

УДК: 007

**МЕТОДИКА ОПРЕДЕЛЕНИЯ ОПТИМАЛЬНОЙ ПЕРИОДИЧНОСТИ
КОНТРОЛЯ СОСТОЯНИЯ СЛОЖНОГО ОБЪЕКТА**
**METHOD FOR DETERMINING OPTIMUM PERIODICITY OF COMPLEX
OBJECT STATE MONITORING**

*Д-р воен. наук Ю.И. Стародубцев, канд. техн. наук С.А. Иванов,
канд. техн. наук П.В. Закалкин, канд. техн. наук Е.В. Вершенник*

*DPhil Yu.I. Starodubcev, PhD S.A. Ivanov,
PhD P.V. Zakalkin, PhD E.V. Vershennik*

Военная академия связи им. С.М. Буденного

Интеграция сложных технологических систем в мировое киберпространство привело к увеличению скоординированных воздействий на них как организованных хакерских сообществ, так и кибертеррористов. Частным случаем таких воздействий является перевод сложных технологических систем в критические (закритические) режимы функционирования за счет изменения условий и параметров функционирования объекта. Непрерывный мониторинг всех параметров сложного объекта требует привлечения больших измерительных и вычислительных ресурсов, что негативно влияет на работу системы. В статье рассматривается методика определения оптимальной периодичности контроля состояния сложного объекта. Предлагаемая методика за счет минимизации количества измеряемых параметров позволяет снизить вычислительную нагрузку на средства контроля и автоматизации управления сложного объекта. Одновременно с этим методика обеспечивает сохранение степени информированности о состоянии сложного объекта и определяет оптимальную периодичность контроля параметров в различных фазах функционирования объекта.

Ключевые слова: сложный объект, периодичность контроля, информированность, аппроксимация.

The integration of complex technological systems into the global cyberspace has led to an increase in the coordinated impact on them of both organized hacker communities and cyberterrorists. Special cases of such impacts are the transfer of complex technological systems to critical (off-critical) modes of operation, due to changes in the conditions and parameters of the operation of the object. Continuous monitoring of all parameters of a complex object requires large measurement and computing resources, which negatively affects the operation of the system. The article deals with the method of determining the optimal frequency of monitoring the state of a complex object. The proposed method, by minimizing the number of measured parameters, reduces the computational load on the control and control automation tools of a complex object. At the same time, the method ensures the preservation of the degree of awareness about the state of a complex object and determines the optimal frequency of monitoring parameters in various phases of the object's operation.

Keywords: complex object, frequency of control, awareness, approximation.

Появление киберпространства и кибероружия предопределило переход к новому типу войн. Это привело к тому, что в целях обеспечения военной безопасности и готовности вооруженных сил и государства в целом к войнам будущего, мировым сообществом активно прорабатывались концепции информационных и техносферных войн. Наиболее подходящей в сложившейся военно-политической обстановке и техническому прогрессу стала концепция техносферных войн впервые представленная и описанная в [1–2].

Воздействие на сложные технологические системы, такие как сети операторов связи, автоматизированные системы управления технологическими процессами и т.д., с дальнейшим переводом их в критические режимы функционирования для достижения поставленных целей (крайним случаем являются техногенные катастрофы) на данный момент проходят обкатку в боевых условиях (например: кибервоздействия на ГЭС Венесуэлы) и является основным сценарием, используемым как вооруженными силами зарубежных государств, так и крупными хакерскими группами.

Частными случаями перевода сложных технологических систем (далее — сложный объект) в деструктивный режим функционирования являются:

- искажение или блокирование исходных данных без непосредственного доступа к системам управления;
- изменение параметров функционирования системы управления;
- изменение условий функционирования, на которые рассчитывалась система управления.

Таким образом, необходимо осуществлять непрерывный контроль всех параметров сложного объекта, что требует привлечения больших измерительных и вычислительных ресурсов, а время реакции на изменения параметров и, следовательно, состояния объекта должно быть максимально высоким. Стоимость систем контроля и автоматизации управления объектом в этом случае может быть неприемлема. Одним из решений данной проблемы является разработка подходов, позволяющих определять оптимальную периодичность контроля параметров (состояний) сложных объектов, которые должны учитывать информативность параметров объек-

та и дестабилизирующих факторов для определения его состояния, взаимосвязи параметров между собой, интенсивность изменения параметров в различных фазах функционирования элементов объекта и объекта в целом, ресурсы системы контроля и автоматизации управления объектом и др.

Известные подходы [3–10] в области периодичности контроля состояния сложных объектов и разрабатываемые способы защиты [11–15] обладают следующими основными недостатками:

- ограниченная область применения. Кроме того, результаты контроля указывают только на критические значения параметров. Восстановление контролируемого процесса с заданной точностью невозможно;

- высокая нагрузка на средства контроля и автоматизации управления сложного объекта, обусловленная реализуемым подходом контроля параметров по наихудшему варианту деструктивных воздействий в течении всего времени функционирования объекта.

Таким образом, задача снижения нагрузки на средства контроля и автоматизации управления сложного объекта за счет минимизации количества измеряемых параметров с сохранением степени информированности о состоянии сложного объекта и определения оптимальной периодичности контроля этих параметров в различных фазах функционирования объекта является актуальной. Для решения поставленной задачи была разработана методика определения оптимальной периодичности контроля состояния сложного объекта [16]. Обобщенная структурно-логическая последовательность предлагаемой методики представлена на рис. 1.

Исходными данными методики являются:

- множество аппроксимирующих функций (функции должны быть гармоническими);
- точность аппроксимации $\epsilon_{тр}$, которая определяет возможность применения гармонических функций для аппроксимации характеристики параметра сложного объекта на временном промежутке, а также является критерием для смены аппроксимирующей функции при аппроксимации характеристики параметра в целом;
- пределы и шаг изменения параметров аппроксимирующих функций;
- N состояний сложного объекта и M параметров, характеризующих его состояние. Задание

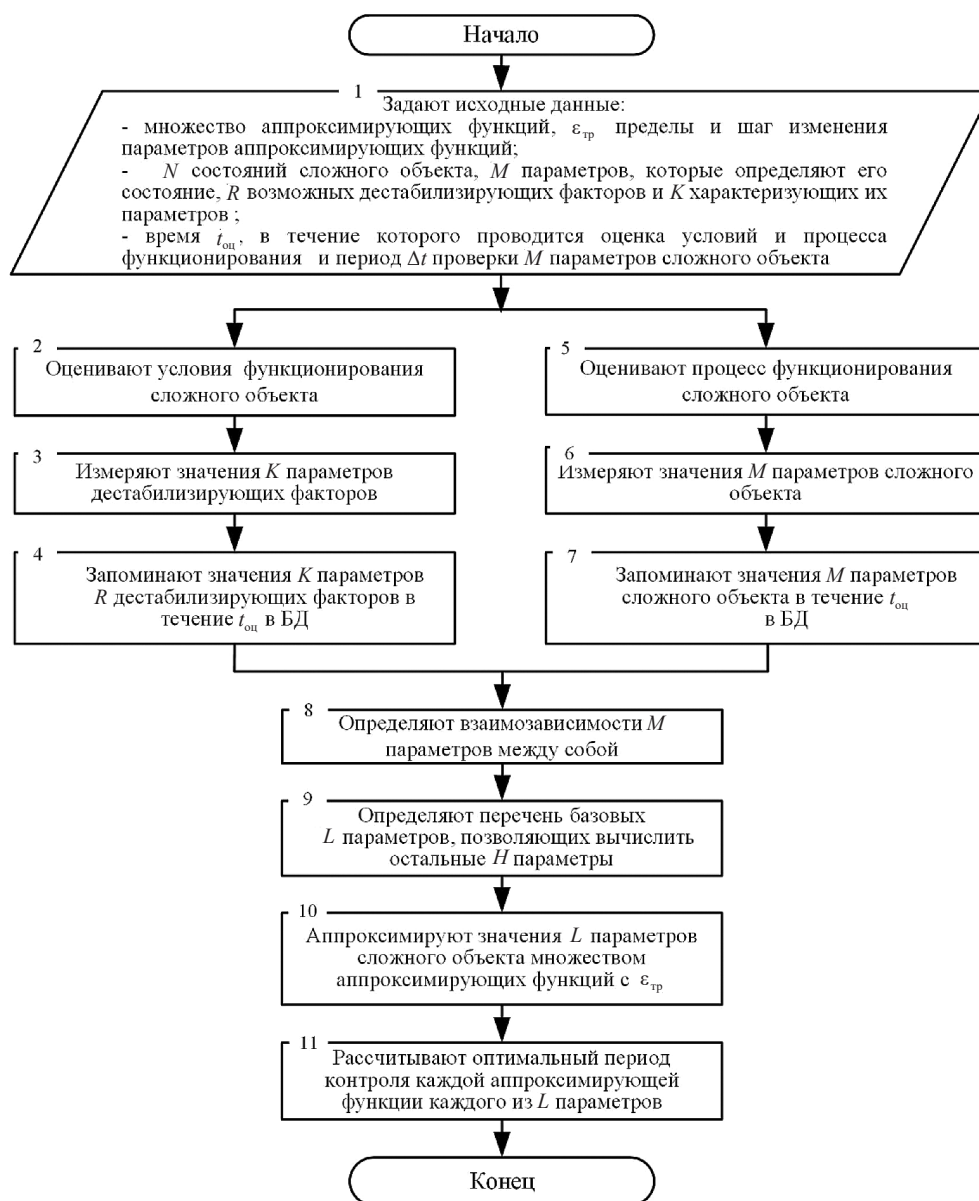


Рис. 1. Обобщенная структурно-логическая последовательность методики определения оптимальной периодичности контроля состояния сложного объекта

состояний и параметров сложных объектов возможно исходя из результатов их моделирования, проектирования и производства, а также исходя из опыта их эксплуатации. Значения параметров сложного объекта должны определять состояние, в котором он находится. Например: сложный объект — сеть связи; состояния — выключена, функционирует штатно, функционирует в час наибольшей нагрузки, функционирует под предкритической нагрузкой, находится в критическом состоянии (возможно восстановление), находится в закритическом состоянии (невоз-

можно восстановление); тогда параметрами, характеризующими ее состояние могут выступать пропускная способность, задержка передачи информации, уровень деградации оптического волокна, загруженность вычислительного ресурса автоматизированной системы управления и др.;

– R возможных внутренних и внешних дестабилизирующих факторов и K характеризующих их параметров. Например, дестабилизирующим фактором для сети электросвязи является физический или технологический процесс внутреннего или внешнего, по отношению к сети

электросвязи характера, приводящее к выходу из строя элементов сети;

– время $t_{\text{оц}}$, в течение которого проводится оценка условий и процесса функционирования сложного объекта, при этом в течении $t_{\text{оц}}$ объект должен находиться в каждом из N возможных состояний под воздействием R дестабилизирующих факторов; например, оценка сложного объекта — самолета, проводимая согласно отраслевого стандарта (ОСТ) в течении $t_{\text{оц}}$, установленной программой и методиками испытаний, в ходе которой самолет подвергается всем возможным деструктивным воздействиям внутреннего и внешнего характера (попадание молнии, град, боковой ветер, выход из строя узлов и агрегатов и др.) в различных состояниях (разгон по взлетной полосе, посадка, набор высоты, автоматическое и ручное управление и т.д.);

– период Δt проверки M параметров сложного объекта. При этом, на этапе оценки может задаваться наихудший случай, определяемый согласно [3, 10].

На следующем этапе исходные данные заносятся в базу данных и осуществляется оценка условий функционирования сложного объекта. При оценке условий функционирования сложного объекта формируют множество данных о времени и характере воздействия различных R дестабилизирующих факторов путем измерения значений соответствующих K параметров и записи их в базу данных в течение времени оценки $t_{\text{оц}}$ (рис. 2).

На следующем этапе производится оценка процесса функционирования сложного объекта, для чего в течение $t_{\text{оц}}$ измеряют значения M параметров сложного объекта. При этом в течении

$t_{\text{оц}}$ объект должен находиться в каждом из N возможных состояний под воздействием R дестабилизирующих факторов. Измеренные значения M параметров сложного объекта заносятся в базу данных.

Для измерения параметров могут использоваться как отдельные средства измерения, так и измерительные комплексы. Например, для волоконно-оптической системы передачи используются: рефлектометр для измерения характеристик линейного тракта (оптического волокна), когерентные измерители рассеянных сигналов для поиска виброакустических (деструктивных) воздействий на оптический кабель и повреждений, микроскоп для определения качества торцов оптического волокна, измерители оптической мощности для определения параметров сигнала, анализаторы транспортных сетей для тестирования канального оборудования и т.д.

Далее определяют взаимозависимости параметров (M) между собой. Определение взаимозависимостей осуществляется на основе корреляционного анализа с получением различных корреляционных коэффициентов (линейный, множественный, ранговый Спирмена, ранговый Кендалла и т.д.) между различными параметрами. При этом часть взаимозависимостей параметров может быть известна.

Определение взаимозависимости параметров M между собой возможно при помощи известных программных средств, например Statistica, MicroSoft Excel, SPSS, позволяющих выполнить корреляционный анализ на ЭВМ. После чего определяют перечень базовых параметров L , позволяющих вычислить остальные параметры H , при этом $M \leq L + H$.



Рис. 2. Обобщенная схема измерения параметров сложного объекта

Перечень базовых параметров должен быть достаточен для вычисления остальных, не вошедших в перечень, параметров и, одновременно, не быть избыточным, т.е. если при определении L базовых параметров посредством измерений и вычислений контролируются все параметры сложного объекта из множества M , недопустимо измерять остальные вычисляемые параметры (т.е. увеличивать нагрузку на средства контроля и автоматизации управления сложного объекта).

К базовым параметрам относят параметры с максимальной информативностью — параметры, установленные взаимосвязи которых позволяют вычислить максимальное количество других параметров. В этих целях строят вариационный ряд параметров в соответствии с количеством вычисляемых взаимосвязей с другими параметрами и выбирают минимальное, достаточное для вычисления остальных параметров, количество старших членов вариационного ряда.

В блоке 10 рис. 1, аппроксимируют значения каждого из L параметров сложного объекта множеством аппроксимирующих функций с заданной точностью $\varepsilon_{\text{тр}}$.

Полученные значения параметров аппроксимируют с заданной точностью $\varepsilon_{\text{тр}}$ непрерывными периодическими функциями (например, простыми гармоническими кривыми вида $y = A \sin(\omega_0 t + \varphi)$, $y = A \cos(\omega_0 t + \varphi)$, где A — амплитуда колебания; ω_0 — круговая (циклическая) частота; φ — начальная фаза колебания и др., удовлетворяющими заданным требованиям).

На рис. 3 представлен пример аппроксимации значений параметра A_l функциями вида $y = A \sin(ax + b)$ в различных фазах функциониро-

вания сложного объекта по l -му параметру. Учитывая, что косинус (синус) — периодическая функция с периодом 2π , ее период T может быть определен как $T = 2\pi/\omega_0$.

Число колебаний в единицу времени называется частотой колебания f . Очевидно, что частота f связана с продолжительностью одного колебания T следующим соотношением: $f = 1/T$.

Точность аппроксимации $\varepsilon_{\text{тр}}$ может оцениваться различными критериями приближения. Наибольшее распространение имеют:

– среднеквадратичное приближение, при котором требуют, чтобы среднее значение квадрата отклонения аппроксимирующей зависимости $i = \tilde{\Phi}(u)$ от действительной $i = \Phi(u)$ не превышало некоторой допустимой величины δ :

$$|\tilde{\Phi}(u) - \Phi(u)| \leq \delta,$$

в интервале $\Delta V = u_2 - u_1$ значений u , в пределах которого производится аппроксимация;

– равномерное приближение, при котором требуют, чтобы при любом значении u интервала ΔV величина отклонения $\tilde{\Phi}(u)$ от $\Phi(u)$ не превышала δ , т.е. $|\tilde{\Phi}(u) - \Phi(u)| \leq \delta$.

Точности аппроксимации и множество аппроксимирующих функций, удовлетворяющих заданным требованиям, задаются в исходных данных.

Согласно [17], как правило, достаточно точности аппроксимации — 0,05. Уменьшение допустимой точности приводит к значительному усложнению аппроксимирующей функции. Алгоритмы нахождения аппроксимирующих функций, в том числе тригонометрических, известны. Одним из примеров является многоступенчатый алгоритм нахождения тригонометрического полинома:

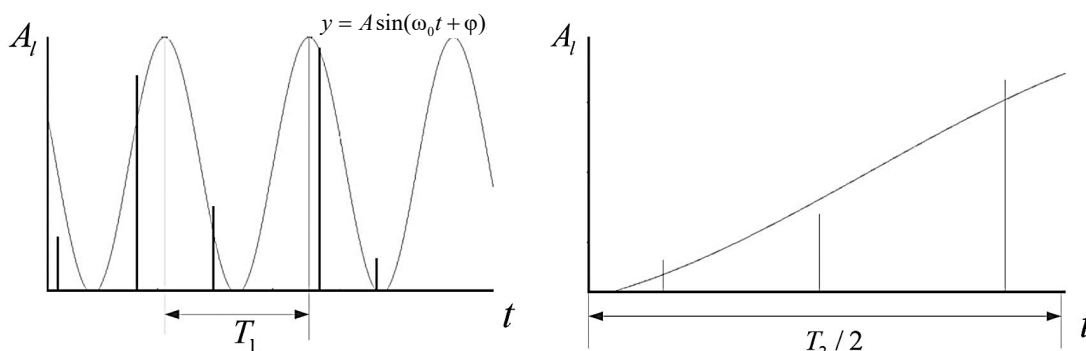


Рис. 3. Пример аппроксимации значений l -го параметра сложного объекта аппроксимирующими функциями вида $y = A \sin(ax + b)$.

- задается допустимая погрешность (точность аппроксимации) ϵ ;
- задаются величины вариаций параметров;
- определяется частота (выбор частоты осуществляется в соответствии с методом статистических испытаний; в заданном интервале генерируется некоторое количество j_1 равномерно распределённых случайных чисел. Из этого набора последовательно выбираются частоты);
- для каждой частоты вычисляются вариации для отдельных составляющих;
- выполняется проверка значения критерия.

В результате будет найдена частота и значения составляющих функции, которая обеспечивает минимальную погрешность при аппроксимации.

При нарушении требований к точности аппроксимации для описания значений l -го параметра сложного объекта находят другую аппроксимирующую функцию из заданного множества. Таким образом, значения каждого из L параметров сложного объекта в течении $t_{\text{оц}}$ аппроксимируют G_l гармоническими функциями из множества заданных функций аппроксимации, а время аппроксимации каждой функцией соответствует отдельной фазе функционирования сложного объекта по l -му параметру.

После определения всех аппроксимирующих функций, для получения значений оптимального периода контроля каждого из L параметров в каждой фазе, определяют частоты соответствующих аппроксимирующих функций.

Данный этап реализации способа базируется на одном из фундаментальных положений теоретической радиотехники — теореме Котельникова, согласно которой произвольный сигнал, спектр которого не содержит частот выше f_b , может быть полностью и однозначно восстановлен,

если известны отсчетные значения этого сигнала, взятые через равные промежутки времени $1/(2f_b)$.

Таким образом, если контроль будет проводиться через промежутки времени, равные отношению $T_{\text{контр}} = 1/(2f_b)$, где f_b — наибольшее значение частоты аппроксимирующей функции, то значения параметров контролируемого процесса могут быть однозначно восстановлены на заданном интервале времени. Поскольку все аппроксимирующие функции равномерные и гармонические, то $f_b = f$, где f — частота аппроксимирующей функции.

Согласно выражению $T_{\text{контр}} = 1/(2f)$ определяется оптимальный период для осуществления контроля каждого из L параметров в каждой фазе в условиях воздействия различных дестабилизирующих факторов.

Вывод

Представленная в статье методика за счет минимизации количества измеряемых параметров позволяет снизить вычислительную нагрузку на средства контроля и автоматизации управления сложного объекта.

Необходимо понимать, что численная оценка эффекта от применения разработанной методики будет зависеть от контролируемых параметров, состава конкретного объекта и изменяться в каждом конкретном случае. На рис. 4, 5 отображено графическое представление потенциального эффекта от применения методики.

На рис. 4 показана зависимость количества средств измерения I_{zm} и вычислительных средств V_s от числа измеряемых параметров N . Чем больше измеряемых параметров, тем больше требуется средств измерения I_{zm} и V_s вычислительных

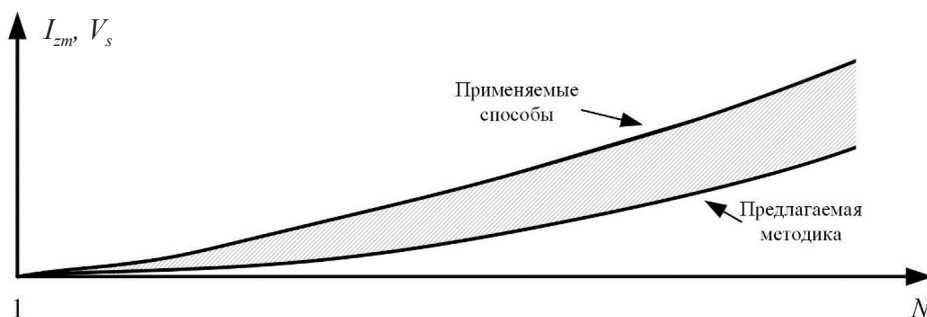


Рис. 4. Графическое представление потенциального эффекта от применения методики

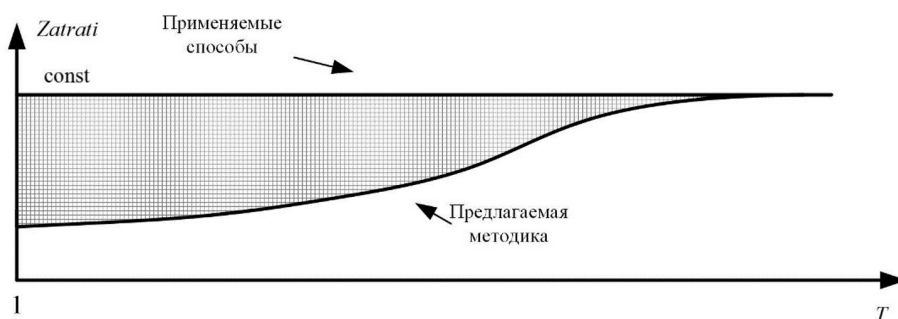


Рис. 5. Графическое представление потенциального эффекта от применения методики

средств. Предлагаемая методика за счет определения оптимальной периодичности контроля позволяет снизить количество используемых средств I_{zm} и V_s при том-же числе измеряемых параметров N .

На рис. 5 показана зависимость затрат на измерения $Zatrati$ от частоты изменения параметров T . В известных способах измерение параметров осуществляет постоянно с фиксированными затратами. Предлагаемая методика позволяет варьировать количеством применяемых средств в зависимости от частоты проводимых измерений. Чем меньше частота проводимых измерений, тем меньше требуется средств измерения и вычислительных средств. Например, возможно проводить несколько различных измерений последовательно с использованием одного средства измерения, а вычисления производить с меньшими затратами на вычислительные средства. Соответственно при снижении частоты проводимых измерений снижаются затраты на них и, наоборот, при увеличении частоты проводимых измерений увеличиваются затраты на них.

Одновременно методика обеспечивает сохранение степени информированности о состоянии сложного объекта и определяет оптимальную периодичность контроля параметров в различных фазах функционирования объекта. Новизна и промышленная применимость предлагаемой методики подтверждается патентом РФ [16].

Литература

1. Стародубцев Ю.И., Закалкин П.В., Иванов С.А. Техносферная война как основной способ разрешения конфликтов в условиях глобализации // Военная мысль. 2020. № 10. С. 16–21.

2. Бухарин В.В., Семенов С.С. и др. Техносферная война // Информационные системы и технологии. 2011. № 1 (63). С. 80–85.

3. Патент 2623791 Российская Федерация, МПК G05B 23/00 (2006.01), МПК G06Q 10/04 (2012.01). Способ определения оптимальной периодичности контроля состояния процессов // Синев С.Г., Сорокин М.А., Сухорукова Е.В. и др.; Заявитель и патентообладатель Стародубцев П.Ю. — 2016102219; заявл. 25.01.2016; опубл. 29.06.2017. бюл. № 19. 13 с.

4. Патент 2659374 Российская Федерация, МПК G05B 23/00 (2006.01), МПК G06F 19/00 (2011.01). Способ определения оптимальной периодичности контроля состояния технических средств и систем при минимальном времени получения результата // Алашеев В.В., Вершенник А.В., Карпов А.В., Латушко Н.А., Чеснаков М.Н. и др.; Заявитель и патентообладатель Алашеев В.В. и др. — 2017137312 заявл. 24.10.2017; опубл. 29.06.2018. бюл. № 19. 14 с.

5. Стародубцев Ю.И., Сухорукова Е.В., Закалкин П.В. Мониторинг корпоративных сетей // Проблемы экономики и управления в торговле и промышленности. 2016. № 1(13). С. 70–74.

6. Вершенник Е.В., Вершенник А.В., Львова Н.В., Стародубцев Ю.И. Предложения по повышению эффективности функционирования комплексов мониторинга // В сборнике: Неделя науки СПбПУ. материалы научной конференции с международным участием. 2017. С. 423–426.

7. Патент 2558333 Российская Федерация, МПК G01S 3/02. Способ определения местоположения несанкционированно установленных на объекте электронных устройств // Савченко Ю.Е., Сухорукова Е.В., Панкова Н.В. и др.; заявитель и патентообладатель Федеральное государственное бюджетное образовательное

учреждение высшего профессионального образования «Санкт-Петербургский государственный торгово-экономический университет». — 2014112381/07; заявл. 31.03.2014; опубл. 27.07.2015. бюл. № 21. 21 с.

8. Starodubcev U.I., Vershennik E.V., Balenko E.G. Method of monitoring the state of communication networks // В сборнике: 2019 International Science and Technology Conference «EastConf», EastConf 2019. 2019. С. 8725400.

9. Вершенник А.В., Вершенник Е.В., Стародубцев Ю.И. К вопросу об определении оптимальной периодичности контроля состояния объектов и процессов // В сборнике: Проблемы технического обеспечения войск в современных условиях. Труды III Межвузовской научно-практической конференции. 2018. С. 206–209.

10. Патент 2646321 Российская Федерация, МПК G06F 17/00 (2017.08); G06F 17/40 (2017.08). Способ мониторинга состояния электрических сетей и сетей связи // Стародубцев П.Ю., Чеснаков М.Н. и др.; заявитель и патентообладатель Стародубцев Ю.И., Вершенник Е.В. — 2017105612; заявл. 20.02.2017; опубл. 02.03.2018. бюл. № 7. 15 с.

11. Иванов С.А., Добрышин М.М. и др. Способ защиты серверов услуг сети связи от компьютерных атак // Вопросы оборонной техники. Серия 16. Технические средства противодействия терроризму. 2020. № 9–10 (147–148). С. 63–67.

12. Сидоренко Е.Н., Стародубцев Ю.И., Сухорукова Е.В., Фёдоров В.Г. Способ защиты информационно-телекоммуникационных сетей специального назначения от сетевых компьютерных атак // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании. Сборник научных статей: в 3-х томах. 2016. С. 333–337.

13. Бегаев А.Н., Гречишников Е.В., Добрышин М.М., Закалкин П.В. Предложение по оценке способности узла компьютерной сети функционировать в условиях информационно-технических воздействий // Вопросы кибербезопасности. 2018. № 3 (27). С. 2–8.

14. Добрышин М.М., Бречко А.А., Гуцын Р.В. и др. Предложение по снижению ущерба, наносимого сетевыми атаками серверу VPN // Вопросы оборонной техники. Серия 16. Техни-

ческие средства противодействия терроризму. 2020. № 3–4 (141–142). С. 111–116.

15. Бегаев А.Н., Добрышин М.М., Закалкин П.В., Реформат А.Н., Рауткин Ю.В. Комплексный алгоритм мониторинга защищенности узлов VPN от компьютерной разведки и DDOS-атак // Электросвязь. 2018. № 7. С. 46–52.

16. Патент 2718152 Российская Федерация, МПК G06F 17/10 (2006.01), МПК G06B 23/00 (2006.01), Способ определения оптимальной периодичности контроля состояния сложного объекта // Иванов С.А., Вершенник А.В., Шевчук А.Л., Карасенко А.О.; Заявитель и патентообладатель Вершенник Е.В. и др. — 2019143358; заявл. 24.12.2019; опубл. 30.03.2020. бюл. № 10. 19 с.

18. Хандрос М.Я. Тригонометрическая аппроксимация экспериментальных последовательностей. Вычисление естественных спектров. Электронный ресурс <http://perviydoc.ru/>. (Дата обращения 03.12.2019).

References

1. Starodubtsev Yu.I., Zakalkin P.V., Ivanov S.A. Technosphere war as the main method of conflict resolution in the context of globalization // Military thought. 2020. № 10. P. 16–21.

2. Bukharin V.V., Semenov S.S. et al. Technosphere war // Information Systems and Technologies. 2011. № 1 (63). P. 80–85.

3. Patent 2623791 Russian Federation, IPC G05B 23/00 (2006.01), IPC G06Q 10/04 (2012.01), Method for determining the optimal frequency of monitoring the state of processes // Sinev S.G., Sorokin M.A., Sukhorukova E.V. et al; Applicant and patentee Starodubtsev P.Yu. — 2016102219; application 25.01.2016; publ. 29.06.2017. byul. № 19. 13 p.

4. Patent 2659374 Russian Federation, IPC G05B 23/00 (2006.01), IPC G06F 19/00 (2011.01), a Method of determining the optimal frequency of monitoring of equipment and systems with a minimum of time of obtaining the result // Alashaev V.V., Vershennik A.V., Karpov A.V., Latushko N.A., Chesnakov M.N. et al; Applicant and patentee Alashaev V.V. and others. — 2017137312 Appl. 24.10.2017; publ. 29.06.2018. bull. № 19. 14 p.

5. Sukhorukova E.V., Zakalkin P.V. et al. Monitoring of corporate networks // Problems of

economics and management in trade and industry. 2016. № 1 (13). P. 70–74.

6. Vershennik E.V., Vershennik A.V., Lvo-va N.V., Starodubtsev Yu.I. Proposals for improving the efficiency of the functioning of monitoring complexes // In the collection: Week of Science of SPbPU. materials of the scientific conference with international participation. 2017. P. 423–426.

7. Patent 2558333 Russian Federation, IPC G01S 3/02. Method for determining the location of unauthorized electronic devices installed on the object // Zakalkin P.V., Savchenko Yu.E., Starodubtsev Yu.I., Sukhorukova E.V., Pan-kova N.V.; applicant and patent holder Federal State Budgetary Educational Institution of Higher Professional Education « Saint Petersburg State Trade and Economic University».

8. Starodubtsev Yu.I., Vershennik E.V., Balenko E.G. Method of monitoring the state of communication networks // In the collection: 2019 International Science and Technology Conference «EastConf», EastConf 2019. 2019. P. 8725400.

9. Vershennik A.V., Vershennik E.V., Staro-dubtsev Yu.I. On the question of determining the optimal periodicity of monitoring the state of objects and processes // In the collection: Problems of technical support of troops in modern conditions. Proceedings of the III Interuniversity Scientific and Practical Conference. 2018. P. 206–209.

10. Patent 2646321 Russian Federation, IPC G06F 17/00 (2017.08); G06F 17/40 (2017.08). Method for monitoring the state of electrical networks and communication networks // Starodubtsev P.Yu., Chesnakov M.N. et al; applicant and patent holder Starodubtsev Yu.I., Vershennik E.V. — 2017105612; application form 20.02.2017; publ. 02.03.2018. byul. № 7–15 p.

11. Ivanov S.A., Dobryshin M.M. et al. The method of protecting servers of communication

network services from computer attacks // Military Enginry. Issue 16. Counter-terrorism technical devices. 2020. № 9–10 (147–148). P. 63–67.

12. Sidorenko E.N., Sukhorukova E.V., Fedorov V.G. et al. Method of protection of information and telecommunications networks of special purpose from network computer attacks // In the collection: Actual problems of infotelecommunications in science and education. Collection of scientific articles: in 3 volumes. 2016. P. 333–337.

13. Begaev A.N., Grechishnikov E.V., Dobryshin M.M., Zakalkin P.V. A proposal for assessing the ability of a computer network node to function in the conditions of information and technical impacts // Cybersecurity issues. 2018. № 3 (27). P. 2–8.

14. Dobryshin M.M., Brechko A.A., Gutsyn R.V. et al. Proposal for reducing the damage caused by network attacks to the VPN server // Military Enginry. Issue 16. Counter-terrorism technical devices. 2020. № 3–4 (141–142). P. 111–116.

15. Begaev A.N., Dobryshin M.M., Zakal-kin P.V., Reformat A.N., Rautkin Yu.V. Complex algorithm for monitoring the security of VPN nodes from computer intelligence and DDOS attacks. 2018. № 7. P. 46–52.

16. Patent 2718152 Russian Federation, IPC G06F 17/10 (2006.01), IPC G06B 23/00 (2006.01), Method for determining the optimal frequency of monitoring the state of a complex object // Ivanov S.A., Vershennik A.V., Bakalkin P.V., Shevchuk A.L., Tarasenko A.O. et al; Applicant and patentee Vershen-nik E.V. — 2019143358; declared on 24.12.2019; published on 30.03.2020. byul. № 10. 19 p.

18. Khandros M.Ya. Trigonometric approx-imation of experimental sequences. The calculation of the natural spectra. Electronic resource <http://perviydoc.ru/>. Date of access 03.12.2019.