УДК 004.7 DOI: 10.17587/it.25.3-10

В. В. Карганов, ст. науч. сотр., канд. техн. наук, доц., e-mail: vitalik210277@mail.ru,
А. А. Шевченко, мл. науч. сотр., e-mail: alex_pavel1991@mail.ru,
Б. Ю. Малышев, оператор научной роты, e-mail: bogdan160596@bk.ru,
Военная академия связи имени Маршала Советского Союза С. М. Буденного, Санкт-Петербург

Способ повышения работоспособности информационно-вычислительной сети за счет адаптивного управления защитой

Рассмотрен способ повышения работоспособности информационно-вычислительной сети, который аккумулирует знания о состоянии и развитии системы управления, методах и инструментах его применения в системных объектах. Инструментом решения является метод адаптивного управления защитой информационно-вычислительных сетей, отличающийся от известных тем, что предлагается применять результаты анализа динамики действий нарушителя. Представлены результаты расчетов.

Ключевые слова: *информационная безопасность, информационно-вычислительная сеть, контейнерная виртуализация, система обнаружения вторжений, угроза, нарушитель*

Введение

В связи с быстрым развитием компьютерных технологий, в том числе появлением 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 проблем [1]. Кроме того, в ходе проведения анализа соответствующих источников в данной предметной области исследования [2—5] было выявлено, что к средствам защиты в настоящее время предъявляются более жесткие требования.

В статье [6] рассматривается способ обеспечения ИБ информационно-вычислительной сети (ИВС) путем реализации ложной сети на основе выделенного сервера с контейнерной виртуализацией [4, 7]. Однако при управлении ИВС не используются данные анализа динамики действий нарушителя. В статье [8] рассматривается способ контроля уязвимостей при масштабировании ИВС без учета динамики действий нарушителя.

При исследовании данных способов защиты ИВС недостаточно внимания уделено анализу динамики действий нарушителя, которые включают сценарии внешних и внутренних вторжений. Возникает противоречие между эффективными новыми средствами информационного вторжения и существующими способами защиты ИВС. Поэтому задача защиты ИВС от вторжений со стороны нарушителей является актуальной.

1. Цель, постановка задачи, условия и ограничения

Целью данной работы является повышение ИБ и работоспособности ИВС за счет анализа динамики действий нарушителя.

Постановка задачи: разработать метод адаптивного управления защитой ИВС на основе анализа динамики действий нарушителя путем контроля ситуационных параметров во взаимной противоборствующей обстановке при стохастической неопределенности [9, 10].

Условия и ограничения: метод адаптивного управления защитой ИВС должен включать

в себя 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.

2. Предлагаемое решение

Рассмотрена возможная структура ИВС, представленная на рис. 1.

Данная ИВС имеет топологию "Звезда" и включает в себя межсетевой экран, систему обнаружения вторжений, выделенный сервер с контейнерной виртуализацией, центр обработки данных, коммутаторы 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 путем заманивая нарушителей на ложные информационные системы и проводить сбор информации о тактике нарушителя, осуществлять идентификацию и нейтрализацию.

В результате сочетания достоверного анализа и прогнозирования динамики действий предлагается адаптировать защиту ИВС, за счет чего должно обеспечиваться повышение оперативности отслеживания фаз развития кризисных ситуаций. На основании анализа деятельности нарушителя определяются слабые стороны системы защиты информации в ИВС.

Метод решения 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 аналогично тому, как изложено в источниках [6, 11]. Учитывается динамический характер модели нарушителя, поэтому поиск и устранение уязвимостей в защите также являются динамически изменяющимися во времени процессами.

Цифровой поток, входящий и исходящий из сети Интернет, вначале проходит предварительную фильтрацию межсетевым экраном, после чего он поступает в систему обнаружения вторжений и анализируется с точки зрения наличия атак [4]. В случае, когда внутренний нарушитель пытается получить несанкционированный доступ к ресурсам ИВС, происходит анализ запросов, и если критический параметр больше допустимого уровня, то цифровой поток перенаправляется на компоненты ложной информационной системы, легитимные же запросы, удовлетворяющие требованиям политик безопасности системы обнаружения вторжений, перенаправляются на истинную информационную систему. Если же системе обнаружения вторжений не удалось обнаружить атаку на сетевом уровне, но при этом действия нарушителя были выявлены после их реализации на определенных хостах информационной системы, осуществляется перенаправление последующего цифрового потока нарушителя на компоненты выделенного сервера с контейнерной виртуализацией.

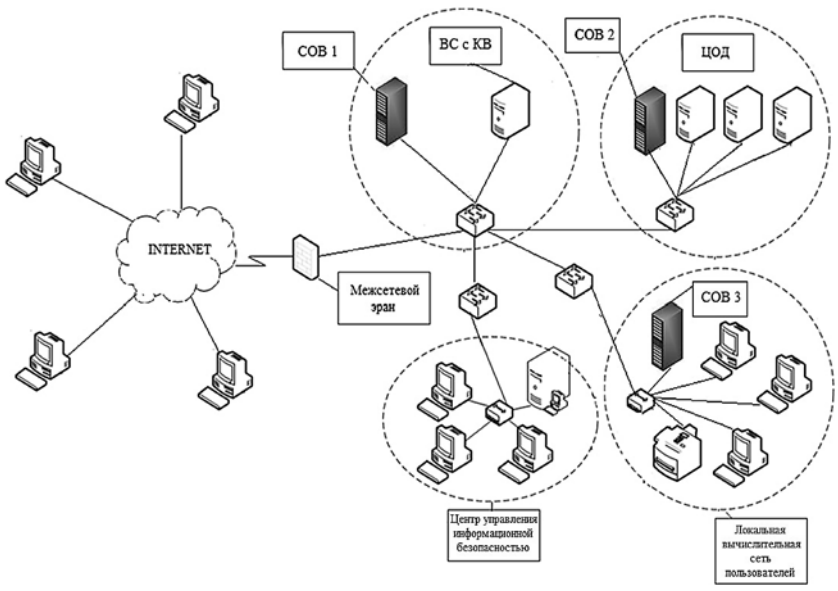

Рис. 1. Структура информационно-вычислительной сети (вариант)

Результаты анализа работ [3—5, 7, 12] позволяют описать процесс мониторинга обстановки. Цифровой поток поступает в систему обнаружения вторжений, после чего происходит сканирование по заданным параметрам, в результате из всего цифрового потока выделяется только тот, который попадает под определенные критерии. После этого происходит выделение признаков и дальнейший анализ. Анализ осуществляется за счет уже имеющихся баз данных угроз. В случае соответствия цифрового потока критериям угроз проводится анализ моделей угроз, после чего принимается решение по защите ИВС.

Когда не удается однозначно определить, какого рода цифровой

поток, он отсеивается (блокируется) и перенаправляется на развернутую вычислительную сеть, и далее запросы такого рода анализируются, после чего принимаются меры по разрешению или запрете доступа. Далее выполняется обновление баз данных с учетом обнаруженных инцидентов.

На рис. 2 изображен алгоритм построения и функционирования рассматриваемой ИВС.

Данный алгоритм включает в себя два параллельных процесса:

1. Тестирование ИВС и выявление уязвимостей. Данное действие представлено в статьях [8, 13] и реализовано в работе [14].

2. Анализ цифрового потока с выявлением аномалий и последующим анализом динамики действий нарушителя. На основании динамики действий нарушителя строится модель угроз и принимаются меры по защите. Данный метод помогает защитить реальную информационную систему от компьютерных атак за счет анализа действий, выполняемых нарушителями, и принятия рациональных мер по защите реальных и возможных уязвимостей в данной сети [15].

Обобщенный алгоритм анализа действий нарушителя для данного вида атак представлен на рис. 3.

В соответствии с тем, обнаружены ли атаки на граничном хосте, их можно разделить на два типа [16—20]: обнаруживаемые и не обнаруживаемые атаки.

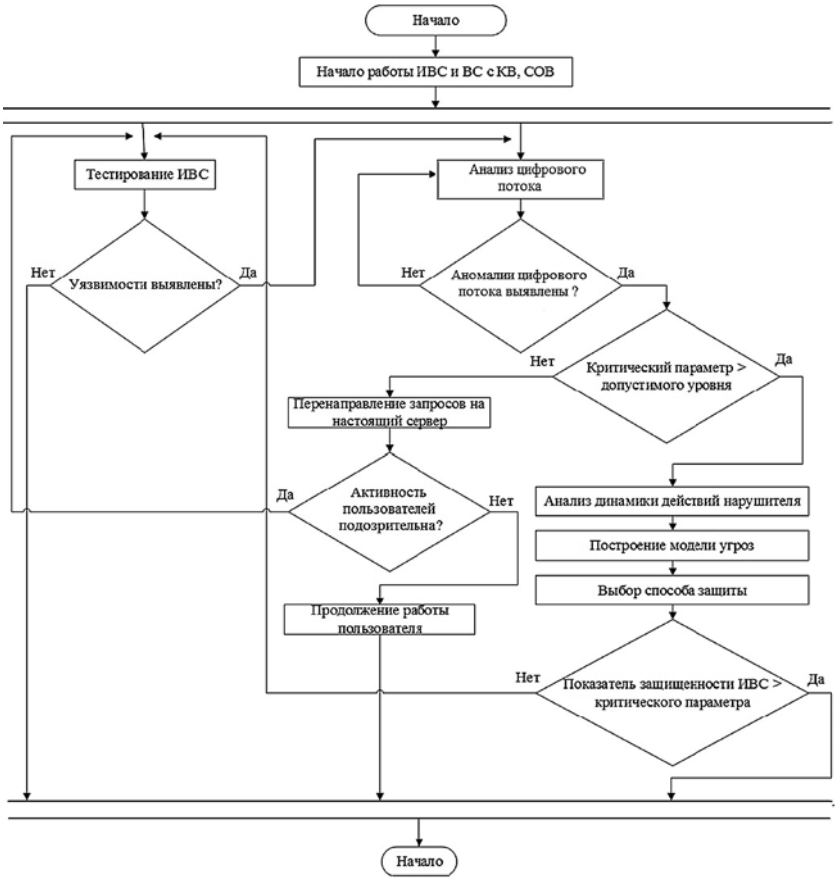

Рис. 2. Обобщенный алгоритм функционирования ИВС (ВС с КВ — выделенный сервер с контейнерной виртуализацией; СОВ — система обнаружения вторжений)

Рис. 3. Общий алгоритм анализа действий нарушителя

Атаки первой группы блокируются граничным хостом, не достигая рабочих серверов. При обнаружении такого рода атак система обнаружения вторжения (СОВ) должна изменять свою конфигурацию, чтобы последующие действия нарушителя перенаправлялись на ложные ИС. К атакам второго вида относят атаки, параметры которых не известны, а также атаки внутренних нарушителей через терминалы пользователей.

На основе возможных реализаций уязвимостей ИВС [21] составим модель нарушителя. 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. 4 представлен вариант графа событий действий нарушителя.

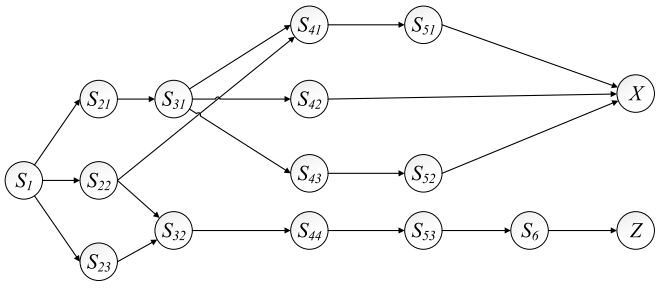

Рис. 4. Граф событий действий нарушителя (вариант)

В качестве одной из возможных моделей можно использовать представление действий нарушителя как систему с переменной структурой, поведение которой на случайных интервалах времени характеризуется различными структурами и описывается вероятностными законами [22, 23]. При этом переход одной структуры в другую происходит в случайный момент времени в зависимости от значения фазовых координат системы.

- событие "S_1" соответствует началу действий нарушителя;
- событие "S_{21}" соответствует событию, в котором происходит измерение характеристик ИВС путем внедрения анализатора трафика;
- событие "S_{22}" соответствует стадии, в которой проводится тестирование состояния ИВС путем анализа запросов;
- событие "S_{23}" соответствует событию анализа "эхо-запросов";
- событие "S_{31}" соответствует событию анализа исходящего цифрового потока;
- событие "S_{32}" соответствует событию выявления хостов;
- событие "S_{41}" соответствует событию выявления паролей;
- событие "S_{42}" соответствует событию дешифрования информации;
- событие "S_{43}" соответствует событию, при котором несанкционированно используется авторизованный IP-адрес в сети;
- событие "S_{44}" соответствует событию, при котором происходит сканирование портов;
- событие "S_{51}" соответствует событию подмены пользователя в сети;
- событие "S_{52}" соответствует событию, при котором изменяются целостность, доступность и конфиденциальность информации;
- событие "S_{53}" соответствует событию, при котором происходит анализ характеристик приложений;
- событие "S_6" соответствует режиму осуществления DDoS атак;
- событие "X" соответствует реализации угрозы хищения информации;
- событие "Z" соответствует реализации отказа в обслуживании.

Для разделения вариантов возможных сценариев развития событий используется схема "дерева вероятностей". Каждая ветвь представляет собой отдельный сценарий развития [21, 24]. На рис. 4 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 вероятности реализуемости событий (элементов графа) для определения динамики действий нарушителя, воспользовавшись методикой работы [25]:

$$P = \frac{K_1 + K_2}{20}, \quad (1)$$

где K_1 — коэффициент исходной защищенности; K_2 — коэффициент реализации угрозы.

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

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

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

Результаты вычислительного эксперемента, основанного на методике [25] и формулах (1) и (2), представлены в табл. 1.

Для определения наиболее вероятного пути реализации угроз небходимо рассчитать вероятности наступления каждого события из графа. Для расчета вероятности наступления события X и Z воспользуемся формулой расчета сложения вероятностей:

$$P_{\text{р}} = P_{(i)} + P_{(i+1)} - P_{(i)} P_{(i+1)},$$

где $P_{(i)}$, $P_{(i+1)}$ _ вероятность наступления двух последующих событий.

Результаты расчета вероятности наступления события реализации угрозы хищения информации по возможному пути $S_{x1} = \{S_1, S_{21}, S_{31}, S_{41}, S_{51}, X\}$:

$$P_1 = P_{S_1} + P_{S_{21}} - (P_{S_1} \times P_{S_{21}}) = 0,36;$$
$$P_2 = P_1 + P_{S_{31}} - (P_1 \times P_{S_{31}}) = 0,584;$$
$$P_3 = P_2 + P_{S_{41}} - (P_2 \times P_{S_{41}}) = 0,75;$$
$$P_4 = P_3 + P_{S_{51}} - (P_3 \times P_{S_{51}}) = 0,9;$$
$$P_{\text{общ}} = P_4 + P_X - (P_4 \times P_X) = 0,99.$$

Таблица 1

Коэффициенты реализуемости возможных событий и время перехода из одного события в другое

Путь S_{x1}	События	S_1	S_{21}	S_{31}	S_{41}	S_{51}	X	
	K_1	9	9	9	9	9	9	
	K_2	7	9	9	7	9	1	
	Время перехода одного события в другое T, ч	14,4	12,48	12,77	13,79	11,6	18,2	
Путь S_{x2}	События	S_1	S_{21}	S_{31}	S_{42}	X		
	K_1	9	9	9	9	9		
	Y_2	7	9	9	3	1		
	Время перехода одного события в другое T, ч	14,4	12,48	12,77	16,34	15,8		
Путь S_{x3}	События	S_1	S_{21}	S_{31}	S_{43}	X		
	K_1	9	9	9	9	9		
	K_2	7	9	9	1	1		
	Время перехода одного события в другое T, ч	14,4	12,48	12,77	17,62	15,19		
Путь S_{x4}	События	S_1	S_{21}	S_{31}	S_{43}	S_{52}	X	
	K_1	9	9	9	9	9	9	
	K_2	7	9	9	1	1	1	
	Время перехода одного события в другое T, ч	14,4	12,48	12,77	17,62	15,19	16,41	
Путь S_{x5}	События	S_1	S_{22}	S_{41}	S_{51}	X		
	K_1	9	9	9	9	9		
	K_2	7	7	7	9	1		
	Время перехода одного события в другое T, ч	14,4	12,48	14,02	11,39	18,31		
Путь S_{z1}	События	S_1	S_{21}	S_{32}	S_{44}	P_{53}	P_6	Z
	K_1	9	9	9	9	9	9	9
	K_2	7	9	4	9	9	7	4
	Время перехода одного события в другое T, ч	14,4	11,04	16,82	8,86	16,03	11,18	16,73
Путь S_{z2}	События	S_1	S_{23}	S_{32}	S_{44}	S_{53}	S_6	Z
	K_1	9	9	9	9	9	9	9
	K_2	7	4	4	9	9	7	4
	Время перехода одного события в другое T, ч	14,4	14,64	14,48	10,97	14,13	12,69	15,75

По аналогии рассчитывается вероятность наступления событий по всем путям графа. Результаты расчета завимости вероятности реализации угроз от времени представлены на рис. 5 (см. вторую сторону обложки).

На рис. 5 S_{x1}, S_{x2}, S_{x3}, S_{x4}, S_{x5}, S_{z1}, S_{z2} — пути реализации угроз X и Z; t_1, t_2, t_3 — время, которое понадобится нарушителю для реализации угроз с учетом вариаций возможных действий нарушителя. Если произойдет событие S_1, то для достижения угрозы хищения информации нарушитель выберет путь реализации S_{x2}, S_{x5}, а для достижения угрозы отказа в обслуживании он выберет путь S_{z2}.

Рассмотрим предлагаемый метод для анализа динамики действий нарушителя на примере защиты от угрозы хищения информации по пути реализации S_{x2}. На рис. 6 (см. вторую сторону обложки) представлена зависимость вероятности реализации угрозы и вероятности защищенности ИВС от времени реализации метода адаптивного управления защитой ИВС на основе анализа динамики действий нарушителя.

В промежуток времени t_1 происходит внедрение анализатора трафика. В момент времени t_2 происходит обнаружение системой обнаружения вторжений 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 V_{31} уже невозможна, в силу снижения вероятности реализации угрозы к нулю защищенность вернется на уровень в 95 %.

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

Таблица 2

Сравнение адаптивного и традиционного методов управления защитой ИВС

Событие	Коэффициент реализуемости события		Время перехода одного события в другое, ч	
	Адаптивный метод управления защитой ИВС	Традиционный метод управления защитой ИВС	Адаптивный метод управления защитой ИВС	Традиционный метод управления защитой ИВС
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**

Результаты сравнительного анадиза адаптивного и традиционного методов управления защитой ИВС представлены в табл. 2. Анализ проводили на основе вычислительного эксперимента в предложенном варианте ИВС с помощью методики [25].

При использовании адаптивного метода управления защитой ИВС нарушитель потратит на 7 % больше времени на реализацию угрозы хищения информации, чем при использовании традиционного метода, что и является положительным эффектом предлагаемого метода защиты ИВС на основе анализа динамики действий нарушителя.

Заключение

Разработан способ повышения работоспособности ИВС за счет адаптивного управления защитой ИВС, отличающийся от известных методов, основанных на использовании специальных мер защиты, тем, что предложено применять результаты анализа динамики действий нарушителя. Предусмотрен алгоритм контроля ситуационных параметров во взаимной противоборствующей обстановке при стохастической неопределенности. Представлена архитектура прототипа этой системы, а также сценарии экспериментов, проводимых с прототипом. Рассмотрены текущее состояние и процедура анализа динамики действий нарушителя. Этот подход можно реализовать на программной эмуляции компонентов информационной системы введения нарушителя в заблуждение:

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

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

3) дубликат сервисов и приложений — программы, которые копируют работу сервисов и приложений.

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

Список литературы

1. **Андрианов В. И., Красов А. В., Липатников В. А.** Инновационное управление рисками информационной безопасности. СПб.: Изд. Федеральное агентство связи, Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2012. С. 396.

2. **Карганов В. В., Левченко Г. Н., Драчев В. О., Котяшичев И. А.** К вопросу о существующих методах защиты информации в информационных системах // Матер. конф. ГНИИ "Нацразвитие". 2017. С. 108—117.

3. **Карганов В. В.** Концептуальные подходы качества обработки информации в информационной системе // Матер. конф. ГНИИ "Нацразвитие". 2017. С. 100—107.

4. **ИСО/МЭК 27001.** Информационные технологии. Методы защиты. Системы менеджмента защиты информации. Требования. Международный стандарт ISO. URL: http://www.novsu.ru/file/1020711 (дата обращения: 15.07.2018).

5. **ГОСТ Р ИСО/МЭК 13335-1-2006**. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий // ГОСТ-эксперт. URL:http://gostexpert.ru/gost/gost-13335-1-2006 (дата обращения: 15.07.2018).

6. **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 (89). С. 67—76. Doi:10.15217/issn1684-8853.2017.4.67.

7. **Лукацкий А.** Обнаружение атак. СПб.: БХВ-Петербург, 2008. 304 с.

8. **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.

9. **Batina I.** Model predictive control for stochastic systems by randomized algorithms. Eindhoven: Technische Universiteit Eindhoven, 2004.

10. **Byres E., Lowe J.** The myths and facts behind cyber security risk for industrial control systems // In ISA Process Control Conference, 2003.

11. **Вандич А. П., Яичкин М. А., Карганов В. В., Привалов А. А., Скуднева Е. В.** К вопросу об организации инфор-

мационного обмена для повышения защищенности сети передачи данных от технической компьютерной разведки // Труды ЦНИИС. Санкт-Петербургский филиал. 2017. Т. 1, № 4. С. 72—78.

12. **Карганов В. В., Драчев В. О., Левченко Г. Н.** Формирование модели предметной области для информационной системы // Инновационные технологии и технические средства специального назначения. Тр. десятой общерос. науч.-практ. конф. 2018. С. 264—268.

13. **Карганов В. В., Пилявец О. Г., Шевченко А. А.** К вопросу предупреждения и обеспечения требуемого уровня информационной безопасности информационно-вычислительной сети специального назначения от несанкционированных воздействий // Вопросы оборонной техники. Сер. 16. Технические средства противодействия терроризму. 2018. № 1—2 (115—116). С. 78—85.

14. **Патент 2635256.** Российская Федерация, МПК G06F 12/14. Способ защиты информационно-вычислительной сети от несанкционированных воздействий / Карганов В. В., Костарев С. В., Липатников В. А., Лобашев А. И., Шевченко А. А.; 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.

15. **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.

16. **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.

17. **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.

18. **Mazurek M., Dymora P.** Network anomaly detection based on the statistical selfsimilarity factor for HTTP protocol // Przeglad elektrotechniczny. 2014. P. 127—130.

19. **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.

20. **Sheth H., Shah B., Yagnik S.** A survey on RBF Neural Network for Intrusion Detection System // Int. Journal of Engineering Research and Applications. 2014. Vol. 4. P. 17—22.

21. **Браницкий А. А., Котенко И. В.** Анализ и классификация методов обнаружения сетевых атак // Тр. СПИИРАН. 2016. Вып. 2(45). С. 207—243.

22. **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.

23. **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.

24. **Ryan J., Lin M.-J.** Intrusion Detection with Neural Networks // Advances in Neural Information Processing Systems. 1998. P. 943—949.

25. **ФСТЭК.** Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах. URL: https://fstec.ru/component/attachments/download/290 (дата обращения: 15.07.2018).

V. V. Karganov, Senior Research Assistant, Candidate Of Technical Sciences, Associate Professor, e-mail: vitalik210277@mail.ru,
A. A. Shevchenko, Junior Research Assistant, e-mail: alex_pavel1991@mail.ru,
B. Y. Malyshev, Operator Of Scientist Company, e-mail: bogdan160596@bk.ru,
S. M. Budyonny Military Academy of Communications, Saint Petersburg, Russia

Method of Increase in Operability of an Information Network Due to the Adaptive Information Security Management

In article describes adaptive management, which is a separate type of management, namely, flexible and innovative. It accumulates knowledge about condition and development of the control system, methods and tools of its application in system objects. The solution tool is a method of adaptive control of informatively — computer network security (IAS), which differs from the known ones, in that the analysis results of the dynamics violator's actions are applied. The method contains: monitoring of the situation, operational control, recognition of the sequence of actions of the violator, modeling the strategy of influence of the violator, the process of determining the situational parameters with a reliable forecast of the invasion strategy. In the process of analysis, the network administrator receives information about the priority goals of the offender, the means used by him and the vulnerabilities of various elements, which makes it possible to quickly take measures to improve the security of the network and avoid compromising it. The situational parameters control algorithm in the mutual opposing situation at stochastic uncertainty is provided. The architecture of the prototype of this system is presented, as well as scenarios of experiments conducted with the prototype. The current state and the procedure for analyzing the dynamics of the violator's actions are considered. The results of calculations in tabular form are presented, namely: probabilities of realizability of possible events time of transition from one event to another; the timing of the realization of the threat of information theft X on the way P_{x1} using methods of adaptive management and the traditional protection of the IVS. Presented the calculation results of dependence probability of threats: from time to time, the probability of protection IVS for implementation of the proposed method based on the analysis of the dynamics offender's actions. The conclusions, the essence of which lies in the fact that the use of the method allows to maintain the efficiency of IVS at the required level with the dynamics of changing the threats set, taking into account the scaling in the planning and making changes to it in the conditions of information confrontation.

Keywords: *the automated organization management system of integrated structure, data-processing network, information security, computer attacks, information security, risk assessment, container virtualization, proactive management, scaling, protectability index, system of detection of invasions, threat, violator*

DOI: 10.17587/it.25.3-10

References

1. **Andrianov V. I., Krasov A. V., Lipatnikov V. A.** *Innovacionnoe upravlenie riskami informacionnoj bezopasnosti* (Innovation information security risk management), SPb., Federal'noe agentstvo svyazi, Sankt-Peterburgskij gosudarstvennyj universitet telekommunikacij im. prof. M. A. Bonch-Bruevicha, 2012, pp. 396 (in Russian).

2. **Karganov V. V., Levchenko G. N., Drachev V. O., Kotyashichev I. A.** *K voprosu o sushchestvuyushchih metodah zashchity informacii v informacionnyh sistemah* (Revisited actual methods of guarding in information systems), *Materialy konferencii GNII "NACRAZVITIE",* 2017, pp. 108—117 (in Russian).

3. **Karganov V. V.** *Konceptual'nye podhody kachestva obrabotki informacii v informacionnoj sisteme* (Conceptual accesses quality of information handling in data system), *Materialy konferencij GNII "NACRAZVITIE",* 2017, pp. 100—107 (in Russian).

4. **ISO/MEHK 27001.** *Informacionnye tekhnologii. Metody zashchity. Sistemy menedzhmenta zashchity informacii. Trebovaniya* (Information technology. Security techniques. Information security management system. Requirements), Mezhdunarodnyi standart ISO, available at: http://www.novsu.ru/file/1020711 (date of access: 15.07.2018) (in Russian).

5. **GOST R ISO/MEHK 13335-1-2006.** *Informacionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. CHast' 1. Koncepciya i modeli menedzhmenta bezopasnosti informacionnyh i telekommunikacionnyh tekhnologii* (Information technology. Security techniques. Part 1. Concepts and models for information and communications technology security management), GOSTehkspert, available at: http://gostexpert.ru/gost/gost-13335-1-2006 (date of access: 15.07.2018) (in Russian).

6. **Lipatnikov V. A., Shevchenko A. A., Yackin A. D., Semenova E. G.** *Upravlenie informacionnoj bezopasnost'yu organizacii integrirovannoj struktury na osnove vydelennogo servera s kontejnernoj virtualizaciej* (Information security management of the integrated structure organization based on a dedicated server with a container virtualization), *Informacionno-Upravlyayushchie Sistemy*, 2017, no. 4 (89), pp. 67—76, doi:10.15217/issn1684-8853.2017.4.67 (in Russian).

7. **Lukackii A.** *Obnaruzhenie atak* (Detection of computer attacks), SPb., BHV-Peterburg, 2008, 304 p. (in Russian).

8. **Lipatnikov V. A., Shevchenko A. A.** *Sposob kontrolya uyazvimostej pri masshtabirovanii avtomatizirovannoj sistemy menedzhmenta predpriyatiya integrirovannoj struktury* (The vulnerability control method applying while automated integrated structure organization management system scaling), *Informacionnye Sistemy i Tekhnologii*, 2016, no.2(94), pp. 128—140 (in Russian).

9. **Ivo Batina.** Model predictive control for stochastic systems by randomized algorithms, Eindhoven, Technische Universiteit Eindhoven, 2004.

10. **Byres E., Lowe J.** The myths and facts behind cyber security risk for industrial control systems, *In ISA Process Control Conference*, 2003.

11. **Vandich A. P., Yaichkin M. A., Karganov V. V., Privalov A. A., Skudneva E. V.** *K voprosu ob organizacii informacionnogo obmena dlya povysheniya zashchishchennosti seti peredachi dannyh ot tekhnicheskoj komp'yuternoj razvedki* (Revisited administration of data exchange for rising immunity of communicatoons network from tecnical computer scouting), *Trudy CNIIS*, 2017, vol. 1, no. 4, pp. 72—78 (in Russian).

12. **Karganov V. V., Drachev V. O., Levchenko G. N.** *Formirovanie modeli predmetnoj oblasti dlya informacionnoj sistemy* (Model formation of application domain for data system), *Innovacionnye Tekhnologii I Tekhnicheskie Sredstva Special'nogo Naznacheniya,* Trudy desyatoj obshcherossijskoj nauchno-prakticheskoj konferencii, 2018, pp. 264—268 (in Russian).

13. **Karganov V. V., Pilyavec O. G., Shevchenko A. A.** *K voprosu preduprezhdeniya i obespecheniya trebuemogo urovnya informacionnoj bezopasnosti informacionno-vychislitel'noj seti special'nogo naznacheniya ot nesankcionirovannyh vozdejstvij* (To the issue of prevention and ensuring the required level of information security of information network of A special purpose from unauthorized influences), *Voprosy oboronnoj tekhniki. Seriya 16: Tekhnicheskie sredstva protivodejstviya terrorizmu*, 2018, no. 1—2 (115—116), pp. 78—85 (in Russian).

14. **Patent 2635256.** *Rossijskaya Federaciya, MPK G06F 12/14. Sposob zashchity informacionno-vychislitel'noj seti ot nesankcionirovannyh vozdejstvij* (Method of defense of information-calculation network from illegal actions), Karganov V. V., Kostarev S. V., Lipatnikov V. A., Lobashev A. I., SHevchenko A. A.; zayavitel' i patentoobladatel' Federal'noe gosudarstvennoe kazennoe voennoe obrazovatel'noe uchrezhdenie vysshego obrazovaniya "Voennaya akademiya svyazi imeni Marshala Sovetskogo Soyuza S. M. Budennogo" Ministerstva oborony Rossijskoj Federacii. — № 2016117662; zayavl. 04.05.2016; opubl. 09.11.2017, Byul. 31, 2 p. (in Russian).

15. **Kuznecov I. A., Lipatnikov V. A., Shevchenko A. A.** *Sposob mnogofaktornogo upravleniya bezopasnost'yu informacionno-telekommunikacionnoj seti sistemy menedzhmenta kachestva predpriyatij integrirovannyh struktur* (Multivariable control technique of information-telecommunication network security of integrated structure organization quality management system), *Voprosy radioehlektroniki*, 2016, no. 6, pp. 23—28 (in Russian).

16. **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.

17. **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.

18. **Mazurek M., Dymora P.** Network anomaly detection based on the statistical selfsimilarity factor for HTTP protocol, *Przeglad Elektrotechniczny*, 2014, pp. 127—130.

19. **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.

20. **Sheth H., Shah B., Yagnik S.** A survey on RBF Neural Network for Intrusion Detection System, *Int. Journal of Engineering Research and Applications*, 2014, vol. 4, pp. 17—22.

21. **Branickij A. A., Kotenko I. V.** *Analiz i klassifikaciya metodov obnaruzheniya setevyh atak* (Analysis and classification of methods for network attack detection), *Trudy SPIIRAN*, 2016, iss. 2(45), pp. 207—243 (in Russian).

22. **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.

23. **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.

24. **Ryan J., Lin M.-J.** Intrusion Detection with Neural Networks, Advances in Neural Information Processing Systems, 1998, pp. 943—949.

25. **FSTEHK.** *Metodika opredeleniya aktual'nyh ugroz bezopasnosti personal'nyh dannyh pri ih obrabotke v informacionnyh sistemah* (Method of determination actual security risks in personal data while their processing in informational systems), available at: https://fstec.ru/component/attachments/download/290 (date of access: 15.07.2018) (in Russian).