ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И СИСТЕМЫ

УДК 004.056.5
DOI: 10.17586/0021-3454-2016-59-5-335-341

АГРЕГИРОВАННАЯ ОПЕРАЦИОННО-ВРЕМЕННАЯ МОДЕЛЬ ОЦЕНИВАНИЯ ЭФФЕКТИВНОСТИ ОТРАЖЕНИЯ ИНФОРМАЦИОННЫХ УГРОЗ В БОЛЬШИХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

И. М. Левкин, А. А. Володина

Университет ИТМО, 197101, Санкт-Петербург, Россия
E-mail: nasti.vol@gmail.com

Рассматривается проблема повышения эффективности систем защиты информации посредством решения задачи по оценке эффективности процесса отражения информационных угроз в больших информационных системах. Процесс отражения информационной угрозы элементу информационной системы предприятия представлен в виде агрегированной операционно-временной модели. Использован математический аппарат, базирующийся на законе распределения случайной величины. Представлена оценка влияния временных затрат на эффективность защиты информации отдельных информационных структур. Произведена оценка эффективности процесса отражения ранее неизвестных информационных угроз системой защиты информации, построенной по адаптационному принципу. Благодаря адаптационной схеме осуществляется перестройка структуры системы защиты информации в зависимости от характера воздействия.

Ключевые слова: *отражение информационных угроз, большие информационные системы, эффективность, операционно-временная модель, адаптация*

В условиях, когда информация становится важнейшим стратегическим ресурсом деятельности страны, региона (отрасли) и любого хозяйствующего субъекта, одной из основных задач является ликвидация информационных угроз различного рода. Особую значимость решение этой задачи приобретает в случае возникновения новых, ранее неизвестных угроз, что объясняется увеличением времени на организацию противодействия новой угрозе. Дополнительные временные затраты обусловлены следующими факторами [1, 2]:

— необходимостью распознавания новой информационной угрозы, степени ее опасности и возможных направлений воздействия на информационную систему объекта;

— необходимостью оценки возможностей существующих сил и средств защиты информации для ликвидации угрозы;

— необходимостью поиска и привлечения дополнительных сил и средств защиты информации (если имеющиеся не способны осуществить защиту).

Большие информационные системы (например, государственные информационные системы — ГИС) состоят из множества информационных структур, разнесенных, как правило, в пространстве на значительные расстояния [3—7]. Одновременное воздействие на все элементы ГИС представляется затруднительным. Поэтому информация о характере воздействия на какую-либо структуру ГИС при построении системы ее защиты по адаптивному принципу

может быть незамедлительно передана на все остальные структуры. Это позволяет существенно сократить время реакции системы защиты информации (СЗИ) отдельных структур ГИС на новые информационные угрозы, тем самым повышая эффективность защиты информации в целом [6—9].

Влияние дополнительных временных затрат на эффективность защиты информации отдельных информационных структур может быть оценено на основе положений методологии внешнего проектирования целенаправленных процессов и целеустремленных систем [10, 11]. Для этого представим процесс отражения информационной угрозы элементу информационной системы предприятия (организации, фирмы) в виде агрегированной операционно-временной модели (рис. 1).

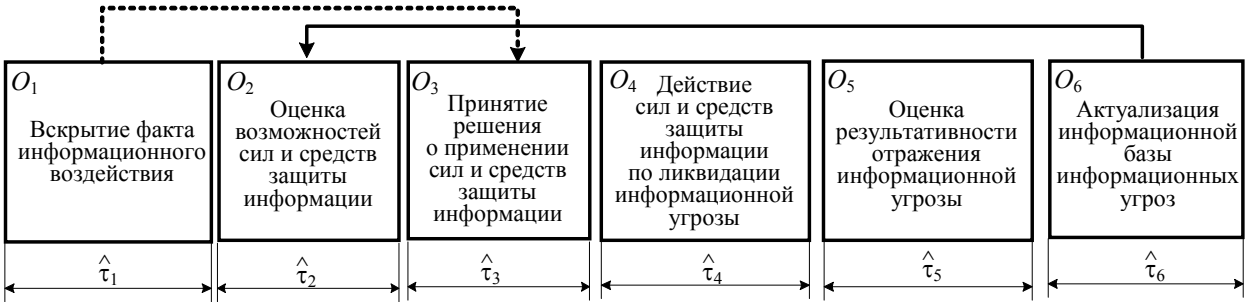

Рис. 1

В соответствии с этой моделью система мониторинга информационных угроз на начальном этапе функционирования должна обнаружить признаки информационного воздействия на систему. На идентификацию информационного воздействия (операция O_1) может быть затрачено время $\hat{\tau}_1$. Продолжительность операции O_1 зависит от многих случайных факторов: количества и особенностей вскрытых информационных признаков, квалификации специалистов системы защиты информации, условий обработки информации и т.д. Поэтому время $\hat{\tau}_1$ является случайной величиной. Если информационная угроза известна, то осуществляется непосредственное принятие решения о применении сил и средств защиты информации (операция O_3). Продолжительность выполнения этой операции $\hat{\tau}_3$.

Если информационная угроза неизвестна, то необходимо оценить возможность ее отражения (операция O_2). Продолжительность выполнения $\hat{\tau}_2$ этой операции зависит от степени новизны предполагаемой информационной угрозы. При этом если система защиты информации объекта не обладает достаточно эффективными силами и средствами противодействия новой информационной угрозе, то возникает необходимость в поиске и привлечении дополнительных сил и средств защиты с последующим принятием решения об их применении.

Действия сил и средств защиты информации по ликвидации информационной угрозы (операция O_4) в случае известной угрозы осуществляются автоматически и занимают непродолжительное время $\hat{\tau}_4$. Если угроза неизвестна, то время $\hat{\tau}_4$ может быть существенно увеличено.

Оценка результативности отражения информационной угрозы (операция O_5 продолжительностью $\hat{\tau}_5$) формируется на основе следующих действий [10, 12, 13]:

— оценки способности имеющихся сил и средств защиты информации эффективно отражать различные информационные угрозы, в том числе в условиях их изменения;

— выявления особенностей изменившихся и новых информационных угроз;

— изучения возможностей перспективных сил и средств защиты информации.

Актуализация информационной базы (операция O_6 продолжительностью $\hat{\tau}_6$) представляет собой процесс накопления данных о различных видах информационных угроз с целью

обеспечения защиты соответствующей информационной структуры. От степени полноты этой базы зависит продолжительность выполнения операций O_2 и O_3 (см. рис. 1).

Эффективность процесса отражения информационных угроз в рассматриваемом случае может быть оценена вероятностью достижения цели — ликвидации угрозы нарушения информационной структуры объекта:

$$P_{\text{д.ц}}(t) = P\left[(\hat{v} \ge v^*) \wedge (\hat{r} \le r^*) \wedge (\hat{\tau} \le \tau^*)\right] = \int_v \int_r \int_\tau \varphi_{<\hat{v},\hat{r},\hat{\tau}>}(v, r, \tau)\delta v \delta r \delta \tau, \quad (1)$$

где $\hat{v}$ — целевой эффект процесса функционирования системы защиты информации, заключающийся в обнаружении информационных признаков угрозы; $\hat{r}$ — ресурс сил и средств защиты информации; $\hat{\tau}$ — время, необходимое для ликвидации угрозы; $\varphi_{<\hat{v},\hat{r},\hat{\tau}>}(v, r, \tau)$ — совместная плотность вероятности случайных величин $\hat{v}$, $\hat{r}$ и $\hat{\tau}$. (Вывод аналитического выражения является самостоятельной задачей, не входящей в рамки данного исследования.)

В связи с тем, что в процессе ликвидации угрозы задействуется весь возможный ресурс сил и средств, выполнение требования $\hat{r} \le r^*$ в формуле (1) может быть принято за достоверное и за счет использования эффекта поглощения исключено из дальнейшего рассмотрения [11]. Тогда выражение (1) может быть представлено следующим образом:

$$P_{\text{д.ц}}(t) = \int_0^v \varphi_{<\hat{v}>}(v)\left[\int_0^\tau \varphi_{<\hat{\tau}/v>}(\tau; v) d\tau\right] dv, \quad (2)$$

где $\varphi_{<\hat{v}>}(v)$ — плотность вероятности случайной величины $\hat{v}$; $\varphi_{<\hat{\tau}/v>}(\tau; v)$ — условная плотность вероятности случайной величины $\hat{\tau}$ при заданном значении v случайной величины $\hat{v}$; при проведении расчетов величина v может принимать значение в интервале от 0 до 1 [14].

Для того чтобы найти аналитические выражения плотностей вероятностей, входящих в уравнение (2), необходимо установить вид функции связности между переменными $\hat{v}$ и $\hat{\tau}$. С этой целью приведем следующие рассуждения.

Пусть средства мониторинга угроз информационной структуре объекта обнаруживают информационный признак угрозы за время t с вероятностью $P(t)$, а за время δt — с вероятностью $P(t, t+\delta t)$. Чтобы быть обнаруженным за время $(t+\delta t)$, информационный признак угрозы должен быть обнаружен либо за время t, либо за время $[t,\ (t+\delta t)]$ (рис. 2). Зависимость между вероятностями $P(t)$ и $P(t, t+\delta t)$ заключается в следующем. Так как необнаружение информационного признака за время $(t+\delta t)$ означает необнаружение его ни в интервале [0, t], ни в интервале $[t,\ (t+\delta t)]$, то в соответствии с основными положениями теории вероятности [11, 14] можно записать:

$$1 - P(t+\delta t) = \left[1 - P(t)\right]\left[1 - P(t, t+\delta t)\right], \quad (3)$$

т.е. вероятность первого события равна произведению вероятностей двух других событий. При этом вероятность $P\left(t, t+\delta t\right)$ представляет собой условную вероятность обнаружения объекта, вычисленную при условии, что поиск объекта до момента времени t был безрезультатным. Эта условная вероятность необнаружения объекта за бесконечно малое время называется *элементарной*. Элементарная вероятность с точностью до бесконечно малой величины высшего порядка $p\left(\delta t\right)$ пропорциональна бесконечно малому временному интервалу δt, что может быть записано в следующем виде:

$$P(t, t+\delta t) = \gamma(t)\delta t + p(\delta t). \quad (4)$$

В этом уравнении величину $\gamma(t)$ называют интенсивностью поиска. Ее физический смысл заключается в математическом ожидании числа обнаружений информационных признаков, приходящихся на единицу времени [4].

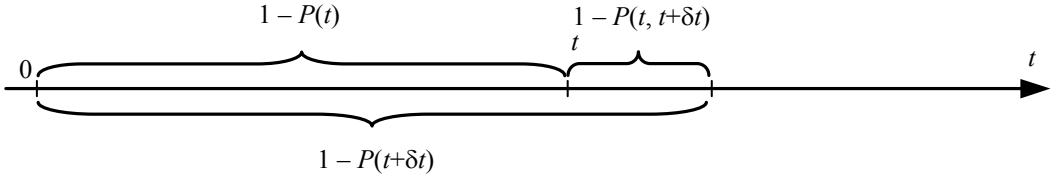

Рис. 2

При $\delta t \to 0$ может быть получено дифференциальное уравнение с разделяющимися переменными:

$$\frac{\delta P(t)}{\delta t} = \left[1 - P(t)\right]\gamma(t). \tag{5}$$

Интегрируя выражение (5) при начальных условиях $P(0) = 0$ (обнаружение информационного признака в момент его возникновения), получаем:

$$P(t) = 1 - e^{-\lambda(t)}, \tag{6}$$

где $\lambda(t) = \int_0^t \gamma(t)\delta t$ — математическое ожидание числа обнаружений за время поиска, называемое потенциалом обнаружения [14].

Предположив, что $\lambda(t) = \text{const}$, можно записать:

$$\hat{v}(t) = 1 - e^{-\lambda(t - \hat{\tau}_1 - \hat{\tau}_з)}, \tag{7}$$

где $\hat{\tau}_1$ – операционное время (время вскрытия факта информационного воздействия); $\hat{\tau}_з = \sum_{i=2}^{6} \hat{\tau}_i$ — технологическая задержка.

В практике моделирования [11] считается, что наиболее корректной моделью плотности распределения операционного времени $\hat{\tau}_1$ является экспоненциальный закон распределения

$$\varphi^{[\lambda]}_{<\hat{\tau}_1>}(\tau) = \lambda e^{-\lambda\tau_1}.$$

Поиск окончательной формы аналитической зависимости (2) предполагает установления вида плотностей распределения вероятностей $\varphi_{<\hat{v}>}(v)$ и $\varphi_{<\hat{\tau}/v>}(\tau; v)$. В соответствии с законом распределения монотонной функции от одного случайного аргумента (функции связности (7)) можно записать [11]:

$$\varphi_{\hat{v}}(v) = \varphi_{\hat{\tau}_1}\left[\tau_1(v)\right]\left[\tau_0(v)\right]', \tag{8}$$

где $\left[\tau_0(v)\right]'$ — производная функции $\tau_0(v)$, обратной функции $v(\tau_0)$;

$$\tau_1(v) = v^{-1}(\tau_1) = \hat{\tau}_з - \frac{1}{\lambda}\ln(1 - v), \tag{9}$$

$$[\tau_1(v)]' = -\frac{1}{\lambda(1 - v)}. \tag{10}$$

В свою очередь, так как $\hat{\tau} = \tau_1 + \hat{\tau}_з = \tau_1 - \frac{1}{\lambda}\ln(1-v) + \hat{\tau}_з$, то

$$\varphi_{\hat{\tau}/\hat{v}}(\tau; v) = \varphi_{\hat{\tau}_1/v}(\tau; v) \otimes \varphi_{\hat{\tau}_з}(\tau) = \delta\left(\tau - \tau_1 \frac{1}{\lambda}\ln(1-v)\right) \otimes \varphi_{\hat{\tau}_з}(\tau), \qquad (11)$$

где $\otimes$ — символ композиции законов распределения случайных величин.

Плотность вероятности случайных величин, характеризующих продолжительность операций, составляющих технологическую задержку, как правило, моделируют нормальным законом распределения. В силу закона композиции нормальных плотностей вероятностей можно записать:

$$\varphi_{\hat{\tau}_з}(\tau) = \frac{1}{\sqrt{2\pi\sum_{i=2}^{6}\sigma^2_{\hat{\tau}_i}}} \exp\left\{\left(\tau - \sum_{i=2}^{6} m_{\hat{\tau}_i}\right)^2 \Big/ 2\sum_{i=2}^{6}\sigma^2_{\hat{\tau}_i}\right\}, \qquad (12)$$

где $m_{\hat{\tau}_i}$ — математическое ожидание случайной величины $\hat{\tau}_i$, $i = \overline{2, 6}$, характеризующей продолжительность выполнения операций O_2 … O_6; $\sigma_{\hat{\tau}_i}$ — дисперсия этих случайных величин.

Результаты интегрирования уравнения (2) с учетом выражений (8) — (12) при помощи пакета прикладных программ MatLab 7 [14, 15] приведены на рис. 3. Расчеты проводились при следующих исходных данных: $\lambda = 1$ обнаружений/ч (размерность величины); $m_{\hat{\tau}_2} = 0{,}01$/ч; $\sigma_{\hat{\tau}_2} = 0{,}002$/ч; $m_{\hat{\tau}_3} = 0{,}03$/ч; $\sigma_{\hat{\tau}_3} = 0{,}008$/ч; $m_{\hat{\tau}_4} = 0{,}1$/ч; $\sigma_{\hat{\tau}_4} = 0{,}03$/ч; $m_{\hat{\tau}_5} = 0{,}225$/ч; $\sigma_{\hat{\tau}_5} = 0{,}062$/ч; $m_{\hat{\tau}_6} = 0{,}3$/ч; $\sigma_{\hat{\tau}_6} = 0{,}09$/ч. При этом сдвиг графиков $P_{д.ц}(t)$ по оси t на величину $\sum_{i=2}^{6} m_{\hat{\tau}_i} = 0{,}6$ ч не показан.

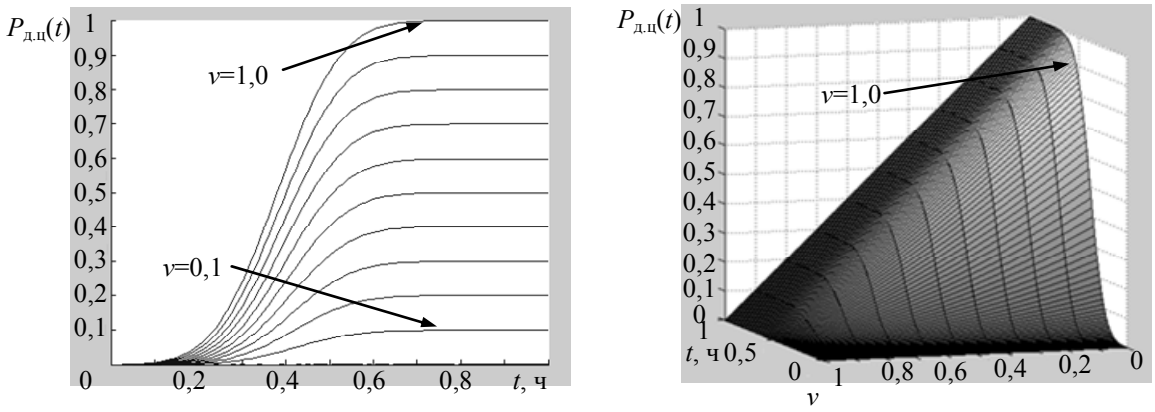

Рис. 3

На рис. 4 представлена операционно-временная модель процесса отражения новой угрозы элементами ГИС, система защиты информации которой построена по адаптационной схеме. Согласно этой схеме в элементе, который подвергся новому информационному воздействию, осуществляется адаптивная перестройка структуры СЗИ в зависимости от характера этого воздействия. Одновременно информация о характере новой информационной угрозы и вариантах перестроения структуры СЗИ поступает в информационные базы информационных угроз всех остальных элементов ГИС. Это позволяет, во-первых, увеличить интенсивность обнаружения λ информационных признаков новых угроз за счет организации их целенаправленного поиска в информационном пространстве (сокращения пространства поиска) и, во-вторых, уменьшить параметры законов распределения случайных величин $\hat{\tau}_2$ и $\hat{\tau}_3$.

Таким образом, в зависимости от степени изменения параметров λ, $m_{\hat{\tau}_2}$, $\sigma_{\hat{\tau}_2}$, $m_{\hat{\tau}_3}$ и $\sigma_{\hat{\tau}_3}$ в соответствующей степени будет повышена эффективность системы защиты информации ГИС в целом.

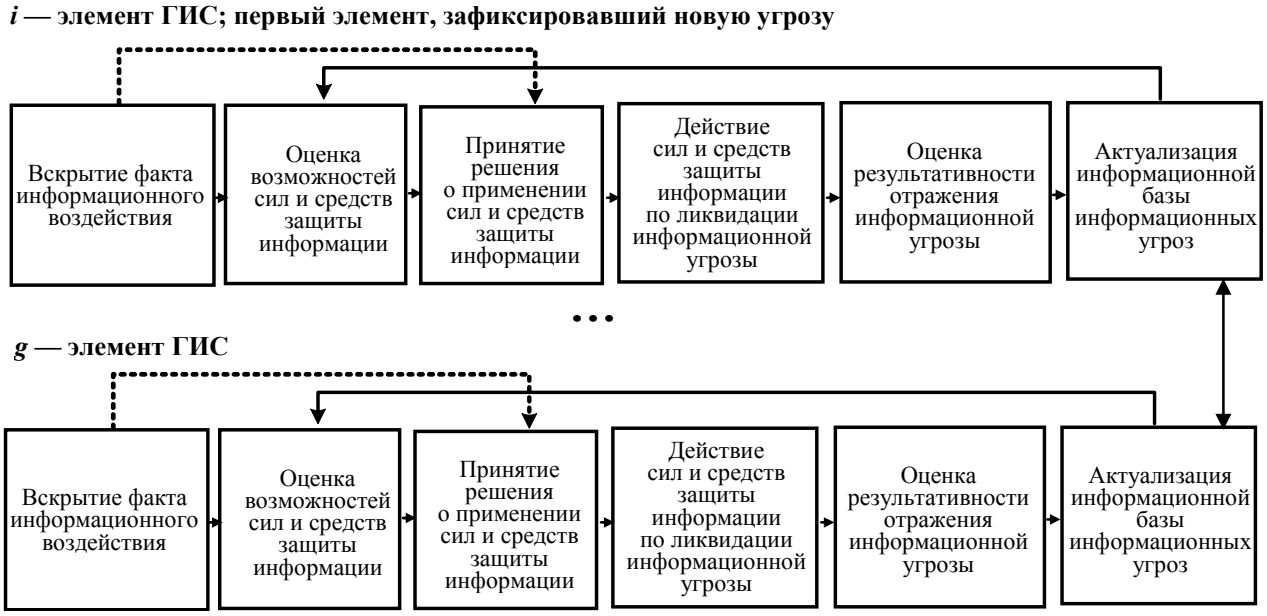

Рис. 4

Результаты представленного исследования направлены на получение объективной оценки эффективности защиты информационных систем, основанной на вероятностном подходе, что позволит избежать субъективности традиционно используемых экспертных оценок.

СПИСОК ЛИТЕРАТУРЫ

1. *Коломойцев В. С., Богатырев В. А.* Оценка эффективности и обоснование выбора структурной организации системы многоуровневого защищенного доступа к ресурсам внешней сети // Информация и космос. 2015. № 3. С. 71—79.

2. *Гатчин Ю. А., Сухостат В. В.* Теория информационной безопасности и методология защиты информации. СПб: СПбГУ ИТМО, 2010. 98 с.

3. *Mesarovic M. D., Yasuhiko Takahara*. General Systems Theory: Mathematical Foundations. N.Y.: Academic Press. 1975.

4. *Stephan C., Kohl M., Turewicz M., Podwojski K., Meyer H. E., Eisenacher M.* Using laboratory information management systems as central part of a proteomics data workflow // Proteomics. 2010. Vol. 10, N 6. P. 1230—1249.

5. *Bowden D.* Information, systems and information systems: making sense of the field // Intern. J. of Information Management. 1998. Vol. 18, N 4. P. 287.

6. *Бабина О. И., Дюмин Н. Ю., Исмаилова Л. Ю., Косиков С. В., Курбанмагомедов К. Д., Кутузов Д. В., Стукач О. В., Морозова А. В., Нифонтова О. М., Богданов А. Н., Жабреев В. С., Половова Т. Н., Сорокун И. В., Багнетова Е. А., Шапошникова Е. А., Корчина Т. Я.* Информационные системы и технологии: Монография. Красноярск: Научно-инновационный центр, 2011. 156 с.

7. *Статьев В. Ю., Тиньков В. А.* Информационная безопасность распределенных информационных систем // Информационное общество. 2001. № 1. С. 12—16.

8. *Богатырев В. А., Богатырев А. В.* Оптимизация резервированного распределения запросов в кластерных системах реального времени // Информационные технологии. 2015. Т. 21, № 7. С. 495—502.

9. *Богатырев В. А., Попова М. В., Богатырев С. В., Кудрявцева В. Ю., Фокин А. Б.* Оптимизация вычислительных систем с объединением межсетевых экранов в отказоустойчивые кластеры // Научно-технический вестник СПбГУ ИТМО. 2011. № 6 (76). С. 140—142.

10. *Богатырев В. А., Богатырев А. В., Богатырев С. В.* Оценка надежности выполнения кластерами запросов реального времени // Изв. вузов. Приборостроение. 2014. Т. 57, № 4. С. 46—48.

11. *Петухов Г. П., Якунин В. И.* Методологические основы внешнего проектирования целенаправленных процессов и целеустремленных систем. М.: АСТ, 2006.

12. *Богатырев В. А.* Оценка надежности и оптимальное резервирование кластерных компьютерных систем // Приборы и системы. Управление, контроль, диагностика. 2006. № 10. С. 18—21.

13. *Богатырев В. А., Фокин С. Б., Попова М. В.* Оценка и выбор отказоустойчивых конфигураций межсетевых экранов // Научно-технический вестник СПбГУ ИТМО. 2011. № 3 (73). С. 139—140.

14. *Вентцель Е. С.* Теория вероятностей: Учебник для вузов. М.: Высш. школа, 1999.

15. *Ануфриев И. Е., Смирнов А. Б., Смирнова Е. Н.* MatLab-7. СПб: БХВ-Петербург, 2005.

Сведения об авторах

Игорь Михайлович Левкин — д-р военных наук, профессор; Университет ИТМО; кафедра бортовых систем управления оружием и вооружением (базовая); E-mail: lev.kin@yandex.ru

Анастасия Андреевна Володина — аспирант; Университет ИТМО; кафедра мониторинга и прогнозирования информационных угроз; E-mail: nasti.vol@gmail.com

Рекомендована кафедрой мониторинга и прогнозирования информационных угроз

Поступила в редакцию 11.02.16 г.

Ссылка для цитирования: *Левкин И. М., Володина А. А.* Агрегированная операционно-временная модель оценивания эффективности отражения информационных угроз в больших информационных системах // Изв. вузов. Приборостроение. 2016. Т. 59, № 5. С. 335—341.

AGGREGATED TIME-OPERATION MODEL FOR ASSESSMENT OF INFORMATION THREAT COMBATING EFFICIENCY IN LARGE INFORMATION SYSTEMS

I. M. Levkin, A. A. Volodina

ITMO University, 197101, St. Petersburg, Russia
E-mail: nasti.vol@gmail.com

The problem of improvement of information protection systems is analyzed on the base of an estimate for the efficiency of information threats combating process in large information systems. The process of combating of threats to an element of information system of an enterprise is represented as an aggregated time-operation model. A mathematical technique based on random variable distribution law is employed. An assessment of time costs correlation with the efficiency of information protection for separate information structures is presented. Efficiency of the process of previously unknown treats combating by an information protection system built on the adaptation principle is estimated. The adapting schema is shown to allow for reconstruction of the structure of information protection system depending on the impact nature.

Keywords: information threat combating, large information systems, efficiency, time-operation model, adaptation

Data on authors

Igor M. Levkin — Dr. Sci., Professor; ITMO University, Department of On-Board Weapons Control Systems; E-mail: lev.kin@yandex.ru

Anastasia A. Volodina — Post-Graduate Student; ITMO University, Department of Monitoring and Information Security Risks' Forecasting; E-mail: nasti.vol@gmail.com

For citation: *Levkin I. M., Volodina A. A.* Aggregated time-operation model for assessment of information threat combating efficiency in large information systems // Izv. vuzov. Priborostroenie. 2016. Vol. 59, N 5. P. 335—341 (in Russian).

DOI: 10.17586/0021-3454-2016-59-5-335-341