УДК 004.7
doi:10.15217/issn1684-8853.2017.4.67

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ОРГАНИЗАЦИИ ИНТЕГРИРОВАННОЙ СТРУКТУРЫ НА ОСНОВЕ ВЫДЕЛЕННОГО СЕРВЕРА С КОНТЕЙНЕРНОЙ ВИРТУАЛИЗАЦИЕЙ

В. А. Липатников[а], *доктор техн. наук, профессор*
А. А. Шевченко[а], *младший научный сотрудник*
А. Д. Яцкин[а], *старший оператор*
Е. Г. Семенова[б], *доктор техн. наук, профессор*
[а]*Военная академия связи им. Маршала Советского Союза С. М. Буденного, Санкт-Петербург, РФ*
[б]*Санкт-Петербургский государственный университет аэрокосмического приборостроения, Санкт-Петербург, РФ*

Постановка проблемы: *существует противоречие между требованиями международных стандартов к организации по установке порядка внутренней и внешней коммуникации по вопросам, относящимся к системе менеджмента качества и касающимся сохранения целостности системы при планировании и внесении в нее изменений в условиях кибернетического противоборства.* ***Цель:*** *разработка способа управления информационной безопасностью, при котором документированная информация системы менеджмента качества будет находиться под управлением для обеспечения ее доступности, а также защищенности от потери конфиденциальности, ненадлежащего использования или потери целостности.* ***Результаты:*** *предложен способ управления информационной безопасностью, основанный на добавлении в демилитаризованную зону информационно-вычислительной сети выделенного сервера, на котором с помощью технологии контейнерной виртуализации развертывается виртуальная копия реальной сети, включающая сетевые сервисы. Злоумышленник, производящий подготовку компьютерной атаки на сеть, работая с данным сервером, предполагает, что взаимодействует с реальной сетью. В процессе анализа действий злоумышленника в реальном времени администратор сети получает информацию о приоритетных целях, используемых средствах злоумышленника и уязвимостях различных элементов сети, что дает ему возможность оперативно принять меры по повышению защищенности сети и избежать ее компрометации.* ***Практическая значимость:*** *использование данного подхода позволяет поддерживать работоспособность системы менеджмента качества на требуемом уровне при динамике изменения множества угроз с учетом масштабирования при планировании и внесении в нее изменений в условиях кибернетического противоборства.*

Ключевые слова *— автоматизированная система менеджмента организации интегрированной структуры, информационно-вычислительная сеть, компьютерная атака, защита информации, оценка рисков, контейнерная виртуализация, проактивное управление, масштабирование, показатель защищенности.*

Введение

Согласно требованиям международного стандарта [1], организация должна установить порядок внутренней и внешней коммуникации по вопросам, относящимся к системе менеджмента качества (СМК). Перспективным направлением управления в организации является внедрение автоматизированных систем менеджмента качества организации интегрированной структуры (АСМК ОИС) [2]. Имеет место противоречие между требованиями международного стандарта к организации по установлению порядка внутренней и внешней коммуникации по вопросам, относящимся к СМК. С одной стороны, должно быть определено, с кем и каким образом будет осуществляться коммуникация. С другой стороны, требуется сохранение целостности СМК при планировании и внесении в нее изменений в условиях кибернетического противоборства. Необходимо разработать способ, при котором документированная информация АСМК ОИС будет находиться под управлением в целях ее доступности и пригодности для применения, а также адекватно защищена (от потери конфиденциальности, ненадлежащего использования или потери целостности).

Требуется сохранение целостности СМК при планировании и внесении в нее изменений. Традиционные средства защиты информации (СЗИ), такие как антивирусное программное обеспечение, межсетевые экраны и системы обнаружения вторжений, как известно, не гарантируют абсолютной защищенности информационно-вычислительных сетей (ИВС), входящих в состав АСМК ОИС. Антивирусное программное обеспечение, являясь средством реактивной защиты, реагирует только на известные системе виды воздействий. Межсетевые экраны и системы обнаружения вторжений не лишены уязвимостей, которые могут быть использованы злоумышленником для проникновения в защищенную ИВС как составную часть АСМК.

Основным показателем защищенности АСМК ОИС в условиях кибернетического противобор-

ства является время бесперебойной работы ИВС $T_з$ на заданном интервале наблюдения. На этапе проектирования задается требуемое время нахождения ИВС в исправном состоянии $T_{тр}$. Для оценки информационной безопасности (ИБ) используется вероятность нахождения ИВС в состоянии защищенности от компьютерной атаки (КА)

$$P_з(T) = P(T_з \geq T_{тр}).$$

В процессе масштабирования АСМК эффективность мер, принятых для обеспечения ИБ, может снижаться, так как возникают новые угрозы, поэтому текущее значение показателя $P_з(T)$ уменьшается. Для поддержания оптимального уровня защищенности необходимо осуществлять управление с учетом текущей обстановки с прогнозированием.

В одном способе [2] прогнозирование состояния ИБ и выявление уязвимостей ИВС АСМК выполняется на основе заданной на начальном этапе таблицы уязвимостей. Такой подход удобен с точки зрения анализа последствий реализации известных уязвимостей и прогнозирования дальнейшего функционирования ИВС. В другом способе контроля уязвимостей [3] также используется предварительно сформированная таблица тестирования и база данных уязвимостей. Общим недостатком вышеперечисленных способов является то, что в них используется фиксированное множество известных уязвимостей. Способы позволяют точно оценить защищенность $P_з(T)$ и принять определенные меры в рамках этого множества, но, в действительности, нельзя пренебрегать тем фактом, что множество угроз постоянно меняется. Злоумышленники находят новые способы обхода СЗИ, обнаруживают новые уязвимости в программах и протоколах.

Одним из подходов, предоставляющих органу управления возможность прогнозировать предстоящие КА, является использование средств обеспечения ИБ, выполняющих имитацию работы реальных элементов ИВС, так называемых honeypot-систем. Средства, такие как Security Studio Honeypot Manager [4], позволяют имитировать работу строго определенных элементов ИВС, например СУБД Oracle, что является существенным ограничением гибкости подобных систем. При этом обеспечивается не полноценное функционирование ложного элемента ИВС, а лишь имитация его работы, как, например, в системе HoneyBot [5], которая имитирует работу хоста под управлением ОС Windows и способна отвечать на запросы по протоколам echo, ftp, telnet, smtp, http, pop3, ident, dcom, socks. Эти системы называются низкоинтерактивными с точки зрения полноты покрытия функционала реальной системы. Такие системы потребляют меньше ресурсов и представляют меньшую угрозу для безопасности ИВС, но при этом легко обнаруживаются злоумышленником, и поэтому информация, полученная с помощью данных систем, не будет содержать действительно важных для администратора безопасности ИВС сведений. Высокоинтерактивные honeypot-системы, обеспечивающие полноценную работу ложных элементов ИВС, такие как HiHat [6], обычно ограничены функционалом только одного приложения. Решения на базе виртуальных машин, имитирующие работу реального хоста, имеют место, но при этом являются слишком дорогими в плане обеспечения их вычислительными ресурсами, что делает их нерентабельными.

Задачей данного исследования является разработка способа управления ИБ ИВС с распознаванием КА и прогнозированием предполагаемого сценария дальнейшего развития КА, учитывающего возможные последствия при принятии решений по предупреждающим действиям.

Предлагаемый способ управления ИБ ИВС на основе выделенного сервера с контейнерной виртуализацией

В качестве решения предлагается внедрение в сеть выделенного сервера, на котором с использованием технологии контейнерной виртуализации развертывается виртуальная копия ИВС, полностью или частично повторяющая все ее элементы. Предполагается, что, получив доступ к этому серверу, злоумышленник будет в течение определенного времени считать, что работает с реальной ИВС и производит действия по подготовке и реализации распределенных атак. Результаты регистрируются и передаются органу управления ИБ для принятия мер по защите реальной ИВС от готовящейся атаки.

Исходными данными для решения являются вероятность нахождения АСМК в состоянии защищенности от КА $P_з(T)$ и критерий ИБ (требуемый уровень защищенности) $P_{з.т}$. Требуется обеспечить $P_{з.т}$ при следующих исходных данных:

$\{H\} = \{h_1, ..., h_i\}$ — элементы ИВС;

$\{D\} = \{d_1, ..., d_i\}$ — средства защиты, используемые в ИВС;

$\{S\} = \{s_1, ..., s_i\}$ — сетевые службы, функционирующие в ИВС.

Исключается возможность злоумышленника обнаруживать признаки того, что его активность подвергается анализу. Процесс получения сведений о действиях злоумышленника не снижает безопасность и производительность АСМК как интеллектуальной многоагентной системы. Обеспечивается отвлечение ресурсов злоумышленника от воздействия на основную часть ИВС.

В работе рассматривается типовая структура ИВС, состоящая из следующих элементов (рис. 1):

1. Транспортной сети. Она включает в себя сетевые устройства, такие как маршрутизаторы и коммутаторы, главной задачей которых является обеспечение обмена данными между различными сегментами ИВС.

2. Демилитаризованной зоны, участка ИВС, находящегося на ее границе и соединяющегося с сетью Интернет через пограничный маршрутизатор. Внутри этого участка ИВС располагаются службы, которые должны быть доступны пользователям внешней сети, такие как веб-сервер, прокси-сервер и др.

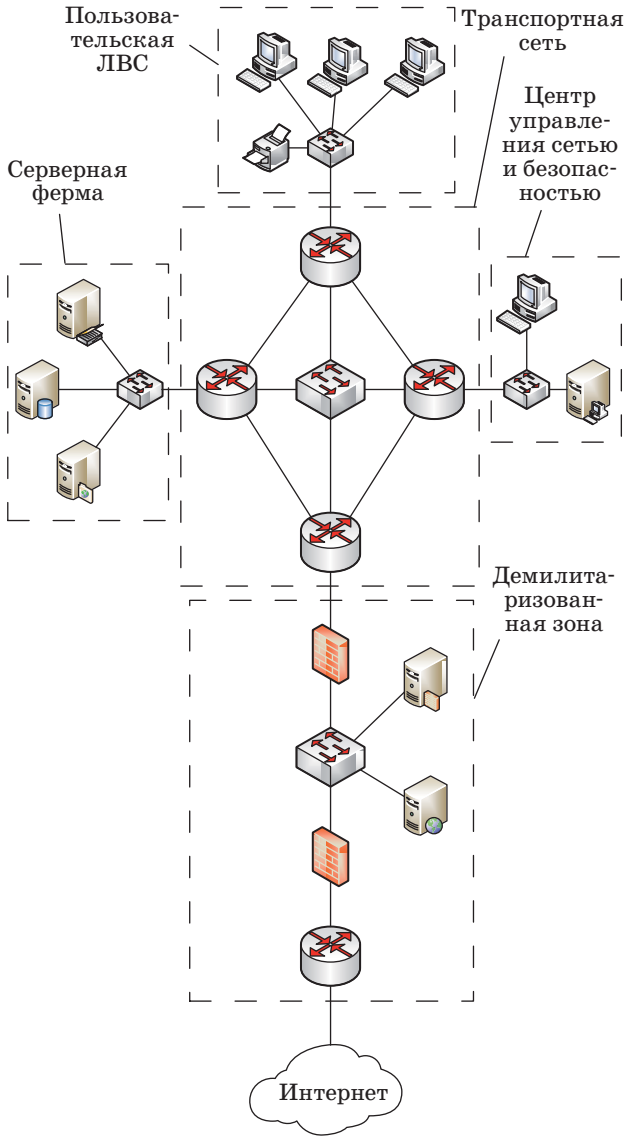
3. Серверной фермы, где располагаются серверы, обеспечивающие работу различных служб, используемых внутри ИВС: файловый сервер, сервер баз данных, сервер службы каталогов и др.

4. Центра управления безопасностью, задачей которого является контроль уязвимостей узлов сети и управление работой используемых СЗИ. Должны быть определены знания, необходимые для функционирования процессов ИВС и для достижения требуемой ИБ. Эти знания должны поддерживаться на соответствующем уровне и быть доступными в необходимом объеме (п. 7.1.6 ISO 9001-2015).

5. Пользовательской локальной вычислительной сети *ЛВС*, состоящей из рабочих мест пользователей, сетевых принтеров и других устройств. Таких сетей обычно бывает несколько; они могут быть разделены по подразделениям или по другому принципу, предложенному администратором сети.

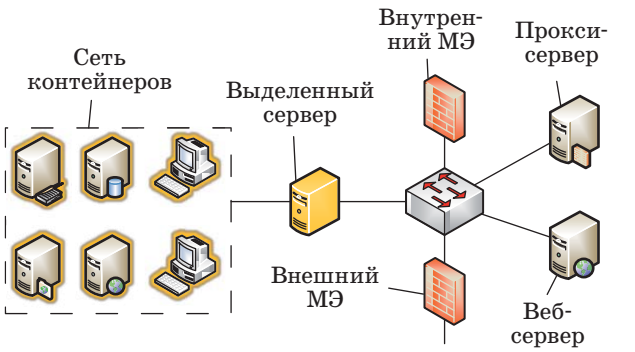
Возможны два способа расположения выделенного сервера в ИВС: в демилитаризованной зоне и внутри ИВС. В первом случае предполагается воздействие на ИВС со стороны внешнего злоумышленника, т. е. через сеть Интернет, а во втором — со стороны внутреннего, т. е. легитимного пользователя.

Рассмотрим первый вариант, когда выделенный сервер располагается в демилитаризованной зоне между двумя межсетевыми экранами *МЭ* (рис. 2) и для внешнего злоумышленника может выглядеть как произвольный сетевой ресурс ИВС. Сеть, развернутая на базе выделенного сервера, представляет собой сеть Linux-контейнеров на базе программного продукта Docker, созданную таким образом, чтобы повторять топологию и функциональную принадлежность элементов реальной ИВС. Получив доступ к данному веб-серверу, злоумышленник в первую очередь попытается произвести мониторинг топологии ИВС, но вместо взаимодействия с реальной ИВС он уже будет обмениваться данными с контейнерами. При этом все его действия будут регистрироваться и анализироваться.



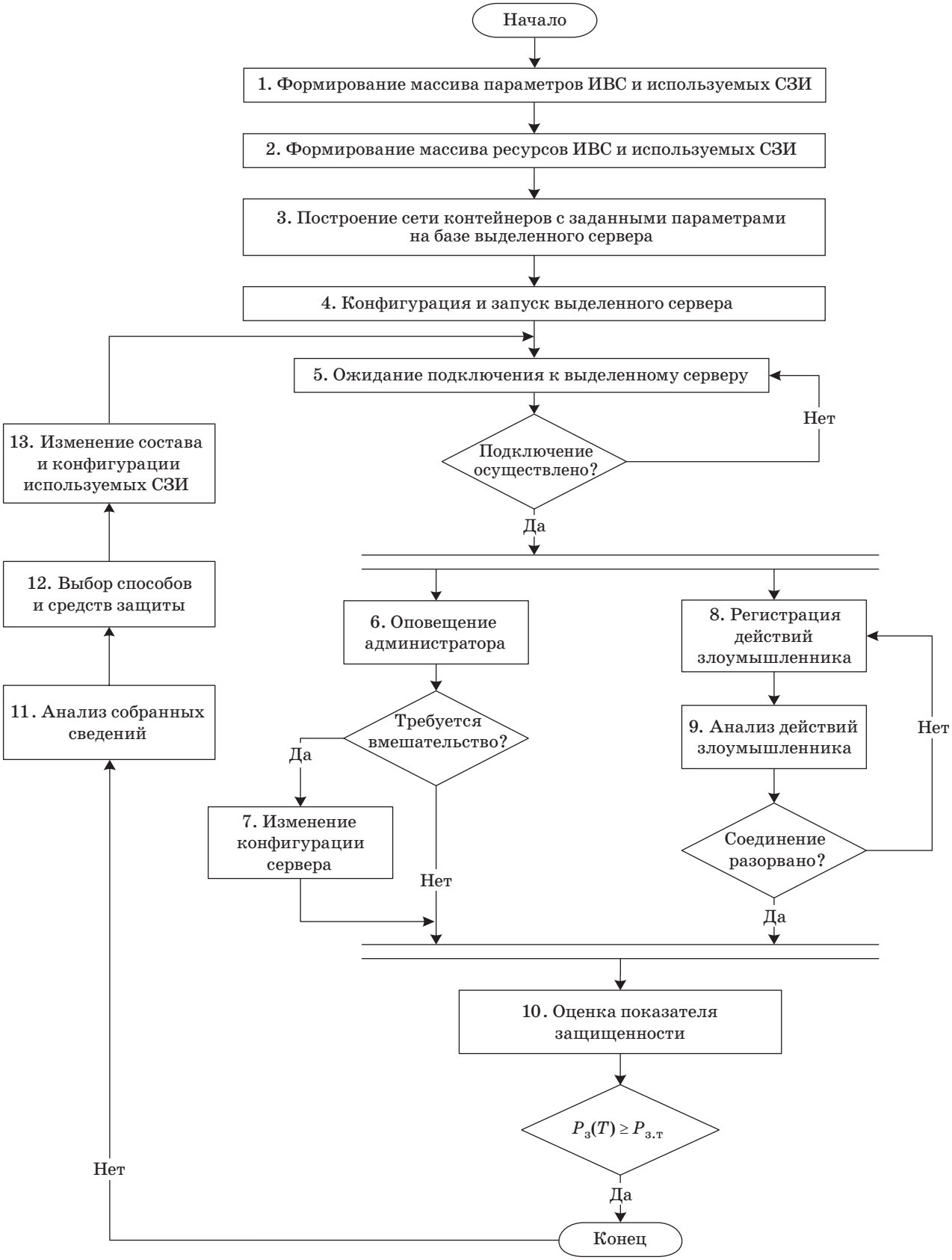
■ ***Рис. 1.*** Структурная схема предлагаемой информационно-вычислительной сети

■ ***Fig. 1.*** Computer network diagram used in the study



■ ***Рис. 2.*** Расположение выделенного сервера с контейнерной виртуализацией

■ ***Fig. 2.*** Dedicated server placement



■ ***Рис. 3.*** Алгоритм проактивного управления ИБ ИВС АСМК на основе выделенного сервера с контейнерной виртуализацией

■ ***Fig. 3.*** Proactive management algorithm based on a dedicated server with a container virtualization

Использование технологии контейнерной виртуализации в рассматриваемой интеллектуальной многоагентной системе позволяет более гибко настраивать элементы сети: вместо создания полноценных виртуальных машин администратор может, пользуясь модульной структурой Docker-контейнеров, оперативно разворачивать элементы сети, конфигурировать их сетевые интерфейсы, разворачивать необходимые сетевые службы, при этом службы, также помещенные в контейнеры, не требуют повторной настройки на каждом из элементов сети, что значительно упрощает процесс конфигурации системы. Используя информацию, полученную в процессе анализа действий злоумышленника, можно установить приоритетные цели, возможности атакующего и средства, используемые для осуществления КА, методы взлома и уязвимости СЗИ; сформировать статистику атак и произвести определение способов противодействия им.

Согласно вышеизложенному предлагается алгоритм проактивного управления ИБ ИВС, состоящий из следующих шагов (рис. 3).

1. На основании данных о структуре ИВС: адресах элементов ИВС и СЗИ, расположении их в сети, наличии связей с другими элементами и их назначении, — формируются массивы $\{H\} = \{h_1, ..., h_i\}$ — элементы ИВС и $\{D\} = \{d_1, ..., d_i\}$ — используемые СЗИ. Элементами массивов являются: $h_i =$ (Идентификатор элемента, Сетевой адрес, Расположение в ИВС, Назначение), $d_i =$ =(Идентификатор СЗИ, Сетевой адрес, Расположение в ИВС, Назначение).

2. Сведения о составе сетевых служб, работающих на элементах ИВС, их назначении, а также о каналах управления используемыми СЗИ позволяют сформировать массив $\{S\} = \{s_1, ..., s_i\}$. Элементы массива имеют вид $s_i =$ (Идентификатор службы, Элемент ИВС, Используемый порт, Назначение).

3. С помошью сформированных массивов с данными о составе ИВС, используемых служб и СЗИ создаются контейнеры, которые будут работать на выделенном сервере: производится настройка сетевых интерфейсов, контейнеров сетевых служб и др.

4. Производится конфигурация и запуск выделенного сервера.

5. Выделенный сервер ожидает подключения со стороны злоумышленника. Легитимные пользователи работают только с реальными хостами, а весь сетевой трафик изолирован от реальных элементов ИВС. Сам факт подключения к выделенному серверу считается нарушением ИБ.

6. При подключении к серверу администратор безопасности оповещается об этом событии.

7. Администратор безопасности может изменить конфигурацию ИВС, например, ослабить или, наоборот, усилить механизмы защиты хостов, работающих на его базе, для того чтобы манипулировать злоумышленником.

8. Параллельно с оповещением администратора о подключении начинается подробная регистрация действий злоумышленника внутри сети.

9. Данные, полученные в ходе регистрации действий злоумышленника с виртуальной сетью, анализируются и передаются администратору, который на их основе принимает решения в п. 8. При анализе данных определяется тип воздействия на ИВС, идентифицируются известные КА, а также их различные параметры. Прогнозируются воздействие и элементы, на которые будет направлена КА, и принимается решение по предупреждающим действиям.

Для прогнозирования состояния ИВС можно применить один из методов методологии прогнозирующих моделей (Model Predictive Control — MPC), например, метод State-Space Model Predictive Control (управление с прогнозированием на основе модели пространства состояний) [7, 8].

Модель процесса функционирования объекта управления используется для предсказания выходных данных объекта управления на основе прошлых и текущих значений параметров обнаружения атак [9] и предполагаемых оптимальных управляющих воздействий в будущем.

10. С учетом данных об уязвимостях ИВС, приоритетных целях злоумышленника и эффективности используемых СЗИ, полученных в процессе взаимодействия злоумышленника с выделенным сервером, производятся оценка вероятности нахождения ИВС в состоянии защищенности от КА и сравнение результатов оценки с заданным критерием $P_{з.т}$.

11. Администратором ИБ ИВС проводится анализ полученных сведений, целью которого является выработка мер, необходимых для повышения уровня защищенности.

12. Определяются необходимые изменения конфигурации используемых СЗИ, целесообразность включения в ИВС новых СЗИ, различные настройки сетевых служб.

13. Производится конфигурация используемых и внедрение новых СЗИ в ИВС.

Практическая значимость

Процесс управления ИБ ИВС АСМК является циклическим, и предполагается, что до момента времени $t = 0$ ИВС находится на этапе подготовки. Он включает в себя начальную оценку рисков, выбор и внедрение требуемых СЗИ. В момент $t > 0$ сеть переходит на этап эксплуатации, что приводит к постоянному снижению показателя защищенности $P_з(T)$. В процессе дальнейшего функционирования ИВС при обнаружении

новых угроз ИБ необходимо также производить оценку рисков, внедрение новых и изменение конфигурации используемых СЗИ. Эти действия и определяют границу одного цикла управления. Время начала очередного цикла управления $t_{у\,i}$ также можно принять за $t = 0$. Основная задача процесса управления состоит в том, чтобы значение показателя $P_з(T) \geq P_{з.т}$ для всех интервалов $[t_{у\,i}, t_{у\,i+1}]$.

Процесс воздействия злоумышленниками на ИВС в наблюдаемом промежутке времени можно рассматривать, как поток случайных событий (КА), имеющий плотность распределения $w_а(t)$, а меры защиты, принимаемые администратором безопасности ИВС, как поток случайных событий с плотностью распределения $w_з(t)$ [10]. Можно определить величину $P_з(T)$ как

$$P_з(T) = \int_0^T w_з(\tau)[1 - \int_0^\tau w_а(t)\mathrm{d}t]\mathrm{d}\tau. \qquad (1)$$

Поскольку случайные события, связанные с подготовкой и осуществлением КА, являются последовательными, то можно предположить, что обе рассмотренные случайные величины имеют экспоненциальное распределение со значением параметра интенсивности $\lambda = 1/T_з$ и $\lambda = 1/T_а$ для действий администратора системы и действий злоумышленника соответственно, т. е.

$$w_з(t) = \frac{1}{T_з}\exp\left(-\frac{t}{T_з}\right);$$

$$w_а(t) = \frac{1}{T_а}\exp\left(-\frac{t}{T_а}\right),$$

где $T_з$ — среднее время, требуемое для реализации мер защиты; $T_а$ — среднее время, необходимое для осуществления КА.

Экспоненциальное распределение характеризуется одним параметром, определяющим среднее значение времени обеспечения $T_з$ или преодоления защиты $T_а$. При задании в выражении (1) плотностей распределения вероятностей $w_з(t)$ и $w_а(t)$, соответствующих экспоненциальному распределению, могут быть получены аналитические выражения для вероятности обеспечения защиты $P_з(T)$ в зависимости от параметров $T_з$ и $T_а$.

Экспоненциальное распределение соответствует простейшему потоку событий и описанию переходов между состояниями защищенности информационной системы марковскими случайными процессами. Вычисление вероятности соответствия уровня защищенности требуемому за заданное время T в соответствии с выражением (1) для экспоненциальных функций плотности распределения вероятностей $w_з(t)$ и $w_а(t)$ с параметрами $T_з$ и $T_а$ дает

$$P_з(T) = \frac{1}{1 + T_з / T_а}\left(1 - \exp\left(-\frac{T(1 + T_з / T_а)}{T_з}\right)\right). \qquad (2)$$

Перед реализацией КА злоумышленнику необходимо получить информацию об уязвимостях ИВС, которые могут быть использованы при реализации атаки. Процесс сбора злоумышленником информации об ИВС в общем случае представляет следующую последовательность действий:

1) пассивный анализ, целью которого является сбор данных, без непосредственного активного взаимодействия с ИВС;

2) вскрытие топологии сети (активное сетевое сканирование);

3) определение используемых операционных систем, состава работающих сетевых служб и их версий;

4) выявление наличия уязвимостей используемых операционных систем и сетевых служб.

Обозначим время, которое потребуется злоумышленнику на проведение пассивной подготовки (п. 1) как $T_{п.п}$, активных процессов в целях подготовки КА (процессы по п. 2–4) как $T_{а.п}$, а время, необходимое для реализации КА с использованием полученных сведений об ИВС, как $T_р$.

Соответственно, весь цикл осуществления КА будет складываться из времени, потраченного злоумышленником на подготовку, и временем, требуемым для непосредственной реализации КА:

$$T_а = T_{п.п} + T_{а.п} + T_р.$$

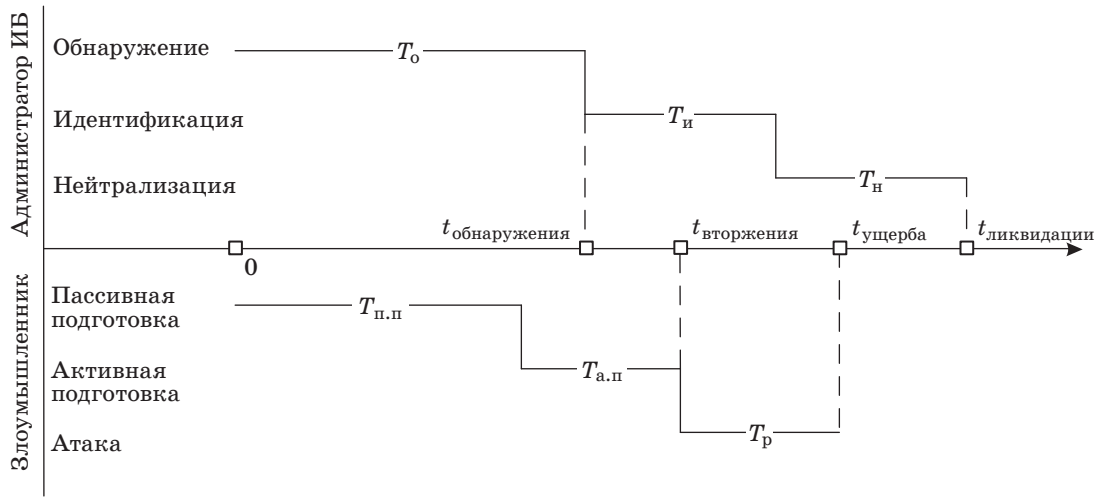
Администратор ИБ ИВС может обнаружить КА только начиная с момента активной подготовки ее злоумышленником. Время от начала атаки до ее обнаружения — $T_о$. При обнаружении факта наличия КА требуется время на идентификацию $T_и$ этой КА и выполнение нейтрализации (минимизации) воздействия $T_н$. Среднее время, требуемое для реализации мер защиты, определяется как

$$T_з = T_о + T_и + T_н.$$

Временная диаграмма вторжения в ИВС представлена на рис. 4. Администратор ИБ получает информацию о наличии КА уже в процессе ее осуществления, т. е. момент времени $t_{обнаружения}$ наступает, когда КА находится уже на этапе активной подготовки.

Система находится в незащищенном состоянии начиная в промежуток времени [$t_{вторжения}$, $t_{ликвидации}$].

Компьютерную атаку можно считать успешно проведенной злоумышленником, так как за



■ ***Рис. 4.*** Временная диаграмма успешной КА на ИВС
■ ***Fig. 4.*** Timing diagram of a successful computer attack

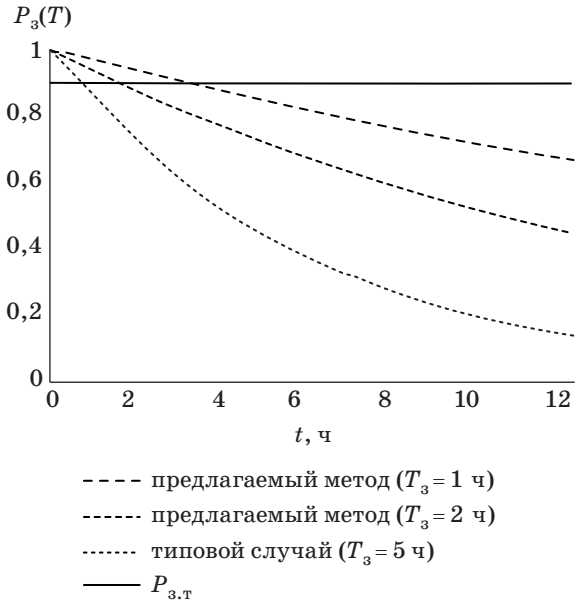
время, необходимое администратору на обнаружение, идентификацию и нейтрализацию КА, могут быть полностью или частично достигнуты цели КА.

Применение предложенного способа позволяет администратору опередить злоумышленника, вторгнувшегося в сеть. Пока злоумышленник взаимодействует с сетью контейнеров, администратору представляется возможность подготовить реальную сеть к противодействию аналогичной атаке со стороны злоумышленника. То есть при условии, что злоумышленник сначала попытается осуществить атаку на сеть контейнеров, администратор ИБ АСМК предполагает, что подобная атака может быть осуществлена и на реальную ИВС, поэтому значительно сокращается время обнаружения КА: $T_о \to 0$. На момент проведения атаки на реальную ИВС у администратора уже будет достаточная информация о предполагаемой КА, а также возможность заранее предпринять меры по защите.

Предложенный способ, помимо сокращения времени $T_о$, позволяет уменьшить величину $T_и$, так как администратор ИБ ИВС, располагая сведениями о предполагаемой атаке, сможет быстрей ее идентифицировать. Таким образом, сокращая интервалы времени $T_о$ и $T_и$, тем самым уменьшая величину $T_з$, мы, в соответствии с формулой (2), можем повысить уровень защищенности ИВС $P_з(T)$.

Рассмотрим $P_з(T)$, где момент $t = 0$ — момент начала управления ИБ. Положим, что плотность вероятности величины, характеризующей действия защиты: $w_з(t) = \delta(t - T_з)$, тогда формула (1) примет вид

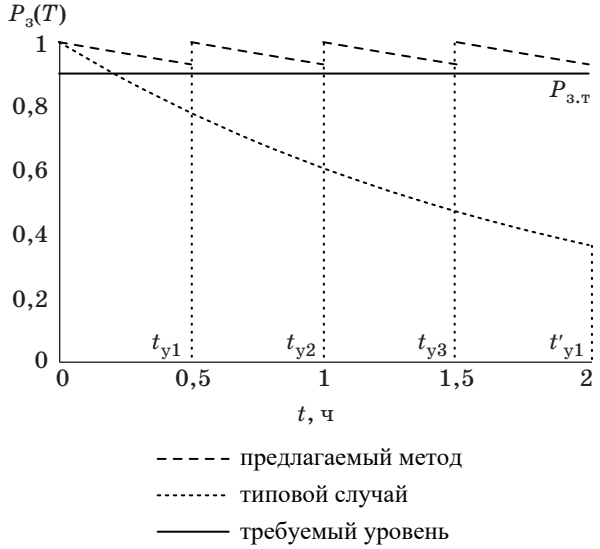
$$P_з(T) = \exp(-tT_з/T_а).$$



■ ***Рис. 5.*** Вероятность защищенности ИВС АСМК в отсутствие мероприятий по управлению ИБ
■ ***Fig. 5.*** Probability chart of a security value without an information security management process

Зафиксируем значение величины $T_а = 10$ ч, а требуемый уровень защищенности ИВС $P_{з.т} = 0{,}9$. График зависимости для типовых условий в случае различных значений $T_з$ представлен на рис. 5.

Определено снижение уровня защищенности в зависимости от времени, а также точка пересечения графиков, в которой $P_з(T) = P_{з.т}$. Этот момент времени является критическим для принятия мер по обеспечению ИБ, т. е. определяются границы интервала $[t_{у0}, t_{у1}]$. При наличии в ИВС



■ ***Рис. 6***. Вероятность защищенности АСМК с учетом циклического управления ИБ

■ ***Fig. 6***. Probability chart of a security value with an information security management process

процесса управления ИБ постоянное падение показателя защищенности $P_з(T)$ компенсируется путем проведения мероприятий по предупреждению и противодействию КА в момент времени t_{yi}.

В типовом случае обнаружение КА может занимать несколько часов с момента начала злоумышленником действий по подготовке к ее осуществлению. Предположим значение $T_о = 3$ ч. Время, которое потребуется на идентификацию КА от момента ее обнаружения, положим равным $T_и = 1$ ч, а время на нейтрализацию КА $T_н = 1$ ч. Как было рассмотрено ранее, предложенный способ позволяет значительно сократить время обнаружения КА, так как после осуществления КА на виртуальную копию ИВС администратор уже будет располагать всеми необходимыми сведениями для проактивного противодействия атаке на реальную ИВС, поэтому можно положить $T_о = 0$ ч, а время на идентификацию КА $T_и = 0{,}5$ ч. Для типового случая $T_з = T_о + T_и + T_н = 3 + 1 + 1 = 5$ ч, а при использовании предложенного метода значение $T_з = 0 + 0{,}5 + 1 = 1{,}5$ ч. Требуемый уровень защищенности оставим прежним $P_{з.т} = 0{,}9$. При этом, с учетом того факта, что время реализации мер защиты $T_з$ уже учтено в модели снижения защищенности в рамках одного цикла управления, примем допущение, что действия по повышению защищенности в конце каждого цикла осуществляются мгновенно, т. е. время между двумя циклами управления не учитывается. График зависимости значения показателя защищенности $P_з(T)$ от времени по формуле (1) с учетом циклического подхода к управлению ИБ представлен на рис. 6.

По сравнению с типовым случаем показатель защищенности $P_з(T)$ снижается медленнее при использовании предложенного метода. Это, а также более низкое время обнаружения и идентификации атаки позволяют принять меры заблаговременно, что дает выигрыш во времени для осуществления проактивного противодействия КА. Использование способа позволяет поддерживать защищенность АСМК выше требуемого значения $P_{з.т}$ в пределах каждой итерации цикла управления ИБ $[t_{yi},\ t_{yi+1}]$, тогда как в типовом случае (при использовании реактивного подхода к управлению ИБ) на момент, когда администратор будет обладать достаточной информацией о КА, чтобы идентифицировать ее и принять меры по повышению защищенности, т. е. в момент времени t'_{y1}, показатель защищенности упадет ниже требуемого значения $P_{з.т}$.

Заключение

Результатом использования предложенного способа управления ИБ в АСМК в условиях кибернетического противоборства является возможность поддерживать защищенность на требуемом уровне, используя получаемую информацию для проактивной борьбы с попытками злоумышленника осуществить КА.

Новизна предлагаемого способа в сравнении с существующими решениями заключается в следующем.

1. В предлагаемом способе управления ИБ добавлены процессы получения информации о приоритетных целях злоумышленника, используемых им средствах и уязвимостях различных элементов сети. Для технической реализации способа в демилитаризованную зону ИВС включается выделенный сервер, на котором с помощью технологии контейнерной виртуализации развертывается виртуальная копия реальной сети, включающая сетевые сервисы в условиях ограниченных ресурсов.

2. Анализ взаимодействия злоумышленника с ИВС в реальном времени позволяет администратору своевременно реагировать на попытки осуществления распределенных атак. Использование эффективных методов анализа и прогнозирования повышает достоверность информации, уменьшает время реагирования на осуществление атаки на АСМК.

Можно выделить следующие преимущества предлагаемого метода:

— возможность своевременно обнаружить попытку несанкционированного воздействия, производить статистику атак и определение способов противодействия им;

— централизованное управление системой позволяет оперативно менять ее структуру, адапти-

ровать под изменения реальной информационно-вычислительной сети, а также производить анализ данных, полученных в результате работы системы;

— проактивная модель работы позволяет обеспечить защиту от новых стратегий воздействия на информационно-вычислительную сеть АСМК;

— изолированность системы от реальной АСМК ОИС предполагает возможность компрометации выделенного сервера с контейнерной виртуализацией без вреда для реальной.

Литература

1. ГОСТ Р ИСО 9001–2015. Системы менеджмента качества. Требования. — М.: Изд-во стандартов, 2005. — 32 с.
2. **Костарев С. В., Липатников В. А.** Анализ состояния и динамики качества объектов автоматизированной системы менеджмента предприятия интегрированной структуры // Информационные системы и технологии. 2015. № 3 (89). С. 52–64.
3. **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.
4. Honeypot Manager. https://www.securitycode.ru/products/honeypot (дата обращения: 04.12.2016).
5. HoneyBOT — the Windows Honeypot. http://www.atomicsoftwaresolutions.com (дата обращения: 04.12.2016).
6. HIHAT — High Interaction Honeypot Analysis Tool. http://hihat.sourceforge.net (дата обращения: 04.12.2016).
7. **Camacho E. F., Bordons C.** Model Predictive Control. — London: Springer-Verlag, 2004. — 405 p.
8. **Кузнецов И. А., Липатников В. А., Сахаров Д. В.** Управление АСМК организации интегрированной структуры с прогнозированием состояния информационной безопасности // Электросвязь. 2016. № 3. С. 28–36.
9. **Лукацкий А.** Обнаружение атак. — СПб.: БХВ-Петербург, 2008. — 304 с.
10. **Мальцев Г. Н., Панкратов А. Н., Лесняк Д. А.** Исследование вероятностных характеристик изменения защищенности информационной системы от несанкционированного доступа нарушителей // Информационно-управляющие системы. 2015. № 1. С. 50–57. doi:10.15217/issn1684-8853.2015.1.50

UDC 004.7
doi:10.15217/issn1684-8853.2017.4.67

Information Security Management of Integrated Structure Organization based on a Dedicated Server with Container Virtualization

Lipatnikov V. A.[a], Dr. Sc., Tech., Professor, lipatnikovanl@mail.ru
Shevchenko A. A.[a], Junior Researcher, alexandr_shevchenko91@mail.ru
Yatskin A. D.[a], Science Company Senior Operator, yatskinandrey@gmail.com
Semenova E. G.[b], Dr. Sc., Tech., Professor, egsemenova@mail.ru
[a]Military Academy of Telecommunication of S. M. Budionov, 3, Tikhoretskii Pr., K-64,194064, Saint-Petersburg, Russian Federation
[b]Saint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaia St., 190000, Saint-Petersburg, Russian Federation

Introduction: There is a contradiction between the requirements of the international standards on internal and external communication concerning the issues related to the quality management system and the system integrity when planning or reconfiguring under the conditions of cyberattacking. **Purpose:** We have to develop a way of information security management in which the documented information of the quality management system is controlled to ensure its accessibility, as well as its protection from a loss of confidentiality, misuse or loss of integrity. **Results:** A method of information security management is proposed, based on adding a dedicated server into the demilitarized zone of a computer network. The method uses the virtual container technology, deploying a virtual copy of the real network including the network services. Attackers, while interacting with the server, presume that they interact with the real network. The network administrator analyzes the attackers' actions in real time and obtains the information about their priority targets, the tools they use and the vulnerabilities of the network elements. This allows the administrator to quickly take measures in order to increase the network security and avoid its compromise. **Practical relevance:** This approach allows you to maintain the operability of a quality management system at the required level considering the dynamics of the increasing number of threats and the process of scaling and making changes to the network under the conditions of cyberattacking.

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

References

1. State Standard ISO 9001–2015. Quality Management Systems. Requirements. Moscow, Standartov Publ., 2005. 32 p. (In Russian).
2. Kostarev S. V., Lipatnikov V. A. Analysis of Status and Trends in the Quality of the Automated Management System of Enterprise Integrated Structure. *Informatsionnye sistemy i tekhnologii* [Information Systems and Technologies], 2015, no. 3 (89), pp. 52–64 (In Russian).
3. Lipatnikov V. A., Shevchenko A. A. The Vulnerability Control Method Applying while Automated Integrated Structure Organization Management System Scaling. *Informatsionnye sistemy i tekhnologii* [Information Systems and Technologies], 2016, no. 2(94), pp. 128–140 (In Russian).
4. *Honeypot Manager — Kod Bezopasnosti* [Honeypot Manager — Security Code]. Available at: https://www.securitycode.ru/products/honeypot (accessed 4 July 2017).
5. *HoneyBOT — the Windows Honeypot*. Available at: http://www.atomicsoftwaresolutions.com (accessed 4 July 2017).
6. *HIHAT — High Interaction Honeypot Analysis Tool*. Available at: http://hihat.sourceforge.net (accessed 4 July 2017).
7. Camacho E. F., Bordons C. Model Predictive Control. London, Springer-Verlag, 2004. 405 p.
8. Kuznetzov I. A., Lipatnikov V. A., Sakharov D. V. The Operation Quality Management Automated System of Organization Integrated Structure with the Prediction Function of Condition of Information Security. *Elektrosviaz'*, 2016, no. 3, pp. 28–36 (In Russian).
9. Lukatskiy A. *Obnaruzhenie atak* [Attack Detection]. Saint-Petersburg, BHV-Peterburg Publ., 2008. 304 p. (In Russian).
10. Maltsev G. N., Pankratov A. V., Lesniak D. A. Probabilistic Characteristics of Information System Security Changes under Unauthorized Access. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2015, no. 1, pp. 50–57 (In Russian). doi:10.15217/issn1684-8853.2015.1.50

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.

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 4, 5, 2002-2003 (*.vsd); Coreldraw (*.cdr); Excel (*.xls); Word (*.doc); AdobeIllustrator (*.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