Russ.)
7. Rjabko B.Ya., Fionov A.N. *Fundamentals of Modern Cryptography for Information Technology Professionals*. Moscow: Nauchnyj mir, 2004, 173 p. (In Russ.)
8. Alferov A.P. et al. *Fundamentals of Cryptography*. Moscow: Gelios ARV, 2002, 480 p. (In Russ.)
9. Kasperskij K. Technique for embedding code in PE files and methods for removing it. *Haker*, 2004, no. 7, 81 p. (In Russ.)
10. Fergjuson N., Shnajer B. *Practical Cryptography*. Moscow: Dialektika, 2018, 432 p. (In Russ.)
11. Vasilev V.L. et al. Digitalization peculiarities of organizations – A case study. *Entrep. Sustain*, 2020, no. 7, pp. 3173–3190.
12. Dudukalov E.V. State regulation of the development of the national segment of the Internet in Russia. *Gosudarstvennoe i munitsipal'noe upravlenie. Uchenye zapiski SKAGS*, 2008, no. 3, pp. 155-164. (In Russ.)
13. Dudukalov E.V. Technological parks in the system of national priorities of post-industrial development of the economy. *Ekonomicheskie i gumanitarnye nauki*, 2014, no. 5 (268), pp. 112–118. (In Russ.)
14. Ignatova T. et al. Assessment of Modern Global Trends in Digital Trade and Finance. *Advances in Economics, Business and Management Research*, 2020, vol. 139, pp. 363–366.
15. Ignatova T.V., Dudukalov E.V., Cherkasova T.P. Knowledge ecosystems and digitalization ratings of national economies. *Tsifrovaja ekosistema ekonomiki*: Materialy VII Mezhdunarodnoj nauchno-prakticheskoj videokonferentsii. Rostov-na-Donu: YuFU, 2020, pp. 391–397. (In Russ.)

Received 20.12.2020

УДК 004.4

РАЗРАБОТКА ИМИТАЦИОННОЙ МОДЕЛИ ДЛЯ ИССЛЕДОВАНИЯ ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЯ В РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМАХ

Ряполова Е.И., Студянникова М.А.
Оренбургский филиал Поволжского государственного университета телекоммуникаций и информатики, Оренбург, РФ
E-mail: studyannikovam@mail.ru

Представлена разработка имитационной модели для исследования поведения пользователя в распределённых информационно-вычислительных системах, разработка языковой модели описания поведения пользователя, описаны права доступа, выявлена ключевая информация для составления профиля нормального поведения пользователя, разработана структурная схема и математическая модель по методу анализа аномального поведения пользователя на основе автоматной модели, которая создается на базе правил несанкционированных действий пользователя и содержит сигнатуры аномального поведения пользователя, описано формальное представление таблицы переходов и последовательности действий пользователя, разработана автоматная модель поведения пользователя, представлена обобщенная модель поведения пользователя как цифрового автомата, а также схема алгоритма действий пользователя. Использованы методы теории информационной безопасности, теории автоматов, теории распознавания образов и теории проектирования вычислительных систем.

Ключевые слова: *аномальное поведение пользователей, мониторинг поведения пользователей, системы информационной безопасности, распределённая информационная система, автоматная модель, сигнатурный подход, имитационная модель*

Введение

Для анализа поведения пользователя необходимо осуществлять анализ ряда его поступков и принимать решение о его аномальности. Нельзя считать неправомерным увеличение сетевого трафика пользователя – для принятия решения о

Таблица 1. Права доступа пользователей

Наименование (тип) ресурса	Права пользователей по доступу к информации		
	Администратор	Пользователь 1	Пользователь n
Ресурс 1	REWAD	REW	RW
Ресурс 2	REWAD	R	R
. . .	REWAD	R	RW
Ресурс *n*	REWAD	REW	R

блокировке его соединения необходимо рассмотреть предшествующие действия и на их основе сделать вывод о нормальности данного трафика или осуществить его блокировку при обнаружении несанкционированного доступа (НСД).

Разработка вербальной модели поведения пользователя

Для пользователя можно выделить ряд ключевых факторов в его поведении, на которые стоит обратить внимание, – это преобладание фото- и видеоматериалов в трафике, большой объем передаваемой информации, использование компьютера в нерабочее время, но осуществление пользователем данного действия еще не говорит о его неправомерности, для выяснения необходимо развернуть всю цепочку предшествующих событий [1].

Согласно теории автоматов, автомат – дискретный преобразователь информации, способный принимать различные состояния, переходить под воздействием входных сигналов из одного состояния в другое и выдавать выходные сигналы, что в общем случае подходит под определение пользователя в информационной системе (ИС), который выполняет ряд операций под влиянием внешнего воздействия; поэтому, если рассматривать пользователя как конечный цифровой автомат, необходимо формализовать его поведение – описать переходы, входные и выходные значения.

Для разработки модели языка поведения пользователя необходимо:

– осуществить классификацию пользователей ИС;

– осуществить классификацию информации, обрабатываемой в ИС;

– определить права пользователей по доступу к информации.

Классификация пользователей необходима для дальнейшей их группировки в группы для назначения им однородных прав для работы с системой, информацию также необходимо классифицировать для объединения в классы доступности для пользователей с различными привилегиями, права пользователей необходимо определять для соотношения групп пользователей и их прав доступа.

В таблице 1 представлен пример классификации пользователей и ресурсов, а также установки соответствий прав доступа пользователей к ресурсам. В данной таблице прокатегорированы пользователи и ресурсы ИС, а также определены права доступа пользователей к ним.

Технология обнаружения атак путем идентификации аномального поведения пользователя основана на следующей гипотезе. Аномальное поведение пользователя (атака или какое-нибудь враждебное действие) часто проявляется как отклонение от нормального поведения. События (поступки) при попытке вторжения отличаются от событий нормальной деятельности и используют различные сигнатуры для определения отклонения от нормального состояния.

Если возможно однозначно описать профиль нормального поведения пользователя, а именно однозначно определить критерии для оценки аномальности поведения, то любое отклонение от них можно идентифицировать как аномальное поведение. Однако аномальное поведение не всегда является атакой, например, одновременную посылку большого числа запросов от администратора сети система защиты может идентифицировать как атаку типа «отказ в обслуживании».

При настройке и эксплуатации систем обнаружения аномального поведения пользователя имеется ряд сложностей: построение профиля нормального поведения пользователя является трудно формализуемой и трудоемкой задачей, требующей от администратора большой предварительной работы; определение граничных значений характеристик поведения пользователя для снижения вероятности появления ошибок первого и второго рода.

Для составления профиля нормального поведения пользователя может использоваться следующая информация:

– обычное число входов в данное время в течение дня, предполагаемое самое раннее время входа, предполагаемая максимальная длительность входа;

Таблица 2. Сигнатуры аномального поведения пользователя

Пользователь	Сигнатуры	10101010	1010	1100
		010100	010	10101010
		000101010	11001010	10101

– предполагаемый тип использования ресурсов, который должна поддерживать данная вычислительная система;

– число IP-адресов, с которыми были взаимодействия, объемы переданного/полученного трафика/пакетов, число клиентских/серверных портов TCP/UDP, на которых были взаимодействия, количество сессий, число уникальных значений типов и кодов ICMP, количество появлявшихся уникальных битов в поле флагов TCP-заголовка и другие;

– попытка запустить или установить программное обеспечение, которое относится к категории системных программ;

– попытка изменения процесса загрузки ОС или внесение изменений в BIOS;

– создание новых разделов на диске;

– установка драйвера;

– попытка добавить нового пользователя в системе или изменить уже имеющегося;

– попытка загрузки операционной системы в безопасном режиме;

– действия, направленные на заполнение анкет, регистрацию на неизвестном сайте с вводом личных/конфиденциальных данных, например вводом паспортных данных;

– работа в Internet через прокси-серверы или использование программного обеспечения для гарантирования анонимности;

– частота чтения и записи некоторых файлов, число отказов на запросы чтения или записи некоторых файлов и другие параметры доступа к файлам.

Технология обнаружения аномалий ориентирована на выявление новых типов атак. Аномалия может быть вызвана неисправностью оборудования или же некорректной работой сетевых сервисов и поддерживающих их систем. Это делает возможным использование таких систем для осуществления аудита сети. В разрабатываемой программе по данному методу анализа аномального поведения пользователя на основе автоматной модели будет создана база правил несанкционированных действий пользователя, которая будет содержать сигнатуры аномального поведения пользователя, с которыми будет сравниваться текущее состояние пользователя и, соответственно, даваться разрешение на выполнение / невыполнение текущих действий пользователя, пример базы сигнатур аномального поведения пользователя показан в таблице 2.

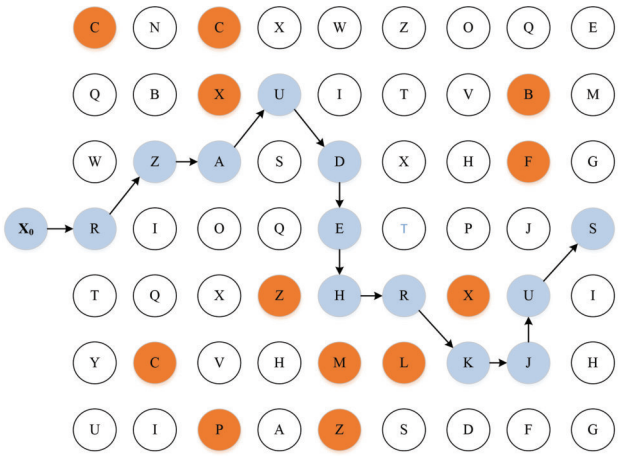

Рисунок 1. Формальное представление таблицы переходов и последовательности действий пользователя

Анализ поведения пользователя осуществляется путем поиска запрещенных сигнатур в таблице переходов, таким образом осуществляется анализ распределенной цепочки действий пользователя, а не тривиальной прямой последовательности. Также возможен режим контроля действий пользователя, когда действия пользователя анализируются по таблице переходов путем ее сравнения с эталонной, при появлении переходов, не описанных в эталонной таблице переходов, переход будет блокироваться.

На рисунке 1 показаны формальное представление таблицы переходов и последовательность действий, которые совершил пользователь (маршрут обозначен указателями), при этом пользователь осуществляет только разрешенные для него переходы, запрещенные переходы отмечены в виде наиболее темных (красных) блоков [7].

Для выполнения одной и той же операции возможно использовать несколько методов, например, для отправки электронного письма можно воспользоваться веб-браузером или почтовой программой, текст письма вводить непосредственно в веб-браузере, почтовой программе или скопировать заранее подготовленный текст из текстового редактора.

Поэтому для описания одного и того же действия необходимо использовать несколько сигна-

тур, описывающих разные алгоритмы достижения цели. Число вариантов выполнения операции напрямую зависит от квалификации пользователя. Так, пользователь с низким уровнем квалификации для решения поставленной задачи будет совершать множество ненужных переходов, совершать ошибки при вводе данных, и все в течении продолжительного периода времени. Пользователь среднего уровня квалификации знает один или два метода решения поставленной задачи, операции выполняет с меньшим количеством ошибок и за меньший период времени. Пользователь высокого уровня квалификации знает несколько методов решения поставленной задачи, редко совершает ошибки, выполняет задачи за короткий промежуток времени.

Распознавание запрещенных действий пользователя основано на методе эталонов. В качестве базы эталонов используется предварительно составленная база сигнатур, полученная из кодов состояний таблиц выходов и переходов пользователя, сравнение осуществляется с текущей таблицей выходов и переходов пользователя.

Разработка и исследование автоматной модели поведения пользователя

Алгебраическая теория автоматов представляет собой ветвь теории систем. В приложениях автомат оказывается наиболее подходящим объектом для моделирования действия ряда логических элементов, когда не удается непосредственно воспользоваться вычислительными системами. Автомат будет адекватной моделью реального электронного устройства, когда для последнего правильно введено абстрактное понятие «состояния».

Абстрактный автомат – это математическая идеализация реального объекта или явления, реагирующего на различные входные возмущения [2]. Автомат $A = \{Q, X, Y, \delta, \lambda\}$, имеет:

– конечное множество состояний $Q = \{q_1, ..., q_k\}$;

– конечный входной алфавит $X = \{x_1, ..., x_m\}$;

– конечный выходной алфавит $Y = \{y_1, ..., y_n\}$.

Действия автомата определяются:

– функцией переходов $\delta : Q \times X \rightarrow Q$;

– функцией выходов $\lambda : Q \times X \rightarrow Y$.

В качестве основной модели была выбрана модель Гогена – Мезигера. Согласно этой модели, система может при каждом действии переходить из одного разрешенного состояния только в несколько других. Субъекты и объекты в данной модели защиты разбиваются на группы – домены. Переход системы из одного состояния в другое выполняется только в соответствии с так называемой таблицей разрешений, в которой указано, какие операции может выполнять субъект, например из домена C над объектом из домена D. В данной модели при переходе системы из одного разрешенного состояния в другое используются транзакции, что обеспечивает общую целостность системы [4; 5].

Разработанный метод реализует анализ поведения пользователя, базируясь на автоматной модели Гогена – Мезигера, где каждый поступок пользователя представляется в виде состояния автомата, при этом система при каждом действии может переходить из одного разрешенного состояния только в несколько других, но в отличие от базовой модели проверяется корректность перехода не только по данным из текущего состояния, а из всей предыстории действий пользователя.

Следует отметить, что данный метод не является заменой существующих методов противодействия НСД, а дополняет их, работая в комплексе – повышает защищенность информационной системы от НСД, путем анализа и предотвращения аномального поведения пользователя.

Метод анализа аномального поведения пользователя на основе автоматной модели: универсален – применяется для защиты как от внешних, так и от внутренних нарушителей; для принятия решения о разрешении или запрещении последующих действий пользователя анализируются все предыдущие действия (состояния) пользователя, если для анализа недостаточно данных, то пользователю необходимо выполнить ряд дополнительных действий либо повторить предыдущие; обучаем – в процессе работы создаются базы сигнатур разрешенных и запрещенных состояний; скрытность работы – пользователь не замечает анализа и фиксации своих действий в системе; удобен в использовании – не накладывает на пользователя выполнение дополнительных длительных операций; незначительное потребление ресурсов системы при мониторинге поведения пользователя.

В разрабатываемом подходе в отличие от классической модели Гогена – Мезигера для контроля действий пользователя учитывается не одно его последнее действие, а вся цепочка действий пользователя. Таким образом выявляется запрещенное действие, состоящее из нескольких операций, которые при поэлементной проверке являются разрешенными [3].

Для создания базы эталонов, шаблонов поведения необходимо учитывать особенности пользователя, работающего с системой. Ручной ввод и составление сигнатур поведения пользователей –

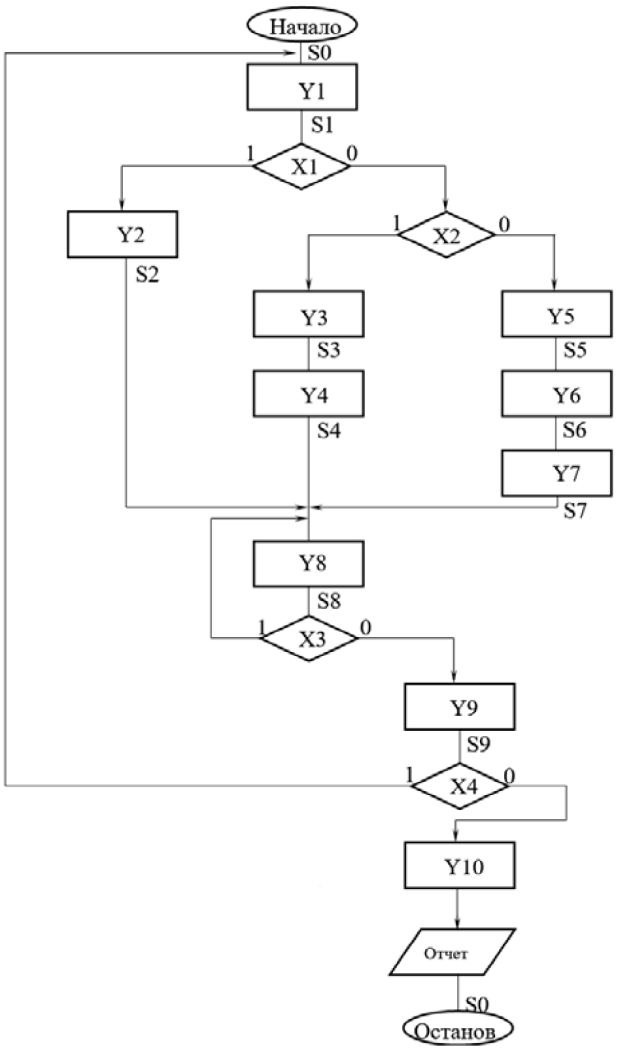

Рисунок 2. Описание поведения пользователя (обобщенная схема алгоритма действий пользователя)

сложный и трудоемкий процесс, в ходе которого возникают ошибки. Для устранения данной проблемы в разрабатываемом подходе используется самообучающаяся система с учителем. При настройке системы мониторинга система записывает все действия пользователя, определяет основные алгоритмы выполнения задач, администратор проверяет данные действия, выявляет запрещенные переходы, и на основе данной выборки создается база эталонов.

Пользователь для осуществления какой-либо операции в системе выполняет определенный алгоритм действий (совершение операций, ввод данных, выполнение условий, вывод данных), данный алгоритм описан согласно теории автоматов и представлен в виде обобщенной схемы управляющего цифрового автомата – см. рисунок 2, в ней указаны все его состояния, входные и выходные значения, что наглядно демонстрирует поведение пользователя как работу цифрового автомата.

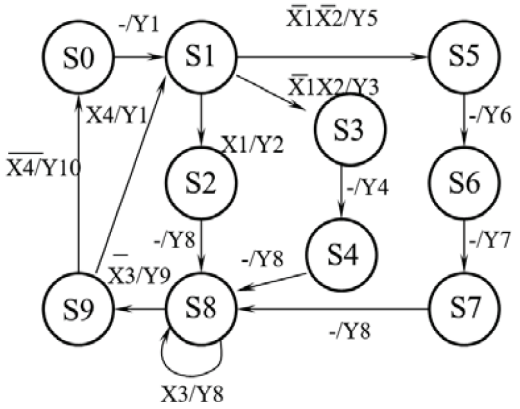

Рисунок 3. Описание поведения пользователя (граф переходов действий пользователя)

При этом алгоритм имеет разветвленную структуру, блоки операций, выбора, условия и вывода. Для обработки алгоритма действий пользователя построен граф переходов – см. рисунок 3, где указана взаимосвязь всех состояний автомата и условияй, при каких входных и выходных значениях осуществляются переходы от одного состояния к другому [2].

В таблицах 3 и 4 показано представление значений функций перехода и выхода, в данных таблицах хранится основная база данных разрешенных действий пользователя, по ним будет осуществляться непосредственный мониторинг его поведения.

Состояние пользователя очень сложно точно описать как состояние цифрового автомата ввиду невозможности формализации состояний человеческого мозга и всех факторов, оказывающих на него воздействия для принятия того или иного решения. Поэтому в данной работе рассматриваются состояния цифрового автомата, достаточно полно отображающие действие пользователя в целом.

В таблице 5 представлены коды состояния цифрового автомата. Для создания базы эталонов, шаблонов поведения необходимо учитывать особенности пользователя, работающего с системой. Согласно разработанному алгоритму, сначала осуществляется регистрация действий пользователя, далее анализ зарегистрированных действий, согласно предварительно составленной базе правил, и в конце принимается решение о разрешении или запрещении входящей последовательности действий пользователя.

При этом осуществляется декомпозиция цепочки действий пользователя, цепочка разбивается на элементарные составные части, далее составляются сочетания этих поступков по времени поступления, и осуществляется сравнительный анализ цепочки действий пользователя с сигнату-

Таблица 3. Таблица переходов

$x_j \backslash a_j$	a_0	…	a_n
x_1	$\delta(a_0, x_1)$	…	$\delta(a_n, x_1)$
…	…	…	…
x_m	$\delta(a_0, x_m)$	…	$\delta(a_n, x_m)$

Таблица 4. Таблица выходов

$x_j \backslash a_j$	a_0	…	a_n
x_1	$\lambda(a_0, x_1)$	…	$\lambda(a_n, x_1)$
…	…	…	…
x_m	$\lambda(a_0, x_m)$	…	$\lambda(a_n, x_m)$

Таблица 5. Кодирование состояний цифрового автомата

№	Состояние ЦА	Код состояния ЦА
1	S0	0000
2	S1	0001
…	…	…
n	Sn	1001

Таблица 6. Принцип сравнения сигнатур по методу эталонов

Сигнатуры действий пользователя	База сигнатур (эталоны)	Анализ сигнатуры действий пользователя	Разрешить действие	Запретить действие
(0111)(0011)(1000)	(0111)	(0111)	(0111)	-
	(0111)(0011)	(0111)(0011)	(0111)(0011)	-
	…..	(0111)(0011)(1000)	-	(0111)(0011)(1000)
	(0000)(1111)(0111)			

рами из базы правил, в случае нахождения совпадений цепочка действий пользователя относится к запрещенным и дальнейшие намерения пользователя блокируются.

В таблице 6 представлен принцип определения запрещенных действий пользователя. На вход поступают сигнатуры действий пользователя, далее они сравниваются с базой сигнатур, при нахождении несовпадений действие пользователя запрещается.

Обобщенная модель поведения пользователя (ПП) в виде цифрового автомата может быть представлена как

$$A = \{S, s_0, X, Y, \delta, \lambda\},$$

где S – текущее технологическое состояние системы, обусловленное действиями пользователя; s_0 – начальное состояние системы; X – входной алфавит действий пользователя; Y – выходной алфавит реакций системы на действия пользователя; $\delta(s, x)$ – функция перехода системы; $\lambda(s, x)$ – функция выходов системы.

Для осуществления определенной операции в системе пользователь выполняет некоторый алгоритм действий (совершение операций, ввод данных, выполнение условий, вывод данных), данный алгоритм описан согласно теории автоматов и представлен на рисунке 4 в виде обобщенной схемы управляющего цифрового автомата, отображающего действия пользователя.

Представленная математическая модель описывает все входные и выходные значения подсистемы мониторинга автоматной модели контроля поведения пользователя.

На рисунке 5 представлена структурная схема данной системы, согласно которой подсистема мониторинга контролирует все входные и выходные значения пользователя и системы, ведет отчет по их работе, оказывает воздействие на систему для осуществления разрешенных переходов согласно таблице выходов и переходов. Пользователь выполняет действие над системой под вилянием предыдущих действий, выполненных над ней.

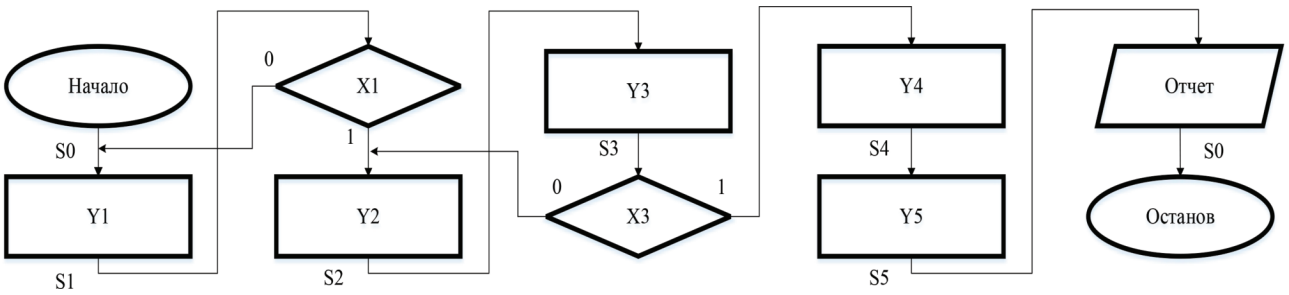

Рисунок 4. Схема алгоритма действий пользователя

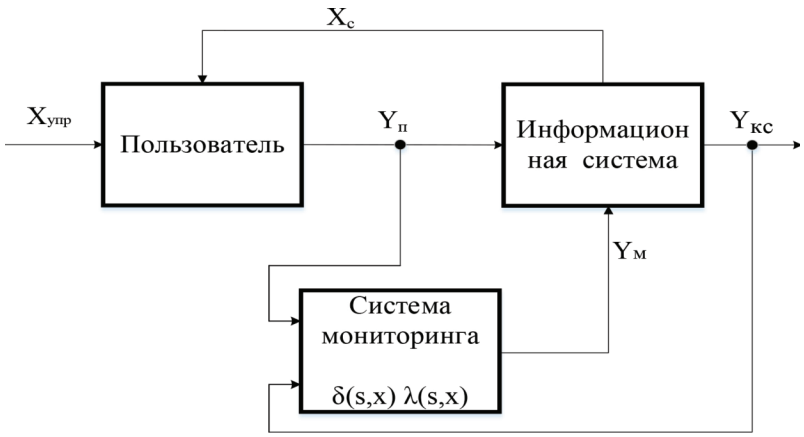

Рисунок 5. Структурная схема автоматной системы контроля ПП

Рисунок 6. Классификация действий пользователя в сигнатурном подходе

Система выполняет действия пользователя только в случае разрешения подсистемы мониторинга. Контроль осуществляется по предварительно составленной таблице выходов и переходов. На рисунке 5 $X_{упр}$ – управляющее воздействие на пользователя; $X_с$ – воздействие системы на пользователя; $Y_п$ – действие пользователя на систему; $Y_м$ – реакция системы мониторинга на действия пользователя; $Y_{кс}$ – реакция системы на действие пользователя (результат работы системы). Классификация действий пользователя в сигнатурном подходе представлена на рисунке 6.

В зависимости от типа поведения и действий пользователя (см. рисунок 5) система способна адекватно реагировать на его действия. Если пользователь выполняет поставленные ему задачи без каких-либо отклонений – система не вмешивается; в случае когда пользователь намерен совершить запрещенное действие – система заблокирует действия пользователя и уведомит администратора об инциденте; в случае когда пользователь не совершает запрещенных переходов, но и не может решить поставленную задачу – система подсказывает пользователю последующие переходы системы для выполнения задачи.

Заключение

Таким образом, для анализа поведения пользователя была разработана модель языка поведения пользователя, для построения которой необходимо: осуществить классификацию пользователей ИС, провести классификацию информации, обрабатываемой в ИС, определить права пользователей по доступу к информации, составить таблицу переходов и выходов для всех пользователей.

Распознавание запрещенных действий пользователя основано на методе эталонов. В качестве базы эталонов используется предварительно составленная база сигнатур, полученная из кодов состояний таблиц выходов и переходов пользователя, сравнение осуществляется с текущей таблицей выходов и переходов пользователя. При этом в отличие от классического подхода применения сигнатур, в котором в качестве сигнатур используются уникальные признаки объекта, в нашем подходе сигнатурами в таблице переходов обозначены все возможные состояния системы (запрещенные и разрашенные).

Контроль осуществляется путем сравнения сигнатур, при этом сравнение осуществляется поэлементно и путем сравнения нескольких или всех сигнатур с эталоном, то есть анализируется не только одно действие пользователя, а последовательность его действий. Для ускорения процесса контроля действий пользователя применяется прогнозирование переходов пользователя от одного действия к другому. Согласно эталонной таблице выходов и переходов, пользователю для выполнения определенной операции необходимо выполнить ряд заранее определенных действий, поэтому при выполнении пользователем текущих действий заранее известно, какой переход должен осуществить пользователь.

Для выполнения одной и той же операции возможно использовать несколько методов, например, для отправки электронного письма можно воспользоваться веб-браузером или почтовой программой, текст письма вводить непосредственно в веб-браузере, почтовой программе или скопировать заранее подготовленный текст из текстового редактора.

Поэтому для описания одного и того же действия над системой необходимо использовать несколько сигнатур, описывающих разные алгоритмы достижения цели. Количество вариантов выполнения операции напрямую зависит от квалификации пользователя. Так, пользователь с низким уровнем квалификации для решения поставленной задачи будет совершать множество ненужных переходов, совершать ошибки при вводе данных, и все в течение продолжительного периода времени. Пользователь среднего уровня квалификации знает один или два метода решения поставленной задачи, операции выполняет с меньшим количеством ошибок и за меньший период времени. Пользователь высокого уровня квалификации знает несколько методов решения поставленной задачи, редко совершает ошибки, выполняет задачи за короткий промежуток времени.

Описывая все разрешенные переходы пользователя в системе, мы создаем шаблоны безопасного поведения пользователей по классической модели информационной безопасности Гогена – Мезигера, согласно которой система может при каждом действии переходить из одного разрешенного состояния только в несколько других, что переход системы из одного состояния в другое выполняется только в соответствии с таблицей разрешений, в которой указано, какие операции может выполнять субъект над объектом.

Литература

1. Мигаль В.П. Сигнатурный подход к анализу и обеспечению безопасности системы «человек-машина» // Открытые информационные и компьютерные интегрированные технологии. 2014. № 65. С. 152–159.
2. Глушков В.М. Абстрактная теория автоматов // Успехи мат. наук. 1961. Т. 16, № 5. С. 3–62.
3. Галатенко А.В. Автоматные модели защиты компьютерных систем // Интеллектуальные системы. 2015. Т. 4, Вып. 3–4. С. 214–271.
4. Модель Гогена-Мезигера // Основные модели информационной безопасности. URL: http://256bit.ru/besopas/indefik119.html (дата обращения: 20.12.2020).
5. Архитектура безопасности. Модели безопасности ее оценки. Общие критерии // Пятифан. URL: http://5fan.ru/wievjob.php?id=24411 (дата обращения: 20.12.2020).
6. Корниенко А.А., Слюсаренко И.М. Системы и методы обнаружения вторжений: современное состояние и направления совершенствования. URL: http://citforum.ru/security/internet/ids_overview (дата обращения: 20.12.2020).
7. Сигнатурный анализ и обнаружение аномалий // Защита информации в компьютерных сетях. URL: https://sites.google.com/site/andallseti/home/sistemy-obnaruzenia-atak (дата обращения: 20.12.2020).
8. Система обнаружения вторжений «Форпост». URL: http://www.razgovorodele.ru/security/safety09/safe-work07.php (дата обращения: 20.12.2020).
9. Источники угроз информационной безопасности России. URL: http://textbooks.studio/uchebnik-mejdunarodnie-otnosheniya/istochniki-ugroz-informatsionnoy-bezopasnosti.html (дата обращения: 20.12.2020).
10. Компьютерная безопасность. Требования к функциональной безопасности системных средств и средств защиты информации // Информационные технологии в бизнесе.

URL: http://www.npp-itb.spb.ru/publications/1.html (дата обращения: 20.12.2020).
11. Угрозы информационной безопасности // Википедия. URL: https://ru.wikipedia.org/wiki/Угрозы_информационной_безопасности (дата обращения: 20.12.2020).

Получено 01.04.2021

Ряполова Елена Ивановна, к.п.н., доцент, кафедра математических и естественно-научных дисциплин (МиЕНД) Оренбургского филиала Поволжского государственного университета телекоммуникаций и информатики (ОФ ПГУТИ). 460022, Российская Федерация, г. Оренбург, ул. Пролетарская/Юркина, 249/76. Тел. +7 906 843-86-00. E-mail: ananeva_ei@mail.ru

Студянникова Марина Александровна, к.п.н, доцент, зам. директора по научно-методической работе ОФ ПГУТИ. 460022, Российская Федерация, г. Оренбург, ул. Пролетарская/Юркина, 249/76. Тел. +7 905 819-44-82. E-mail: studyannikovam@mail.ru

SIMULATION MODEL FOR RESEARCHING THE USER BEHAVIOR IN DISTRIBUTED INFORMATION COMPUTER SYSTEMS

Ryapolova E.I., Studyannikova M.A.
Orenburg Branch of the Volga State University of Telecommunications and Informatics, Orenburg, Russia
E-mail: studyannikovam@mail.ru

This article presents the development of a simulation model for the study of user behavior in distributed information computing systems, the development of a language model for describing user behavior, access rights are described, key information for compiling a profile of normal user behavior is revealed, a structural diagram and a mathematical model based on the method of analyzing abnormal user behavior are developed. based on an automaton model, which is created on the basis of the rules of unauthorized user actions, and contains signatures of anomalous user behavior, a formal representation of the transition table and a sequence of user actions is described, an automaton model of user behavior is developed, a generalized model of user behavior as a digital automaton is presented, as well as an algorithm diagram user actions. The study used the methods of information security theory, automata theory, pattern recognition theory and the theory of computing systems design.

Keywords: *abnormal user behavior, monitoring of user behavior, information security systems, distributed information system, automaton model, signature approach, simulation model*

DOI: 10.18469/ikt.2021.19.2.09

Ryapolova Elena Ivanovna, Orenburg Branch of the Povolzhskiy State University of Telecommunications and Informatics, 249/76, Proletarskaya Street / Yurkina Street, Orenburg, 460022, Russian Federation; Associate Professor of Mathematical and Natural Science Disciplines Department, PhD in pedagogy, Associate Professor. Tel. +7 906 843-86-00. E-mail: ananeva_ei@mail.ru

Studyannikova Marina Aleksandrovna, Orenburg Branch of the Povolzhskiy State University of Telecommunications and Informatics, 249/76, Proletarskaya Street / Yurkina Street, Orenburg, 460022, Russian Federation; Deputy Director of scientific and methodological work, Associate Professor of Mathematical and Natural Science Disciplines Department, PhD in Pedagogy, Associate Professor. Tel. +7 905 819-44-82. E-mail: studyannikovam@mail.ru

References

1. Migal' V.P. Signature approach to the analysis and security of the «man-machine» system. *Otkrytye informatsionnye i komp'juternye integrirovannye tehnologii*, 2014, no. 65, pp. 152–159. (In Russ.)

2. Glushkov V.M. Abstract automata theory. *Uspehi mat. nauk*, 1961, vol. 16, no. 5, pp. 3–62. (In Russ.)
3. Galatenko A.V. Automatic models of computer systems protection. *Intellektual'nye sistemy*, 2015, vol. 4, no. 3, pp. 214–271. (In Russ.)
4. The Gauguin-Meziger model. Basic information security models. URL: http://256bit.ru/besopas/indefik119.html (accessed: 20.12.2020). (In Russ.)
5. Security architecture. Security models for its assessment. General criteria. Pyatifan. URL: http://5fan.ru/wievjob.php?id=24411 (accessed: 20.12.2020). (In Russ.)
6. Kornienko A.A., Sljusarenko I.M. Intrusion detection systems and methods: current state and areas of improvement. URL: http://citforum.ru/security/internet/ids_overview (accessed: 20.12.2020). (In Russ.)
7. Signature analysis and anomaly detection. *Information protection in computer networks*. URL: https://sites.google.com/site/andallseti/home/sistemy-obnaruzenia-atak (accessed: 20.12.2020). (In Russ.)
8. Intrusion detection system «Forpost». URL: http://www.razgovorodele.ru/security/safety09/safework07.php (accessed: 20.12.2020). (In Russ.)
9. Sources of threats to information security in Russia. URL: http://textbooks.studio/uchebnik-mejdunarodnie-otnosheniya/istochniki-ugroz-informatsionnoy-bezopasnosti.html (accessed: 20.12.2020). (In Russ.)
10. Computer security. Requirements for the functional safety of system tools and information protection tools. Information technology in business. URL: http://www.npp-itb.spb.ru/publications/1.html (accessed: 20.12.2020). (In Russ.)
11. Information security threats. Wikipedia. URL: https://ru.wikipedia.org/wiki/Ugrozy_informatsionnoj_bezopasnosti (accessed: 20.12.2020). (In Russ.)

Received 01.04.2021

НОВЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 658.5

РАЗРАБОТКА ИМИТАЦИОННОЙ МОДЕЛИ ДЛЯ СОВЕРШЕНСТВОВАНИЯ БИЗНЕС-ПРОЦЕССА ЭНЕРГЕТИЧЕСКОЙ КОМПАНИИ

Богданова Е.А., Бородина О.Ю.
Поволжский государственный университет телекоммуникаций и информатики, Самара, РФ
E-mail: helen.bogdan@mail.ru, oksana.borodina.2000@bk.ru

В статье приведено обоснование применения статистического имитационного моделирования как одного из методов обработки больших объемов данных, что позволяет существенно повысить эффективность принимаемых решений в различных сферах деятельности. Рассматриваются вопросы, связанные с совершенствованием бизнес-процесса по установке прибора контроля потребления электроэнергии на примере ПАО «Россети Волга». Приведена блок-схема бизнес-процесса, его детальное описание, а также проведен анализ рассматриваемого бизнес-процесса в интересах имитационного моделирования, в ходе которого выделены наиболее значимые для моделирования данного процесса случайные величины. Для создания модели были определены законы распределения всех выделенных случайных величин, разработан моделирующий алгоритм (приведен в статье) и план эксперимента с моделью. В статье приведен результат эксперимента, проведенного на имитационной модели.

Ключевые слова: *статистическое имитационное моделирование, бизнес-процесс, случайные величины, алгоритм моделирования, совершенствование бизнес-процесса*

Введение

В условиях непрерывного развития перед каждой организацией на первый план становится вопрос грамотного и эффективного управления предприятием, что представляет собой достаточно трудный и кропотливый процесс, требующий определенной компетентности в области рационального сочетания разнообразных методов