УДК 004.942

ИССЛЕДОВАНИЕ ПРИМЕНЕНИЯ ПРОГНОЗНОЙ МОДЕЛИ В ПРОЦЕССЕ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ

Шишкин Владимир Михайлович
К.т.н., доцент, старший научный сотрудник
Санкт-Петербургский институт информатики и автоматизации РАН,
199178, Россия, Санкт-Петербург, 14 линия, дом 39, e-mail: vms@iias.spb.su
Колесников Константин Евгеньевич
Специалист, Главное управление Министерства юстиции Российской Федерации
по Санкт-Петербургу, 190000, Санкт-Петербург, Исаакиевская пл., д.11,
e-mail: kolesnikovib@gmail.com

Аннотация. В работе показана возможность дифференциальной модели противоборства (ДМП) для предоставления прогноза развития инцидентов безопасности в информационных системах. Предложены методика и технология её взаимодействия с системами класса SIEM. Проведены эксперименты по имитации работы дифференциальной модели противоборства с потоком данных от SIEM системы, показаны некоторые результаты и пояснения.
Ключевые слова: система дифференциальных уравнений, противоборство, информационная безопасность, SIEM, моделирование.

Цитирование: Шишкин В.М., Колесников К.Е. Исследование применения прогнозной модели в процессе управления безопасностью // Информационные и математические технологии в науке и управлении. 2018. № 4 (12). С. 96–104. DOI: 10.25729/2413-0133-2018-4-10

Введение. В агрессивной среде каждая система, которая нацелена на продолжительный период стабильного функционирования, принимает меры для обеспечения непрерывной деятельности. При этом происходит не только взаимодействие с окружением, но и адаптивное управление внутренним состоянием. С усилием внешней агрессии увеличивается скорость адаптации, но теряется её качество, из-за чего провоцируются внутренние угрозы. Таким образом, важным условием обеспечения выживания и развития является наличие системы обеспечения безопасности, которая будет учитывать не только внешние воздействия, но и собственное состояние, способной предотвращать текущие и предупреждать будущие угрозы в условиях сложного взаимодействия разнородных противоречивых факторов.

Всё сказанное в равной мере относится и к информационным системам (ИС), особенно имеющим доступ к сети Интернет, которые находятся в откровенно агрессивной среде. На фоне событий 2017 года, когда множество компаний подверглось атаке вирусов-шифровальщиков, а применяемые средства защиты были неспособны предотвратить заражение, большую актуальность начали приобретать концепции проактивной защиты [4]. В их основе лежит тотальный мониторинг критических элементов ИС и прогнозирование будущих инцидентов безопасности.

В настоящее время в практике мониторинга безопасности, сбора и накопления статистики наиболее популярны так называемые системы управления информацией и событиями безопасности (Security Information and Event Management, SIEM), реализующие

событийный подход к обеспечению безопасности [5]. Они работают по правилам, задаваемыми администратором безопасности, который настраивает SIEM систему, исходя из знаний о защищаемой ИС, а не руководствуясь общими правилами, которые просто могут не подходить для конкретного случая, что позволяет более точно определять признаки возможных угроз.

Прогнозирование развития ситуации с целью проактивного реагирования на потенциальную возможность деструктивных воздействий на ИС является непростой задачей в любом случае и, тем более, если реакция происходит только на события или инциденты. Так на основе собранной статистики SIEM система способна давать прогноз появления в будущем выявленной угрозы. Но это относится только к тем инцидентам, которые уже были обнаружены и записаны в базу данных, что не позволяет предупреждать целевые атаки на ИС. Качество предоставляемого прогноза напрямую зависит от объема собранной статистики, и если событие безопасности выявляется недостаточно часто, то в будущем оно может быть убрано из рассмотрения, с целью повышения производительности и экономии обслуживания SIEM системы. Другой проблемой является то, что подобные прогнозы могут указать время возникновения угрозы, но не способны дать оценку потенциальному ущербу от её реализации.

Для решения этой проблемы предлагается применить дифференциальную модель противоборства, которая учитывает системно связанную информацию о защищаемой системе и её противнике. Такой подход позволяет увидеть тенденцию в поведении противника, прогнозировать динамику противоборства и выбрать упреждающие контрмеры

Дифференциальная модель противоборства. В первоначальной версии модель описывала взаимодействие развития информационно-коммуникационных технологий (ИКТ) и обеспечения национальной безопасности [10]. В своём развитии она была существенно модифицирована, размерность фазового пространства снижена, смысловое содержание переменных несколько переформулировано, введены ресурсы, как источник управляющих воздействий, подключена симметричная система противника [7]. В таком виде модель приобрела более универсальный вид и на экспериментах [2, 8, 9] подтвердила возможность применения аппарата обыкновенных дифференциальных уравнений для исследований не только физических или технических объектов, но и для анализа процессов, происходящих в плохо формализуемых системах, не имеющих узко физическую природу. Концептуально эту модель можно отнести к классической традиции, заложенной, в частности, работами Дж. Форрестера [1, 6] или Н.Н. Моисеева [3] в области глобальной динамики.

Модель представляется системой обыкновенных линейных дифференциальных уравнений:

$$M = \begin{cases} Y \begin{cases} \dot{y}_i = f(t, \bar{y}, \dot{\bar{y}}, z_2, s^{(y)}) \\ s^{(y)} = f(t, s^{(y)}, y_3) \end{cases} \\ Z \begin{cases} \dot{z}_i = f(t, \bar{z}, \dot{\bar{z}}, y_2, s^{(z)}) \\ s^{(z)} = f(t, s^{(z)}, z_3) \end{cases} \end{cases},$$

где $i = \overline{1,5}$; y_i и z_i – фазовые переменные (ФП) модели; $\dot{y}_i$, $\dot{z}_i$ – производные от переменных y и z; $s^{(y)}$, $s^{(z)}$ – ресурсы стороны Y и Z соответственно.

Иначе данная модель представляется структурной схемой (рис. 1).

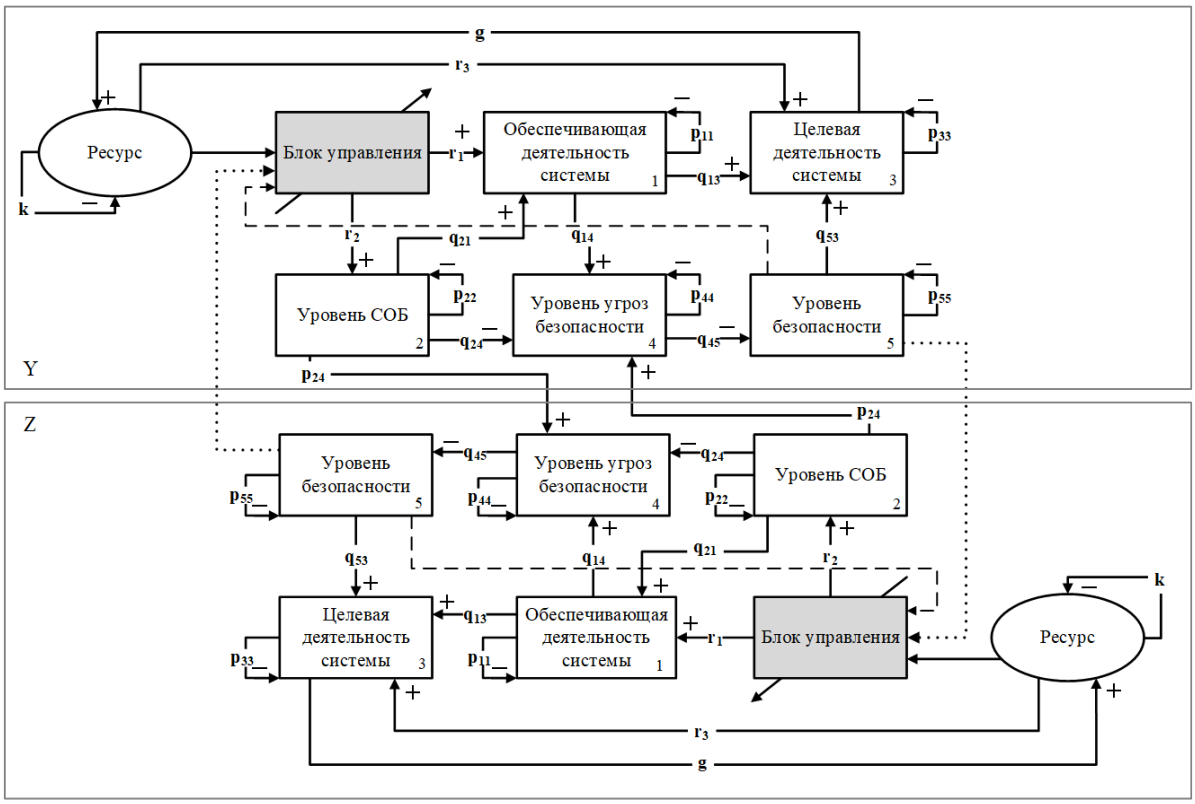

Рис. 1. Структурная схема дифференциальной модели противоборства

Структурная схема состоит из блоков, которые представляют фазовые переменные (номер блока соответствует номеру ФП), и связей. В зависимости от интерпретации, каждая фазовая переменная приобретает другое название, что не меняет её смысла, а служит только для упрощения восприятия. Подразумевается, что структурно все системы подобные, но семантически они могут отличаться. В таблице 1 представлено описание фазовых переменных информационной системы и злоумышленника, и фазовые переменные с номерами 1-3 имеют другое описание.

Таблица 1. Описание фазовых переменных

№	Семантическое описание фазовых переменных		
	В общих терминах	В терминах конфронтации ИС и злоумышленника	
		Для ИС (Y)	Для злоумышленника (Z)
1	Обеспечивающая деятельность системы (ОДС)	Обновление и поддержка	Обучение и улучшение методов нанесения вреда ИС
2	Уровень системы обеспечения безопасности (СОБ)	Уровень средств защиты информации	Анонимность и сокрытие следов
3	Целевая деятельность системы (ЦДС)	Хранение и обработка информации	Нанесение вреда
4	Уровень угроз безопасности (УУ)		
5	Уровень безопасности (УБ)		
s	Ресурс		

Выделяются четыре вида связей:

1. Влияние i-ой фазовой переменной на динамику изменения j-ой (i может быть равно j). Силу действия влияния определяют коэффициенты системы уравнений (p – скорость старения ФП, k – амортизация ресурса, r – доля ресурса, направленная для ФП, g – преобразование продуктов целевой деятельности

2. Влияние производной i-ой фазовой переменной на динамику изменения j-ой. В системе уравнений представлена коэффициентом q_{ij};

3. Информация об уровне безопасности собственной системы (для блока управления);
4. Информация об уровне безопасности противника (для блока управления).

На схеме также присутствует блок управления, который осуществляет распределение ресурсов в зависимости от целевой функции. Основными стратегиями управления являются: *паритет*, *доминирование* и *подавление*. Каждая имеет свое математическое описание:

$$F_{пар}(t) = \left| y_5(t) - z_5(t) \right| < \delta,$$
$$F_{дом}(t) = y_5(t) - z_5(t) > \delta,$$
$$F_{под}(t) = z_5(t) < \delta,$$

где $y_5(t)$ – уровень безопасности системы, применяющей стратегию;

$z_5(t)$ – уровень безопасности системы противника;

$\delta \geq 0$ – пороговое значение, задаваемое пользователем.

Основными стратегиями являются: *паритет* – стремление стороны удерживать разницу между уровнями безопасности в определенном интервале, *доминирование* – желание стороны иметь преимущество в уровне безопасности над противником не ниже определенного значения, *подавление,* целью которой – держать уровень безопасности противника не выше определенного порога.

Для работы модели необходимо определиться с источником данных для идентификации системы уравнений. В применении к описанию безопасности информационной системы, таким источником будет являться SIEM система.

Взаимодействия ДМП с SIEM. Технология работы дифференциальной модели противоборства и SIEM системы состоит из 8 этапов (рис. 2).

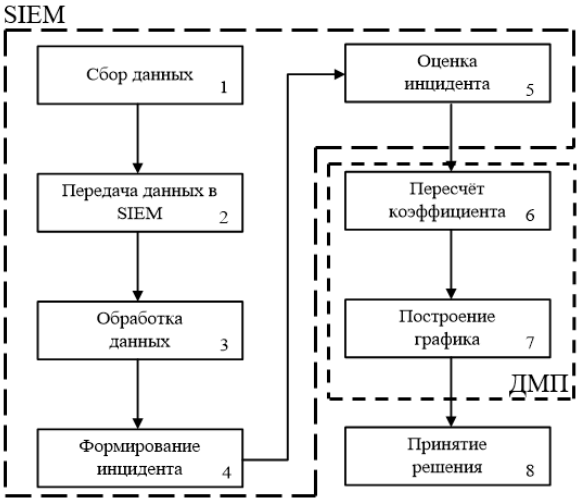

Рис. 2. Технология работы дифференциальной модели конфронтации и SIEM системы

Первые 5 этапов отражают работу SIEM системы: *Сбор данных* и *Передача данных* осуществляется программами-агентами, которые установлены на критических элементах информационной системы. *Обработка данных, Формирование и оценка инцидента* происходят уже в главной части комплекса мониторинга.

Этап 6 – Пересчёт коэффициента. В зависимости от источника угрозы (внутренний или внешний) происходит пересчёт соответствующего коэффициента ($p_{24}^{(y)}$ или $q_{14}^{(y)}$ соответственно) по формуле:

$$f_{пер}(k)=\begin{cases}\max(O_{SIEM}), \text{если поступала информация от SIEM}\\ k, \text{если информация от SIEM не поступала}\end{cases},$$

где k – коэффициент, который подлежит перерасчету; O_{SIEM} – оценка инцидента присвоенная SIEM системой (предварительно накладывается ограничение $O_{SIEM} \in [0;1]$).

Этап 7 – Построение графика. После пересчета коэффициентов происходил корректировка графика фазовых переменных.

Этап 8 – Принятие решения. Полученные графики отображаются на рабочей машине администратора безопасности и он, анализируя изменение динамики фазовой переменной, принимает соответствующее решение.

Описанная технология представляет собой цикл (рис. 3), в котором инцидент регистрируется на физическом уровне средствами защиты информации (СЗИ) и средствами, установленными на автоматизированной рабочей станции (АРМ), передается в SIEM, обрабатывается, оценка инцидента передается в ДМП, где происходит корректировка прогноза динамики фазовой переменной, что также отображается на графике. Далее специалист по информационной безопасности анализирует полученную информацию и принимает решение (например, настройка СЗИ).

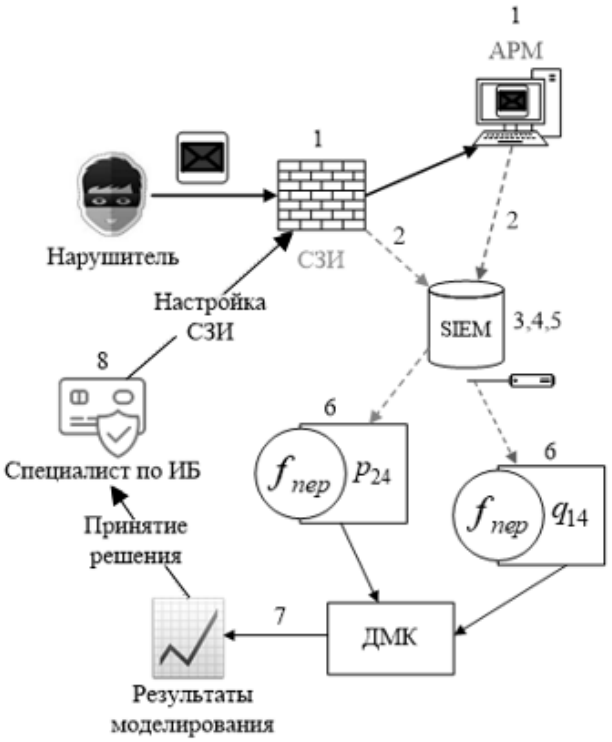

Рис. 3. Цикл обнаружения инцидента и принятия решения специалистом

Имитация работы ДМП и SIEM. Рассмотрим пример работы дифференциальной модели противоборства на имитации потока событий от SIEM системы. В действительности этот поток представляет из себя массив инцидентов и значений их оценок (рис. 4).

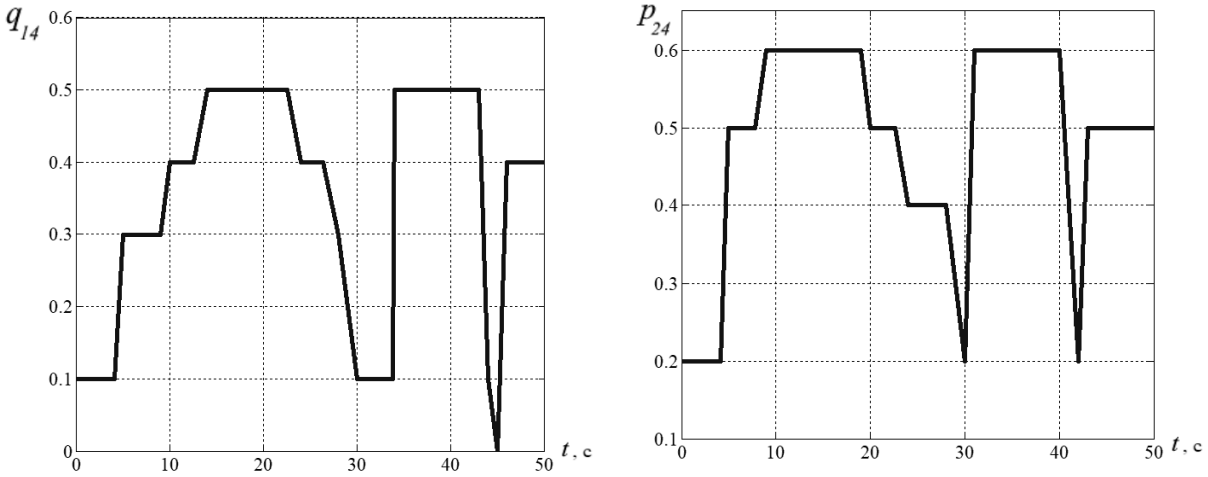

Рис. 4. Графики изменения коэффициентов модели (слева – по событиям внешних угроз, справа – по событиям внутренних угроз)

Представленные графики отображают пересчет коэффициентов p_{24} и q_{14}, которые в модели отвечают за определение влияния внешних и внутренних угроз соответственно.

Уровень угроз информационной системы описывается переменной y_4 (рис. 5).

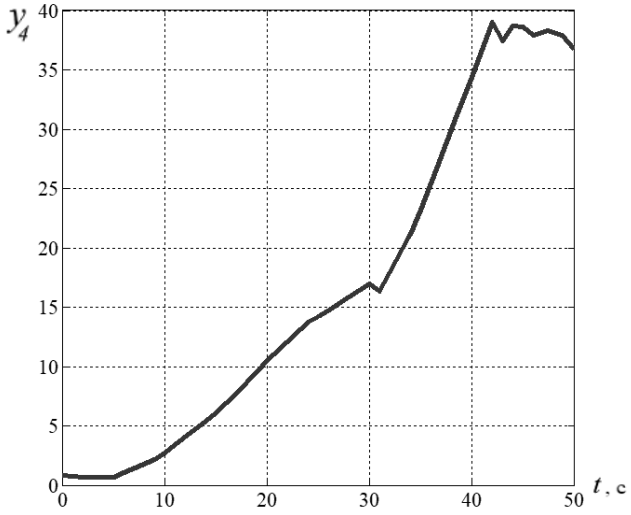

Рис. 5. График уровня угроз ИС

Когда специалист по информационной безопасности получит график уровня угроз, он обратит внимание, что на его рост, а также на колебания под конец моделирования. Это означает, что была зафиксирована атака, и средствам защиты информации потребуется время для её предотвращения. Проанализировав состояние уровня угроз необходимо понять, как это скажется на уровне безопасности информационной системы.

Состояние безопасности ИС описывается переменной y_5 (рис. 6).

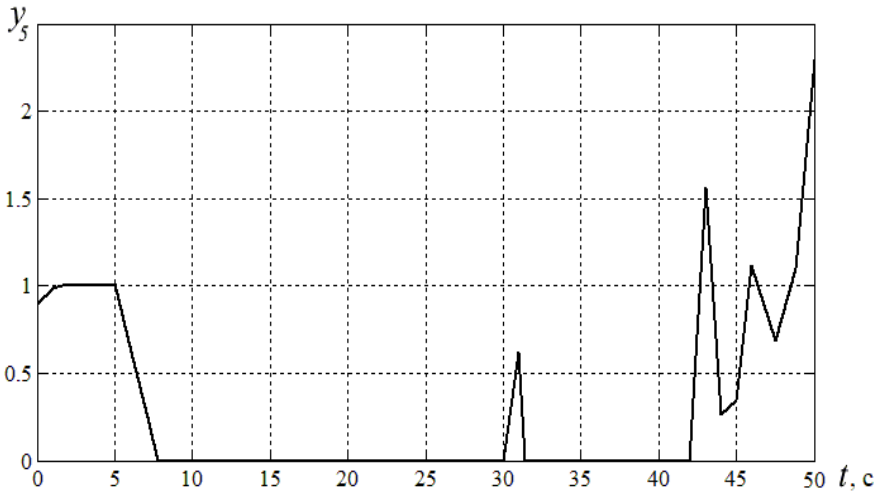

Рис. 6. График уровня безопасности ИС

Как видно из графика, уровень безопасности большее время моделирования находится около нулевого значения, что показывает серьезность инцидента, так как, если бы атака проходила более интенсивно, то средства защиты могли не успеть предотвратить вторжение.

Проведенный эксперимент показал, что дифференциальная модель противоборства на основании потока событий может показывать адекватные результаты и полезную информацию. Так как поток событий можно связать с конкретными событиями, то можно однозначно определить какие события несут большую опасность системе.

Заключение. Дифференциальную модель противоборства в своей работе могут использовать, как аналитики, так и руководители отделов обеспечения безопасности. На основе предоставляемых прогнозов, способных показать степень деструктивного воздействия на основные активы информационной системы, специалисты получают дополнительный источник информации для принятия решения, что должно улучшить применение проактивных действий.

В работе представлено методика и технология взаимодействия дифференциальной модели противоборства и SIEM системы. Данное решение подразумевает упрощение сбора необходимых данных для работы модели.

Несмотря на то, что работа модели была проверена на имитации потока инцидентов безопасности, она показала работоспособность предложенного алгоритма. Это показывает перспективность исследования и необходимость проведения натурных испытаний, для чего необходимо выбрать одну из SIEM систем и разработать программный комплекс, реализующий описанное выше взаимодействие.

СПИСОК ЛИТЕРАТУРЫ

1. Геловани В.А., Егоров В.А., Митрофанов В.Б., Пионтковскй А.А. Решение одной задачи управления для глобальной динамической модели Форрестера. М.: Институт прикладной математики АН СССР. 1974. 29 с.
2. Колесников К.Е., Шишкин В.М. Исследование динамики симметричного противоборства на дифференциальной модели // Информационная безопасность социально-

экономических систем: монография / Апатова Н.В. и др. / под ред. проф. О.В. Бойченко. Симферополь: ИП Зуева Т.В. 2017. С. 202–218.
3. Моисеев Н.Н. Простейшие математические модели экономического прогнозирования. М.: «Знание». 1975. 63 с.
4. Осипов П.А., Минзов А.С. О необходимости развития концепции проактивной защиты. Режим доступа: http://www.mce.su/archive/doc313244/rus.pdf (дата обращения 14.04.2018)
5. Федорченко А.В., Левшун Д.С., Чечулин А.А., Котенко И.В. Анализ методов корреляции событий безопасности в SIEM-системах. Часть 1. // Тр. СПИИРАН. 47 (2016), С. 5–27
6. Форрестер Дж. Мировая динамика. СПб.: Terra Fantastica. 2003. 379 с.
7. Шишкин В.М., Абросимов И.К. Динамическая модель системы взаимодействия развития ИКТ и обеспечения национальной безопасности // VIII Санкт–Петербургская межрегиональная конференция “Информационная безопасность регионов России” - ИБРР–2013. (Санкт-Петербург, 23–25 октября 2013.): Материалы конференции. СПб. СПОИСУ. 2013. С. 25.
8. Шишкин В.М. Колесников К.Е. Динамическая модель противоборства – интерпретации и эксперименты // XI Международная школа-симпозиум «Анализ, моделирование, управление, развитие социально-экономических систем» - АМУР-2017 (Симферополь-Судак, 14-27 сентября): сборник научных трудов / Под общей редакцией А.В. Сигала. Симферополь. ИП Корниенко А.А. 2017. С. 438–444.
9. Шишкин В.М., Колесников К.Е. Исследование дифференциальной модели информационного противоборства // III межрегиональная научно-практическая конф. «Перспективные направления развития отечественных информационных технологий» (Севастополь, 19-23 сентября 2017 г. Севастопольский гос. Университет) : материалы. Севастополь: «РИБЕСТ». 2017. С. 67–69.
10. Юсупов Р.М, Шишкин В.М. О некоторых противоречиях в решении проблем информационной безопасности // Труды СПИИРАН. Вып. 6. СПб.: Наука. 2008. С. 11–23.

UDK 519.711.2

INVESTIGATION OF THE FORECASTING MODEL OF APPLICATION IN THE PROCESS OF SECURITY MANAGEMENT

Vladimir M. Shishkin
Ph.D., Associate Professor, Senior Scientist
St. Petersburg Institute for Informatics and Automation of the RAS,
39, 14-th Linia, VI, St. Petersburg, 199178, Russia, e-mail: vms@iias.spb.su
Konstantin E. Kolesnikov
Specialist, General Department of the Ministry of Justice
of the Russian Federation for St. Petersburg,
11, St. Isaac's Square, St. Petersburg, 190000, Russia, e-mail: kolesnikovib@gmail.com

Abstract. In the paper, the possibility of a differential model of confrontation (DSM) is shown to provide a forecast of the development of security incidents in information systems. The methodology and technology of its interaction with SIEM class systems

are proposed. Experiments have been carried out to simulate the work of the differential confrontation model with the data flow from the SIEM system, some results are shown.
Keywords: system of differential equations, confrontation, information security, SIEM, modeling

References

1. Gelovani V.A., Egorov V.A., Mitrofanov V.B., Piontkovsky A.A. Resheniye odnoy zadachi upravleniya dlya global'noy dinamicheskoy modeli Forrestera [The solution of one problem of control for the global dynamic model of Forrester]. Moscow. IPM AN SSSR = IPM AS of the USSR. 1974. 29 p. (in Russian)
2. Kolesnikov K.E., Shishkin V.M. Issledovaniye dinamiki simmetrichnogo protivoborstva na differentsial'noy modeli [Investigation of the Dynamics of a Symmetric Contrast on a Differential Model] // Information Security of Socio-Economic Systems: Monograph / Apatova NV and others. Ed. prof. O.V. Boychenko. Simferopol. IP Zueva T.V. 2017. Pp. 202–218. (in Russian)
3. Moiseyev N.N. Prosteyshiye matematicheskiye modeli ekonomicheskogo prognozirovaniya [The simplest mathematical models of economic forecasting]. Moscow. Znanie = Knowledge. 1975. 63 p. (in Russian)
4. Osipov P.A., Minzov A.S. O neobkhodimosti razvitiya kontseptsii proaktivnoy zashchity [On the need to develop a concept of proactive protection]. Available at: http://www.mce.su/archive/doc313244/eng.pdf (accessed 14.04.2018) (in Russian)
5. Fedorchenko A.V., Levshun D.S., Chechulin A.A., Kotenko I.V. Analiz metodov korrelyatsii sobytiy bezopasnosti v SIEM-sistemakh. Chast' 1. [Analysis of methods of correlation of security events in SIEM-systems. Part 1.] // Tr. SPIIRAN. 47 (2016). Pp. 5–27. (in Russian)
6. Forrester J. Mirovaya dinamika [World Dynamics]. St. Petersburg: Terra Fantastica. 2003. 379 p. (in Russian)
7. Shishkin V.M., Abrosimov I.K. Dinamicheskaya model' sistemy vzaimodeystviya razvitiya IKT i obespecheniya natsional'noy bezopasnosti [Dynamic model of the system of interaction between the development of ICT and ensuring national security] // VIII St. Petersburg Interregional Conference «Information security of Russian regions» - IBRD-2013 (St. Petersburg, October 23-25, 2013): proceedings. SPb. SPOISU. 2013. P. 25. (in Russian)
8. Shishkin V.M. Kolesnikov K.E. Dinamicheskaya model' protivoborstva – interpretatsii i eksperimenty [Dynamic model of confrontation - interpretations and experiments] // XI International School Symposium “Analysis, modeling, management, development of socio-economic systems” - AMUR-2017 (Simferopol-Sudak, September 14-27): proceedings / Ed. A.V. Sigal. Simferopol. IP Kornienko A.A. 2017. Pp. 438–444. (in Russian)
9. Shishkin V.M., Kolesnikov K.E. Issledovaniye differentsial'noy modeli informatsionnogo protivoborstva [Investigation of the differential model of information confrontation] // III interregional scientific and practical conference “Perspective directions of the development of domestic information technologies” (Sevastopol, The Sevastopol state. University, September 19-23, 2017) Sevastopol. "RIBEST". 2017. Pp. 67–69. (in Russian)
10. Yusupov R.M., Shishkin V.M. O nekotorykh protivorechiyakh v reshenii problem informatsionnoy bezopasnosti [About some contradictions in the solution of information security problems] // Proceedings of SPIIRAS. Issue. 6. SPb . Science. 2008. Pp. 11–23. (in Russian)