УДК 004.7, 004.056, 004.056.5
doi:10.31799/1684-8853-2018-4-61-72

Научные статьи
Articles

МЕТОД АДАПТИВНОГО УПРАВЛЕНИЯ ЗАЩИТОЙ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ НА ОСНОВЕ АНАЛИЗА ДИНАМИКИ ДЕЙСТВИЙ НАРУШИТЕЛЯ

Г. И. Коршунов[а, б], *доктор техн. наук, профессор, kgi@pantes.ru*
В. А. Липатников[в], *доктор техн. наук, профессор, lipatnikovanl@mail.ru*
А. А. Шевченко[в], *младший научный сотрудник, alex_pavel1991@mail.ru*
Б. Ю. Малышев[в], *старший оператор научной роты, bogdan160596@bk.ru*
[а]*«ПантесГруп», Ириновский пр., д. 2, лит. А, Санкт-Петербург, 195248, РФ*
[б]*Санкт-Петербургский государственный университет аэрокосмического приборостроения, Б. Морская ул., 67, Санкт-Петербург, 190000, РФ*
[в]*Военная академия связи им. Маршала Советского Союза С. М. Буденного, Тихорецкий пр., 3, Санкт-Петербург, 194064, РФ*

Постановка проблемы: *известные методы адаптивного управления защитой информационно-вычислительных сетей с применением специальных мер защиты в современных условиях недостаточно эффективны, так как учитывают только одну сторону информационного противоборства.* ***Цель:*** *разработка метода адаптивного управления защитой информационно-вычислительных сетей на основе анализа динамики действий нарушителя.* ***Результаты:*** *предложен метод адаптивного управления защитой информационно-вычислительной сети на основе использования результатов анализа динамики действий нарушителя, определении ситуационных параметров в противоборствующей обстановке при стохастической неопределенности. Метод включает мониторинг обстановки, оперативный контроль последовательности действий нарушителя, моделирование стратегии воздействия нарушителя, процесс определения ситуационных параметров с достоверным прогнозом стратегии вторжений. В процессе анализа администратор сети получает информацию о приоритетных целях нарушителя, используемых им средствах и уязвимостях сети. Это дает возможность оперативно принять меры по повышению защищенности сети и избежать ее компрометации.* ***Практическая значимость:*** *использование данного подхода позволяет поддерживать работоспособность автоматизированных систем менеджмента организации интегрированной структуры с учетом масштабирования при планировании и внесении в нее изменений в условиях информационного противоборства на требуемом уровне при динамике изменения множества угроз.*

Ключевые слова *— автоматизированная система, менеджмент организации, интегрированная структура, информационно-вычислительная сеть, компьютерные атаки, защита информации, оценка рисков, контейнерная виртуализация, проактивное управление, масштабирование, показатель защищенности.*

Цитирование: Коршунов Г. И., Липатников В. А., Шевченко А. А., Малышев Б. Ю. Метод адаптивного управления защитой информационно-вычислительных сетей на основе анализа динамики действий нарушителя// Информационно-управляющие системы. 2018. № 4. С. 61–72. doi:10.31799/1684-8853-2018-4-61-72
Citation: Korshunov G. I., Lipatnikov V. A., Shevchenko A. A., Malyshev B. Y. Adaptive Management of Information Network Protection with Analysis of Intruder's Actions. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2018, no. 4, pp. 61–72 (In Russian). doi:10.31799/1684-8853-2018-4-61-72

Введение

В связи с быстрым развитием компьютерных технологий, в том числе сети Интернет, объединяющей разнородные сети, и переходом к информационному обществу проблема обеспечения информационной безопасности (ИБ) и построения автоматизированных систем менеджмента организации интегрированной структуры стала одной из наиболее актуальных [1]. К средствам защиты в настоящее время предъявляются более жесткие требования [2, 3].

Известны методы обеспечения необходимого уровня защищенности различных систем, например, способ управления ИБ информационно-вычислительной сети (ИВС) путем реализации ложной сети на основе выделенного сервера с контейнерной виртуализацией [4, 5]. Однако в этом случае при управлении ИВС не используются данные анализа динамики действий нарушителя. Также известен способ контроля уязвимостей при масштабировании автоматизированных систем менеджмента организации интегрированной структуры, который заключается в том, что управление ИБ основано на выявлении уязвимостей [6]. Данный способ является реактивным и не учитывает результатов анализа динамики действий нарушителя. С учетом быстрого развития способностей злоумышленников использование этого метода не обеспечит повышение защищенности разрабатываемых систем.

При исследовании известных способов защиты ИВС [7–10] недостаточное внимание уделено анализу динамики действий нарушителя, кото-

рые включают сценарии внешних и внутренних вторжений. Возникает противоречие между эффективными новыми средствами информационного вторжения и существующими способами защиты ИВС. Поэтому задача повышения защиты ИВС от вторжений со стороны нарушителей является актуальной.

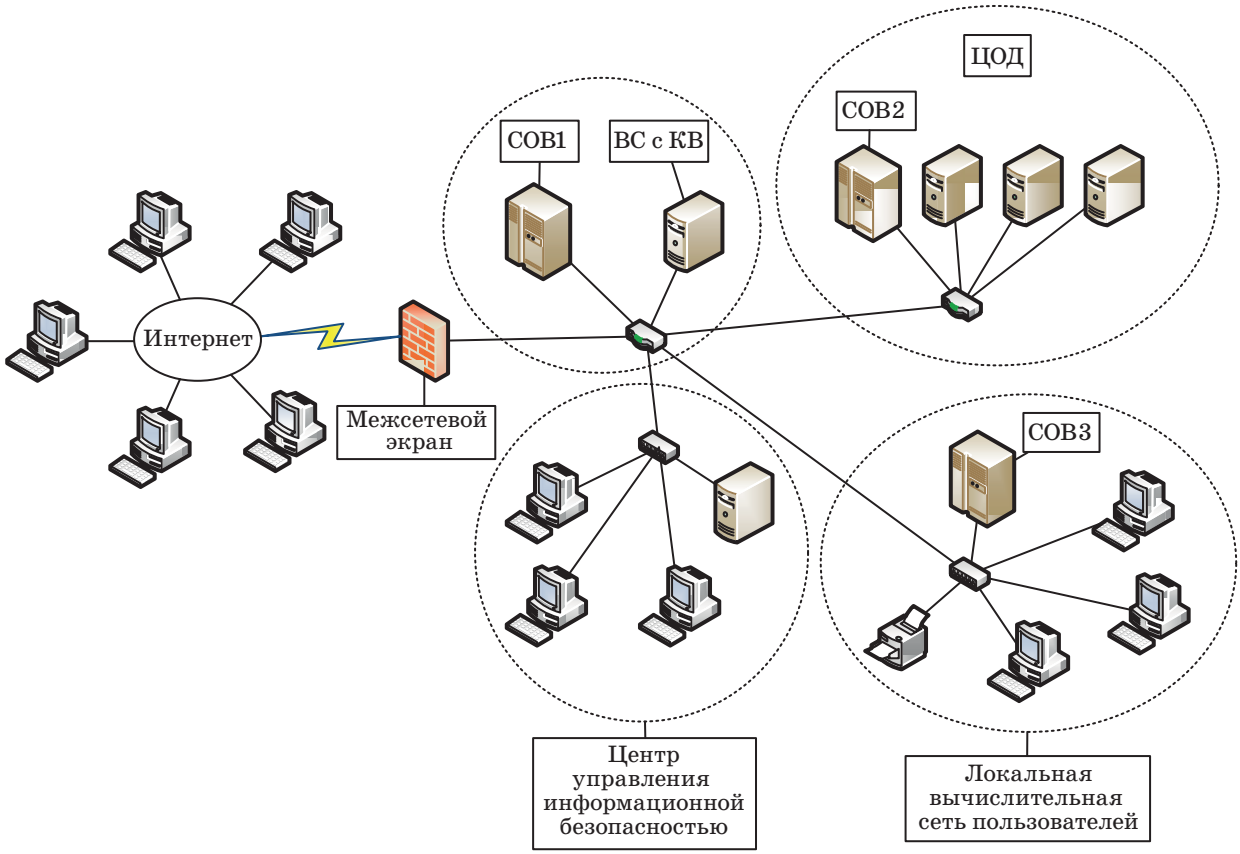
Целью данной работы является повышение ИБ ИВС на основе метода, включающего анализ и прогноз действий нарушителя.

Разработка алгоритма адаптивного управления защитой ИВС на основе анализа динамики действий нарушителя и его экспериментальное тестирование

Представляется эффективной ИВС, имеющая топологию «Звезда» (рис. 1) в составе: межсетевого экрана, системы обнаружения вторжений *СОВ*, выделенного сервера с контейнерной виртуализацией *ВС* с *КВ*, центра обработки данных, коммутаторов и ЭВМ пользователей. Для решения задач защиты и мониторинга ИВС необходимо не только обнаруживать и блокировать действия нарушителей, но также анализировать атаки и отвлекать нарушителей. Это достигается путем заманивая нарушителей на ложные информационные системы и сбора информации о тактике нарушителя, его идентификации и нейтрализации. Для сочетания достоверного анализа и прогнозирования динамики действий предложено адаптировать защиту ИВС и обеспечить повышение оперативности отслеживания фаз развития кризисных ситуаций. На основании результатов анализа деятельности нарушителя определяются слабые стороны системы защиты информации в ИВС.

Решение задачи заключается в анализе динамики действий нарушителя, обработке, определении уязвимостей системы защиты информации при использовании выделенного сервера с контейнерной виртуализацией, прогнозировании возможных вторжений, представлении данных для выбора оптимального решения по повышению вероятности защищенности ИВС с учетом подхода, описанного в работе [4]. Учитывается динамический характер модели нарушителя, поэтому процессы поиска и устранения уязвимостей в защите также динамически изменяются во времени.

Цифровой поток (ЦП), входящий и исходящий из сети Интернет, вначале проходит пред-



■ ***Рис. 1.*** Структура информационно-вычислительной сети
■ ***Fig. 1.*** Structure of the information network

варительную фильтрацию межсетевым экраном, после чего поступает в СОВ и анализируется на предмет наличия атак. В случае когда внутренний нарушитель пытается получить несанкционированный доступ к информационным ресурсам ИВС, происходит анализ запросов, и если критический параметр больше допустимого уровня, то ЦП перенаправляется на компоненты ложной информационной системы. Легитимные запросы, удовлетворяющие требованиям политик безопасности СОВ, перенаправляются на истинные информационные системы. Если СОВ не удалось обнаружить атаку на сетевом уровне, но при этом действия нарушителя были выявлены после их реализации на определенных хостах системы, осуществляется перенаправление последующего ЦП нарушителя на компоненты выделенного сервера с контейнерной виртуализацией.

Структура процесса мониторинга обстановки (рис. 2) показывает, что ЦП поступает в СОВ, далее происходит сканирование по заданным параметрам. СОВ выделяет из всего ЦП только тот, который попадает под определенные критерии. Затем происходит выделение признаков и их дальнейший анализ. Анализ осуществляется за счет уже имеющихся баз данных описания известных видов угроз. В случае соответствия ЦП критериям угроз производится анализ моделей угроз и принимается решение по способам защиты ИВС. Когда не удается однозначно определить, какого рода ЦП, то он отсеивается (блокируется) и перенаправляется на развернутую виртуальную сеть, и далее запросы такого рода анализируются, в результате принимаются меры по разрешению или запрету доступа. Далее производится обновление баз данных с добавлением новых видов угроз с учетом обнаруженных инцидентов.

Алгоритм функционирования ИВС включает в себя два параллельных процесса (рис 3).

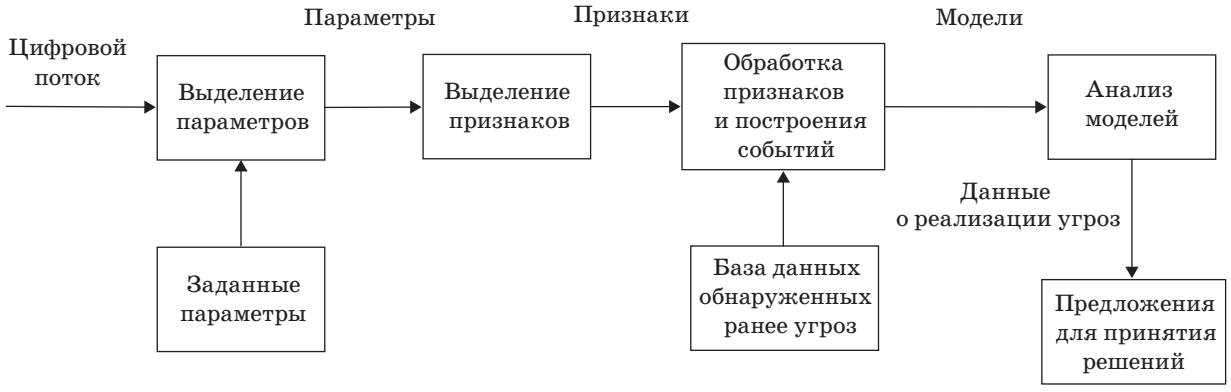
Первый процесс представляет собой тестирование ИВС и выявление уязвимостей. Данное действие представлено в статье [6] и реализовано в работе [9]. Второй процесс представляет собой анализ ЦП с выявлением аномалий и последующим анализом динамики действий нарушителя. Задача детального анализа корреляции действий нарушителя необходима для выявления их параметров, что позволит определить эффективность применения мер защиты на различных этапах. По результатам строится прогнозная модель угроз и выбираются средства защиты [11].

Обобщенный алгоритм анализа действий нарушителя для данного вида атак можно описать рис. 4.

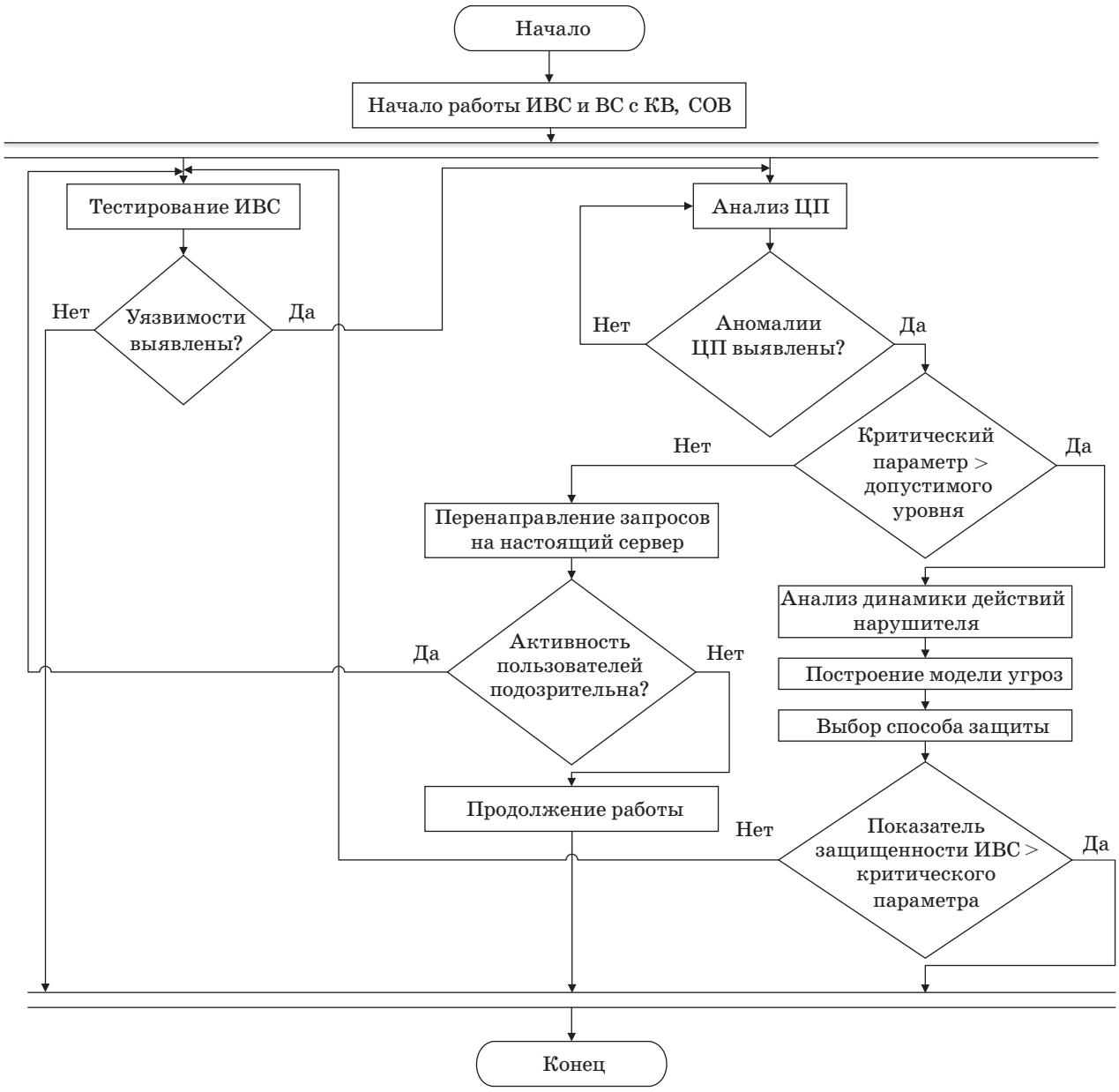
В соответствии с тем, обнаружены ли атаки на граничном хосте или нет, их можно разделить на два типа [12–20]: обнаруживаемые и не обнаруживаемые атаки.

Атаки первой группы блокируются граничным хостом, не достигая рабочих серверов. При обнаружении такого рода атак СОВ должна изменять свою конфигурацию, чтобы последующие действия нарушителя перенаправлялись на ложные информационные системы. К атакам второго вида относят атаки, параметры которых неизвестны, атаки внутренних нарушителей через терминалы пользователей. В таком случае действия нарушителя возможно выявить при анализе общего журнала регистрации событий (сообщений от системы контроля целостности файлов; изменений настроек устройств в ИВС). В ходе выявления в журнале регистрации этих событий действия нарушителя блокируются с оповещением администратора. На рис. 5 изображен граф событий действий нарушителя.

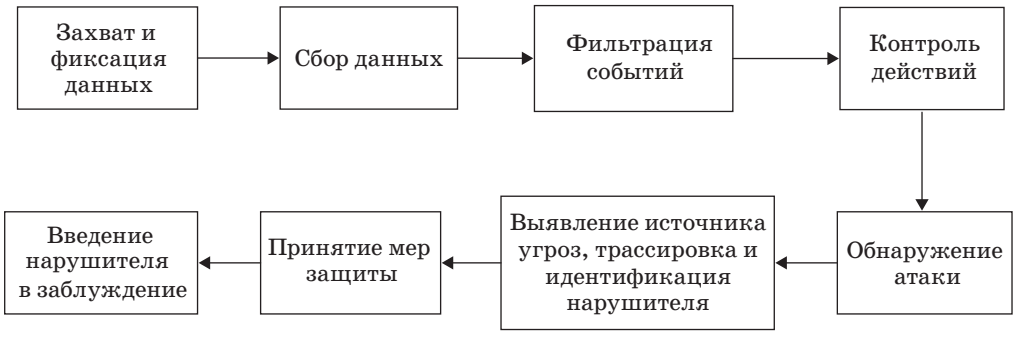
В качестве одной из возможных моделей предлагается представлять действия нарушителя как систему с переменной структурой, поведение которой на случайных интервалах времени харак-



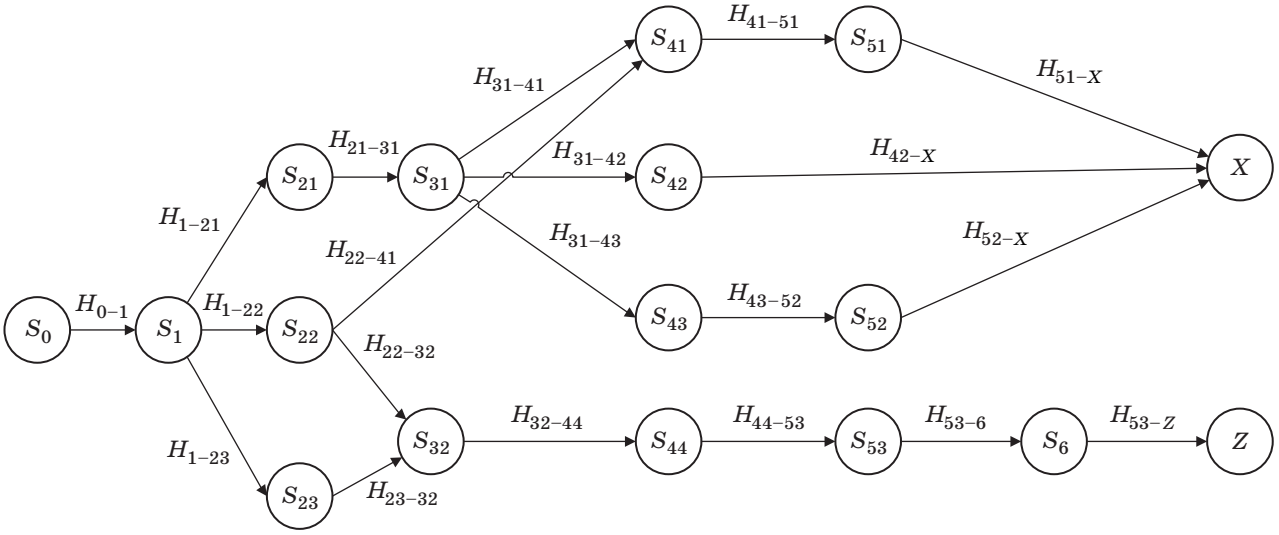
■ ***Рис. 2.*** Структура процесса мониторинга обстановки
■ ***Fig. 2.*** Structure of the process of monitoring the situation



■ ***Рис. 3.*** Обобщенный алгоритм функционирования ИВС
■ ***Fig. 3.*** Generalized algorithm for the operation of information network



■ ***Рис. 4.*** Общий алгоритм анализа действий нарушителя
■ ***Fig. 4.*** General algorithm for analyzing the actions of the intruder



■ ***Рис. 5***. Граф событий действий нарушителя
■ ***Fig. 5***. The graph of events of the actions of the intruder

теризуется различными структурами и описывается вероятностными законами [21, 22]. При этом переход одной структуры в другую происходит в случайный момент времени в зависимости от текущих фазовых координат системы, которые обозначены H_i.

Описания каждого события из графа на рис. 5 представлены в табл. 1.

Для разделения возможных сценариев развития событий мы будем использовать схему «дерева вероятностей». Каждая ветвь представляет собой отдельный сценарий развития [23]. На рис. 5 представлены семь путей для реализации угрозы хищения информации и отказа в обслуживании:

$$S_{x1} = \{S_1, S_{21}, S_{31}, S_{41}, S_{51}, X\};$$
$$S_{x2} = \{S_1, S_{21}, S_{31}, S_{42}, X\};$$
$$S_{x3} = \{S_1, S_{21}, S_{31}, S_{43}, X\};$$
$$S_{x4} = \{S_1, S_{21}, S_{31}, S_{43}, S_{52}, X\};$$
$$S_{x5} = \{S_1, S_{22}, S_{41}, S_{51}, X\};$$
$$S_{z1} = \{S_1, S_{22}, S_{32}, S_{44}, S_{53}, S_6, Z\};$$
$$S_{z2} = \{S_1, S_{23}, S_{32}, S_{44}, S_{53}, S_6, Z\}.$$

Определим коэффициенты реализуемости событий (элементов графа) для установления динамики действий нарушителя, воспользовавшись методикой, представленной в работе [24].

В данной методике исходная защищенность определяется по ранжированию в зависимости от суммы предъявляемых критериев:

0 — для высокой степени исходной защищенности;

■ ***Таблица 1***. Описание событий действий нарушителя
■ ***Table 1***. Description of events of the actions of the intruder

Событие	Описание
S_0	Защищенное состояние ИВС (без действий нарушителя)
S_1	Начало действий нарушителя
S_{21}	Измерение характеристик ИВС путем внедрения сниффера
S_{22}	Тестирование состояния ИВС путем анализа запросов
S_{23}	Анализ «эхо-запросов»
S_{31}	Анализ исходящего цифрового потока
S_{32}	Выявление хостов
S_{41}	Выявление паролей
S_{42}	Дешифрование информации
S_{43}	Несанкционированное использование авторизованного IP-адреса в сети
S_{44}	Сканирование портов
S_{51}	Подмена пользователя в сети
S_{52}	Изменение целостности, доступности и конфиденциальности информации
S_{53}	Анализ характеристик приложений
S_6	Осуществление DDoS-атак
X	Реализация угрозы хищения информации
Z	Реализация отказа в обслуживании

5 — для средней степени исходной защищенности;

10 — для низкой степени исходной защищенности.

А для определения коэффициента реализации угрозы используют следующие шкалы ранжирования:

0 — для маловероятной реализации угрозы;

2 — для низкой вероятности реализации угрозы;

5 — для средней вероятности реализации угрозы;

10 — для высокой вероятности реализации угрозы.

Такой тип ранжирования не подходит для более точного получения результата, поэтому при оценке исходной защищенности и определении коэффициента реализации угрозы воспользуемся десятибалльной шкалой с единичными делениями:

$$G = \frac{Y_1 + Y_2}{20}, \quad (1)$$

где Y_1 — коэффициент исходной защищенности; Y_2 — коэффициент реализации угрозы.

Время перехода из одного события в другое зависит от коэффициента реализуемости события:

$$T_i = T_{\max j} - G_i \times T_{\text{исх } ij}, \quad (2)$$

где $T_{\max j}$ — максимальное время реализации j-го события ($T_{\max j} = 24$ ч); G_i — коэффициент реализуемости S_i-го события; $0 \le G_i \le 1$; $T_{\text{исх } ij}$ — исходное время перехода из i-го события в j-е событие ($T_{\text{исх } ij}$ от 0 до 24 ч).

Применяя подход, описанный в работе [25], составляем производящую функцию для графа на рис. 5 на примере пути S_{x1}:

$$H_{\text{угр}} = H_{0-1} \times H_{1-21} \times H_{21-31} \times \times H_{31-41} \times H_{41-51} \times H_{51-x}, \quad (3)$$

где $H_y = P_y \cdot x^{T_y}$, а P_y — вероятность перехода из одного состояния в другое; T_y — время, необходимое для перехода из одного состояния в другое; x — весовой коэффициент (от 0 до 1).

Вероятность реализации угрозы, согласно графу, для пути S_{x1} определяется в виде

$$P_{\text{угр}} = H_{\text{угр}}(x = 1) = P_{0-1} \times P_{1-21} \times P_{21-31} \times \times P_{31-41} \times P_{41-51} \times P_{51-x}. \quad (4)$$

Вероятность защищенности определяется по формуле

$$P_{\text{защ}} = 1 - P_{\text{угр}}. \quad (5)$$

По методике, представленной в работе [24], и формулам (1)–(5) рассчитываются время и вероятность перехода из одного события в другое, представленные в табл. 2.

Из графика зависимости защищенности от вероятности начала действий нарушителя (рис. 6) видно, что даже при малой вероятности начала действий нарушителя $P_{0-1} = 0{,}4$ вероятность защищенности $P_{\text{защ}}$ будет ниже требований уровня 0,95. Тем самым реализация угрозы по пути S_{x2} будет наиболее вероятной и привлекательной с точки зрения нарушителя, поэтому администратору безопасности необходимо устранить «бреши» в защите, которые приведут к реализации угрозы хищения информации по пути S_{x2}. Данный метод позволяет расставить приоритеты при организации защиты информации.

Зависимость вероятности реализации угрозы и вероятности защищенности ИВС от времени для реализации метода адаптивного управления защитой ИВС на основе анализа динамики действий нарушителя показана на рис. 7, где S_{x2} — последовательность действий нарушителя для реализации угрозы X; $P_з$ — уровень ИБ ИВС; t_1, t_2, t_3, t_4 — время; $S_{з\,i}$ — график зависимости защищенности ИВС от вероятности реализации угрозы; S_{x2i} — зависимость действий нарушителя от принятых мер защиты.

В промежуток времени t_1 происходит внедрение сниффера. В момент времени t_2 происходит обнаружение СОВ данного воздействия, при этом уровень защищенности падает. В дальнейшем происходит построение модели угроз. Затем принимаются меры по нейтрализации угрозы, которая была обнаружена с принятием актуальных мер защиты объектов ИВС, которые будут атакованы нарушителем в ближайшее время согласно графу действий нарушителя.

После принятия в момент t_4 мер защиты реализация следующего воздействия нарушителя S_{31} уже невозможна в силу снижения вероятности реализации угрозы до нуля, защищенность вернется на уровень 95 %.

Процесс проактивного обнаружения вторжений основывается на превентивном анализе запросов и удовлетворении их критериям, при этом сравнение производится не только по идеальным моделям и критериям ранее обнаруженных угроз, но также и при помощи построения путей реализации угрозы, позволяющих определить динамику действий нарушителя.

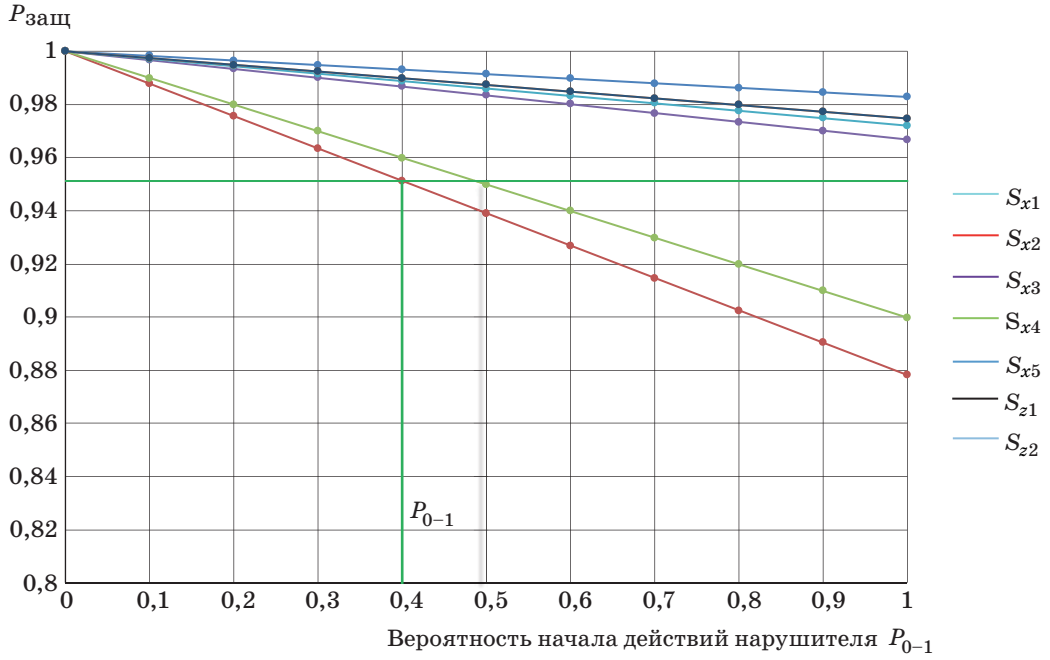
На основе методики, изложенной в работе [4], в табл. 3 приведены результаты расчета времени реализации угрозы хищения информации X по пути P_{x1}, полученные методами адаптивного и традиционного управления защитой ИВС.

При использовании адаптивного метода защиты ИВС нарушитель потратит на 7 % больше

■ ***Таблица 2.*** Время и вероятность перехода из одного события в другое

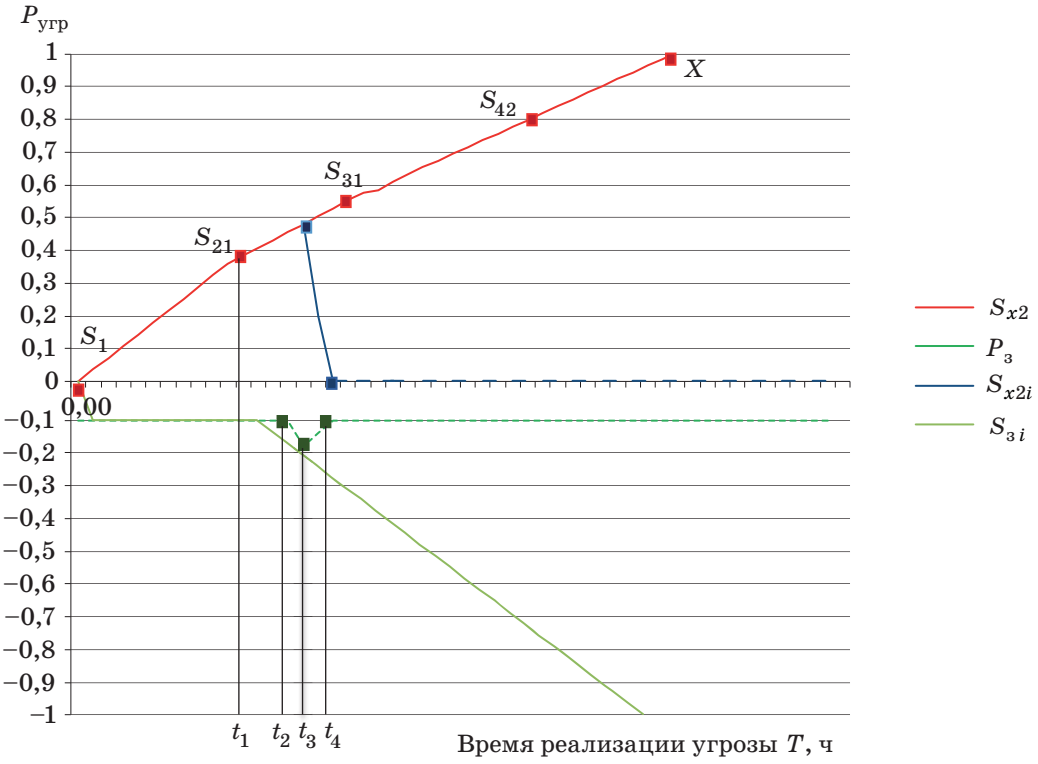
■ ***Table 2.*** Time and probability of transition from one event to another

Путь S_{x1}	События	S_1	S_{21}	S_{31}	S_{41}	S_{51}	X	
	Время перехода одного события в другое T, ч	14,4	12,48	12,77	13,79	11,6	18,2	
	Вероятность перехода из одного состояния в другое	0,4	0,48	0,47	0,43	0,52	0,24	
Путь S_{x2}	События	S_1	S_{21}	S_{31}	S_{42}	X		
	Время перехода одного события в другое T, ч	14,4	12,48	12,77	16,34	15,8		
	Вероятность перехода из одного состояния в другое	0,4	0,48	0,47	0,32	0,34		
Путь S_{x3}	События	S_1	S_{21}	S_{31}	S_{43}	X		
	Время перехода одного события в другое T, ч	14,4	12,48	12,77	17,62	15,19		
	Вероятность перехода из одного состояния в другое	0,4	0,48	0,47	0,27	0,37		
Путь S_{x4}	События	S_1	S_{21}	S_{31}	S_{43}	S_{52}	X	
	Время перехода одного события в другое T, ч	14,4	12,48	12,77	17,62	15,19	16,41	
	Вероятность перехода из одного состояния в другое	0,4	0,48	0,47	0,27	0,37	0,32	
Путь S_{x5}	События	S_1	S_{22}	S_{41}	S_{51}	X		
	Время перехода одного события в другое T, ч	14,4	12,48	14,02	11,39	18,31		
	Вероятность перехода из одного состояния в другое	0,4	0,48	0,42	0,52	0,24		
Путь S_{z1}	События	S_1	S_{21}	S_{32}	S_{44}	P_{53}	P_6	Z
	Время перехода одного события в другое T, ч	14,4	11,04	16,82	8,86	16,03	11,18	16,73
	Вероятность перехода из одного состояния в другое	0,4	0,54	0,3	0,63	0,33	0,53	0,3
Путь S_{z2}	События	S_1	S_{23}	S_{32}	S_{44}	S_{53}	S_6	Z
	Время перехода одного события в другое T, ч	14,4	14,64	14,48	10,97	14,13	12,69	15,75
	Вероятность перехода из одного состояния в другое	0,4	0,39	0,4	0,54	0,41	0,47	0,44



■ ***Рис. 6.*** Зависимость показателя защищенности $P_{защ}$ от вероятности начала действий нарушителя P_{0-1}

■ ***Fig. 6.*** Dependencies of probability of realization of threats $P_{защ}$ from probability of transition from one state to another P_{0-1}



■ ***Рис. 7.*** Зависимости вероятности реализации угрозы и вероятности защищенности ИВС от времени при реализации метода адаптивного управления защитой с анализом динамики действий нарушителя

■ ***Fig. 7.*** Dependence of the probability of the threat realization and the probability of the ITT's protection against time for implementing the method of adaptive management of the IVS defense based on the analysis of the dynamics of the violator's actions

■ ***Таблица 3***. Сравнение предлагаемого и традиционного методов защиты ИВС

■ ***Table 3***. Comparison of proposed and traditional methods of protection of information network

Событие	Коэффициент реализуемости события при методе управления защитой ИВС		Время перехода из одного события в другое, ч, при методе управления защитой ИВС	
	адаптивном	традиционном	адаптивном	традиционном
S_1	0,8	0,8	14,4	14,4
S_{21}	0,8	0,9	12,48	11,04
S_{31}	0,9	0,9	12,77	14,06
S_{41}	0,8	0,8	13,79	12,75
S_{51}	0,9	0,9	11,6	12,52
X	0,5	0,9	18,2	12,73
Время реализации угрозы			**82,64**	**77,5**

времени на реализацию угрозы хищения информации, чем при использовании традиционного метода управления защитой ИВС, что и является положительным эффектом предлагаемого метода защиты ИВС.

Заключение

Разработан метод адаптивного управления защитой ИВС автоматизированной системы менеджмента организации интегрированной структуры, отличающийся от известных тем, что предложено применять результаты превентивного анализа динамики действий нарушителя. Данный метод включает мониторинг обстановки, оперативный контроль, распознавание последовательности действий нарушителя, моделирование стратегии воздействия нарушителя, процесс определения ситуационных параметров во взаимной противоборствующей обстановке с достоверным прогнозом стратегии вторжений.

Представлен алгоритм контроля ситуационных параметров при стохастической неопределенности. Предложена архитектура прототипа ИВС, а также сценарии экспериментов, проводимых с прототипом. Рассмотрены текущее состояние и процедура анализа динамики действий нарушителя. Этот подход возможно реализовать на программной эмуляции компонентов информационной системы введения нарушителя в заблуждение:

1) сегмента сети — где производится эмулирование работы выделенного сервера с контейнерной виртуализацией (дубликат сети с рабочими серверами);

2) дубликата хоста рабочих серверов (хост-приманка);

3) дубликата сервисов и приложений — программ, которые копируют работу сервисов и приложений.

Управление превентивной защитой ИВС на основе результатов анализа динамики действий нарушителя ведет администратор безопасности. Выделенный сервер с контейнерной виртуализацией и СОВ могут поддерживаться стандартными операционными системами, включаться как дополнительные средства в действующие системы безопасности, повышая вероятность защищенности ИВС.

Приведены экспериментальные результаты аналитического моделирования, которые показали, что предложенный подход обеспечивает требуемый уровень достоверности принимаемых решений, что позволяет повысить вероятностно-временные характеристики работы ИВС.

Литература

1. **Андрианов В. И., Красов А. В., Липатников В. А.** Инновационное управление рисками информационной безопасности. — СПб.: СПбГУТ им. проф. М. А. Бонч-Бруевича, 2012. — 396 с.
2. ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. http://docs.cntd.ru/document/1200058325 (дата обращения: 6.08.2018).
3. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий (с Поправкой). http://docs.cntd.ru/document/1200048398 (дата обращения: 6.08.2018).
4. **Липатников В. А, Шевченко А. А., Яцкин А. Д., Семенова Е. Г.** Управление информационной безопасностью организации интегрированной структуры на основе выделенного сервера с контейнерной виртуализацией // Информационно-управляющие системы. 2017. № 4. С. 67–76. doi:10.15217/issn1684-8853.2017.4.67
5. **Лукацкий А.** Обнаружение атак. — СПб.: БХВ-Петербург, 2008. — 304 с.

6. **Липатников В. А., Шевченко А. А.** Способ контроля уязвимостей при масштабировании автоматизированной системы менеджмента предприятия интегрированной структуры // Информационные системы и технологии. 2016. № 2(94). С. 128–140.
7. **Ivo Batina.** Model Predictive Control for Stochastic Systems by Randomized Algorithms. — Eindhoven: Technische Universiteit Eindhoven, 2004. — 157 p.
8. **Byres E., Lowe J.** The Myths and Facts Behind Cyber Security Risk for Industrial Control Systems // ISA Process Control Conf., 2003. P. 1–6. https://www.controlglobal.com/assets/Media/MediaManager/The_Myths_and_Facts_behind_Cyber_Security_Risks.pdf (дата обращения: 6.08.2018).
9. Пат. 2635256 РФ, МПК[51] G06F 12/14. Способ защиты информационно-вычислительной сети от несанкционированных воздействий / В. В. Карганов, С. В. Костарев, В. А. Липатников, А. И. Лобашев, А. А. Шевченко; заявитель и патентообладатель Федеральное государственное казенное военное образовательное учреждение высшего образования «Военная академия связи имени Маршала Советского Союза С. М. Буденного» Министерства обороны Российской Федерации. — № 2016117662; заявл. 04.05.2016; опубл. 09.11.2017, Бюл. № 31. — 2 с.
10. **Кузнецов И. А., Липатников В. А., Шевченко А. А.** Способ многофакторного управления безопасностью информационно-телекоммуникационной сети системы менеджмента качества предприятий интегрированных структур// Вопросы радиоэлектроники. 2016. № 6. С. 23–28.
11. **Baddar S. A.-H., Merlo A., Migliardi M.** Anomaly Detection in Computer Networks:A State-of-the-Art Review//Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications. 2014. Vol. 5. N 4. P. 29–64.
12. **Brindasri S., Saravanan K.** Evaluation of Network Intrusion Detection using Markov Chain//International Journal on Cybernetics & Informatics (IJCI). 2014. Vol. 3. N 2. P. 11–20.
13. **Babaie T., Chawla S., Ardon S.** Network Traffic Decomposition for Anomaly Detection. 2014. http://arxiv.org/pdf/1403.0157.pdf (дата обращения: 06.08.2018).
14. **Mazurek M., Dymora P.** Network Anomaly Detection based on the Statistical Selfsimilarity Factor for HTTP Protocol//Przegląd Elektrotechniczny. 2014. Vol. 90. N 1. P. 127–130.
15. **Japertas S., Cincikas G.** Company's Information and Telecommunication Networks Security Risk Assesment Algorithm. http://www.eejournal.ktu.lt/index.php/elt/article/download/1648/1425 (дата обращения: 06.08.2018).
16. Suricata. Open Source IDS/IPS/NSM Engine. http://suricata-ids.org/ (дата обращения: 6.08.2018).
17. **Ranjan R., Sahoo G.** A New Clustering Approach for Anomaly Intrusion Detection//International Journal of Data Mining & Knowledge Management Process (IJDKP). 2014. Vol. 4. N 2. P. 29–38.
18. **Sheth H., Shah B., Yagnik S.** A Survey on RBF Neural Network for Intrusion Detection System//International Journal of Engineering Research and Applications. 2014. Vol. 4. P. 17–22.
19. **Pawar S. N.** Intrusion Detection in Computer Network using Genetic Algorithm Approach: A Survey// International Journal of Advances in Engineering & Technology. 2013. Vol. 6. Iss. 2. P. 730–736.
20. **Dave M. H., Sharma S. D.** Improved Algorithm for Intrusion Detection using Genetic Algorithm and SNORT//International Journal of Emerging Technology and Advanced Engineering. 2014. P. 273–276.
21. **Браницкий А. А., Котенко И. В.** Анализ и классификация методов обнаружения сетевых атак // Тр. СПИИРАН. 2016. Вып. 2(45). С. 207–243.
22. **Ryan J., Lin M.-J.** Intrusion Detection with Neural Networks // Advances in Neural Information Processing Systems: Proc. of Conf. 1998. P. 943–949.
23. **Tan K.** The Applicationof Neural Networks to UNIX Computer Security // Proc. of the IEEE Intern. Conf. on Neural Networks. 1995. Vol. 1. P. 476–481.
24. ФСТЭК. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах. https://fstec.ru/component/attachments/download/290 (дата обращения: 6.08.2018).
25. **Липатников В. А., Шевченко А. А.** Модель процесса управления информационной безопасностью распределенной информационной системы на основе выявления и оценки уязвимостей // Информационные системы и технологии. 2018. № 1 (105). С. 114–123.

UDC 004.7, 004.056, 004.056.5
doi:10.31799/1684-8853-2018-4-61-72

Adaptive Management of Information Network Protection with Analysis of Intruder's Actions

Korshunov G. I.[a,b], Dr. Sc., Tech., Professor, kgi@pantes.ru
Lipatnikov V. A.[c], Dr. Sc., Tech., Professor, lipatnikovanl@mail.ru
Shevchenko A. A.[c], Junior Researcher, alex_pavel1991@mail.ru
Malyshev B. Y.[c], Science Company Senior Operator, bogdan160596@bk.ru
[a]Pantes, Ltd, Irinovskij Ave., 2, Let. A, 195248, Saint-Petersburg, Russian Federation
[b]Saint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaia St., 190000, Saint-Petersburg, Russian Federation
[c]S. M. Budyonny Military Academy of Telecommunication, 3, Tikhoretskii Ave., 194064, Saint-Petersburg, Russian Federation

Introduction: The known methods of adaptive management of information network protection with special security measures are not effective enough in modern conditions, as they only take into account collected and processed data on security events and do not analyze the dynamics of the actions. **Purpose:** Developing a method of adaptive control of information network protection based on the analysis of violator's actions. **Results:** A method has been proposed for adaptive management of information network protection. Unlike other known methods, it is based on analyzing the dynamics of the violator's actions and determining the situational confrontation parameters under stochastic uncertainty. The method includes situation monitoring, operational control of the sequence of violator's actions, modeling the attacker's strategy, determining the situational parameters with a reliable prediction of the intrusion strategy. During the analysis, the network administrator receives information about the priority purposes of an intruder, the tools used and the vulnerabilities of the network. This provides an opportunity to promptly take measures to increase the security of the network and avoid its compromise. **Practical relevance:** This approach allows you to maintain the operation of automated management systems for an organization with integrated structure, taking into account the scaling in planning and making changes to the structure on the background of information confrontation at the required level when multiple threats are changing their dynamics.

Keywords — Automated System, Management for an Organization, Integrated Structure, Information and Computer Network, Computer Attacks, Data Protection, Risk Assessment, Container Virtualization, Proactive Management, Scaling, Security Index.

Citation: Korshunov G. I., Lipatnikov V. A., Shevchenko A. A., Malyshev B. Y. Adaptive Management of Information Network Protection with Analysis of Intruder's Actions. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2018, no. 4, pp. 61–72 (In Russian). doi:10.31799/1684-8853-2018-4-61-72

References

1. Andrianov V. I., Krasov A. V., Lipatnikov V. A. *Innovatsionnoe upravlenie riskami informatsionnoj bezopasnosti* [Innovative Management of Information Security Risks]. Saint-Petersburg, SPbGUT im. prof. M. A. Bonch-Bruevicha Publ., 2012. 396 p. (In Russian).
2. State Standard R ISO/MEHK 27001-2006. Information Technology. Methods of Protection. Information Security Management Systems. Requirements. Available at: http:// http://docs.cntd.ru/document/1200058325 (accessed 6 August 2018).
3. State Standard R ISO/MEHK 13335-1-2006. Information Technology. Methods and Means of Ensuring Security. Part 1. The Concept and Models of Security Management of Information and Telecommunication Technologies. Available at: http: // docs.cntd.ru/document/1200048398 (accessed 6 August 2018).
4. Lipatnikov V. A., Shevchenko A. A., Yatskin A. D., Semenova E. G. Information Security Management of Integrated Structure Organization based on a Dedicated Server with Container Virtualization. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2017, no. 4, pp. 67–76 (In Russian). doi:10.15217/issn1684-8853.2017.4.67
5. Lukatsky A. *Obnaruzhenie atak* [Detection of Attacks]. Saint-Petersburg, BKhV-Peterburg Publ., 2008. 304 p. (In Russian).
6. Lipatnikov V. A., Shevchenko A. A. A Way to Control Vulnerabilities when Scaling an Automated Enterprise Management System of an Integrated Structure. *Informatsionnye sistemy i tekhnologii* [Information Systems and Technologies], 2016, no. 2 (94), pp. 128–140 (In Russian).
7. Ivo Batina. *Model Predictive Control for Stochastic Systems by Randomized Algorithms*. Eindhoven, Technische Universiteit Eindhoven, 2004. 157 p.
8. Byres E., Lowe J. The Myths and Facts Behind Cyber Security Risk for Industrial Control Systems. *ISA Process Control Conference*, 2003, pp. 1–6. Available at: https:// www.controlglobal.com/assets/Media/MediaManager/ The_Myths_and_Facts_behind_Cyber_Security_Risks. pdf (accessed 6 August 2018).
9. Karganov V. V., et al. *Sposob zaschity informatsionno-vychislitel'noj seti ot nesanktsionirovannykh vozdejstvij* [A Way to Protect the Information Network from Unauthorized Influences]. Patent RF, no. 2016117662, 2017.
10. Kuznetsov I. A., Lipatnikov V. A., Shevchenko A. A. The Way of Multifactor Management of the Security of the Information and Telecommunications Network of the Quality Management System of Enterprises of Integrated Structures. *Voprosy radioehlektroniki* [Questions of Radio Electronics], 2016, no. 6, pp. 23–28 (In Russian).
11. Baddar S. A.-H., Merlo A., Migliardi M. Anomaly Detection in Computer Networks: A State-of-the-Art Review. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 2014, vol. 5, no. 4, pp. 29–64.
12. Brindasri S., Saravanan K. Evaluation of Network Intrusion Detection using Markov Chain. *International Journal on Cybernetics & Informatics (IJCI)*, 2014, vol. 3, no. 2, pp. 11–20.
13. Babaie T., Chawla S., Ardon S. *Network Traffic Decomposition for Anomaly Detection*. 2014. Available at: http://arxiv.org/pdf/1403.0157.pdf (accessed 6 August 2018).
14. Mazurek M., Dymora P. Network Anomaly Detection based on the Statistical Selfsimilarity Factor for HTTP Protocol. *Przegląd Elektrotechniczny*, 2014, vol. 90, no. 1, pp. 127–130.
15. Japertas S., Cincikas G. *Company's Information and Telecommunication Networks Security Risk Assesment Algorithm*. Available at: http://www.eejournal.ktu.lt/index.php/elt/article/download/1648/1425 (accessed 6 August 2018).
16. *Suricata. Open Source IDS/IPS/NSM Engine*. Available at: http://suricata-ids.org/ (accessed 6 August 2018).
17. Ranjan R., Sahoo G. A New Clustering Approach for Anomaly Intrusion Detection. *International Journal of Data Mining & Knowledge Management Process (IJDKP)*, 2014, vol. 4, no. 2, pp. 29–38.
18. Sheth H., Shah B., Yagnik S. A Survey on RBF Neural Network for Intrusion Detection System. *International Journal of Engineering Research and Applications*, 2014, vol. 4, pp. 17–22.

19. Pawar S. N. Intrusion Detection in Computer Network using Genetic Algorithm Approach: A Survey. *International Journal of Advances in Engineering & Technology*, 2013, vol. 6, iss. 2, pp. 730–736.
20. Dave M. H., Sharma S. D. Improved Algorithm for Intrusion Detection using Genetic Algorithm and SNORT. *International Journal of Emerging Technology and Advanced Engineering*, 2014, pp. 273–276.
21. Branitsky A. A., Kotenko I. V. Analysis and Classification of Methods for Detecting Network Attacks. *Trudy SPIIRAN* [SPIIRAS Proceedings], 2016, vol. 2 (45), pp. 207–243 (In Russian).
22. Ryan J., Lin M.-J. Intrusion Detection with Neural Networks. *Proc. of conf. "Advances in Neural Information Processing Systems"*, 1998, pp. 943–949.
23. Tan K. The Application of Neural Networks to UNIX Computer Security. *Proc. of the IEEE Intern. Conf. on Neural Networks*, 1995, vol. 1, pp. 476–481.
24. *FSTEHK. Metodika opredeleniya aktual'nykh ugroz bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh* [Methodology for Determining Actual Threats to the Security of Personal Data when Processing them in Information Systems]. Available at: https://fstec.ru/component/attachments/download/290 (accessed 6 August 2018).
25. Lipatnikov V. A., Shevchenko A. A. Model of Information Security Management Process of Distributed Information System based on Vulnerability Detection and Evaluation. *Informatsionnye sistemy i tekhnologii* [Information Systems and Technologies], 2018, no. 1 (105), pp. 114–123 (In Russian).

Уважаемые авторы!

При подготовке рукописей статей необходимо руководствоваться следующими рекомендациями.

Статьи должны содержать изложение новых научных результатов. Название статьи должно быть кратким, но информативным. В названии недопустимо использование сокращений, кроме самых общепринятых (РАН, РФ, САПР и т. п.).

Объем статьи (текст, таблицы, иллюстрации и библиография) не должен превышать эквивалента в 20 страниц, напечатанных на бумаге формата А4 на одной стороне через 1,5 интервала Word шрифтом Times New Roman размером 13, поля не менее двух сантиметров.

Обязательными элементами оформления статьи являются: индекс УДК, заглавие, инициалы и фамилия автора (авторов), ученая степень, звание (при отсутствии — должность), полное название организации, аннотация и ключевые слова на русском и английском языках, электронные адреса авторов, которые по требованию ВАК должны быть опубликованы на страницах журнала. При написании аннотации не используйте аббревиатур и не делайте ссылок на источники в списке литературы. Предоставляйте подрисуночные подписи и названия таблиц на русском и английском языках.

Статьи авторов, не имеющих ученой степени, рекомендуется публиковать в соавторстве с научным руководителем, наличие подписи научного руководителя на рукописи обязательно; в случае самостоятельной публикации обязательно предоставляйте заверенную по месту работы рекомендацию научного руководителя с указанием его фамилии, имени, отчества, места работы, должности, ученого звания, ученой степени — эта информация будет опубликована в ссылке на первой странице.

Формулы набирайте в Word, не используя формульный редактор (Mathtype или Equation), при необходимости можно использовать формульный редактор; для набора одной формулы не используйте два редактора; при наборе формул в формульном редакторе знаки препинания, ограничивающие формулу, набирайте вместе с формулой; для установки размера шрифта никогда не пользуйтесь вкладкой Other…, используйте заводские установки редактора, не подгоняйте размер символов в формулах под размер шрифта в тексте статьи, не растягивайте и не сжимайте мышью формулы, вставленные в текст; в формулах не отделяйте пробелами знаки: + = –.

Для набора формул в Word никогда не используйте Конструктор (на верхней панели: «Работа с формулами» — «Конструктор»), так как этот ресурс предназначен только для внутреннего использования в Word и не поддерживается программами, предназначенными для изготовления оригинал-макета журнала.

При наборе символов в тексте помните, что символы, обозначаемые латинскими буквами, набираются светлым курсивом, русскими и греческими — светлым прямым, векторы и матрицы — прямым полужирным шрифтом.

Иллюстрации предоставляются отдельными исходными файлами, поддающимися редактированию:

— рисунки, графики, диаграммы, блок-схемы предоставляйте в виде отдельных исходных файлов, поддающихся редактированию, используя векторные программы: Visio (*.vsd, *.vsdx); Coreldraw (*.cdr); Excel (*.xls); Word (*.docx); Adobe Illustrator (*.ai); AutoCad (*.dxf); Matlab (*.ps, *.pdf или экспорт в формат *.ai);

— если редактор, в котором Вы изготавливаете рисунок, не позволяет сохранить в векторном формате, используйте функцию экспорта (только по отношению к исходному рисунку), например, в формат *.ai, *.esp, *.wmf, *.emf, *.svg;

— фото и растровые — в формате *.tif, *.png с максимальным разрешением (не менее 300 pixels/inch).

Наличие подрисуночных подписей обязательно (желательно не повторяющих дословно комментарии к рисункам в тексте статьи).

В редакцию предоставляются:

— сведения об авторе (фамилия, имя, отчество, место работы, должность, ученое звание, учебное заведение и год его окончания, ученая степень и год защиты диссертации, область научных интересов, количество научных публикаций, домашний и служебный адреса и телефоны, e-mail), фото авторов: анфас, в темной одежде на белом фоне, должны быть видны плечи и грудь, высокая степень четкости изображения без теней и отблесков на лице, фото можно представить в электронном виде в формате *.tif, *.png с максимальным разрешением — не менее 300 pixels/inch при минимальном размере фото 40×55 мм;

— экспертное заключение.

Список литературы составляется по порядку ссылок в тексте и оформляется следующим образом:

— для книг и сборников — фамилия и инициалы авторов, полное название книги (сборника), город, издательство, год, общее количество страниц;

— для журнальных статей — фамилия и инициалы авторов, полное название статьи, название журнала, год издания, номер журнала, номера страниц;

— ссылки на иностранную литературу следует давать на языке оригинала без сокращений;

— при использовании web-материалов указывайте адрес сайта и дату обращения.

Список литературы оформляйте двумя отдельными блоками по образцам lit.dot на сайте журнала (http://i-us.ru/paperrules) по разным стандартам: Литература — СИБИД РФ, References — один из мировых стандартов.

Более подробно правила подготовки текста с образцами изложены на нашем сайте в разделе «Оформление статей».

Контакты
Куда: 190000, Санкт-Петербург,
Б. Морская ул., д. 67, ГУАП, РИЦ
Кому: Редакция журнала «Информационно-управляющие системы»
Тел.: (812) 494-70-02
Эл. почта: ius.spb@gmail.com
Сайт: www.i-us.ru