

УДК 681.518
DOI: 10.15827/0236-235X.118.307-313

Дата подачи статьи: 26.12.16
2017. Т. 30. № 2. С. 307–313

ПРОГРАММНО-АЛГОРИТМИЧЕСКИЙ КОМПЛЕКС ЗАЩИТЫ И УПРАВЛЕНИЯ ПРЕДПРИЯТИЕМ

В.Г. Матвейкин, д.т.н., профессор;
Б.С. Дмитриевский, д.т.н., доцент;
В.И. Медников, соискатель;
С.Г. Семержинский, аспирант, ipu@ahp.tstu.ru
(Тамбовский государственный технический университет,
ул. Советская, 106, г. Тамбов, 392000, Россия)

В статье описана математическая модель предприятия во взаимодействиях с внешней средой, осуществляемых за счет обмена ресурсами.

Через воздействия на ресурсы происходит как текущее управление предприятием менеджментом, так и реальное несанкционированное влияние на его деятельность со стороны субъекта или внешней среды. Несанкционированные воздействия выявляются при сравнении фактических и расчетных значений показателя деятельности на выбранном уровне исполнения функций. Если такое воздействие определено, система противодействия выполняет свою профильную функцию с целью достижения значения защищенности.

Показатель успешности защиты принят в форме минимальных требований к эффективности на основе статистик или экспертным путем. Найден технический параметр безопасности предприятия, который количественно характеризует неэффективность защиты.

Построена структура системы защиты и управления предприятием, которая выявляет и локализует несанкционированные влияния на его внутренние процессы и процессы взаимодействия с внешней средой без участия человека. Одновременно органично совмещает управление и защиту предприятия, существенно отличается от известных систем. Реализованная как программно-алгоритмический комплекс, система защиты и управления позволяет описывать все производственные процессы.

Предложены средства повышения достоверности и получения измерительной информации о состоянии ресурсов, контролирующие и идентифицирующие внешние влияния на каждый ресурс без участия человека. Разработаны средства получения количественной информации о состоянии ресурсов и найдены условия технической реализации предложенной системы защиты и управления предприятием.

Предложенные алгоритмы безопасного управления используют систему защиты ресурсов, которая надежно обеспечивает достоверность информации на всех уровнях управления. За счет использования представленной системы защиты и управления повышается эффективность предприятия во взаимодействиях с внешней средой.

Ключевые слова: модель предприятия, структура защиты, параметры защиты, риск, производственные ресурсы, субъект влияния, несанкционированное воздействие, показатель успешности защиты, уравнение безопасности ресурсов, угроза.

Вопросы управления предприятиями рассматривались во многих работах, например в [1–8]. Наибольшую актуальность они приобретают с точки зрения безопасности.

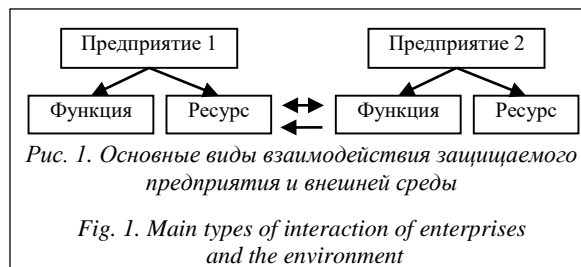
Законность защиты деятельности предприятий продиктована исполнением ими фундаментальной функции $f(s)$ в системе государства, поскольку целями создания любого из предприятий – производственного, оборонного, бюджетного и т.д. – являются удовлетворение потребности внешней среды в их продукции, в пополнении бюджетов разных уровней, в обеспечении благосостояния работающих на них людей.

Состояние предприятия в числе прочих критериев характеризуют его безопасное взаимодействие с внешней средой, влияние и рынок (рис. 1).

Безопасность предприятия закладывается на стадии его проектирования или приобретается во взаимодействиях в результате выполнения им функции защиты. Защита предприятия – его неотъемлемая как функция, так и ресурс; в свою очередь, функция защиты имеет две составляющие: обнаружение негативных влияний на ресурсы (функция

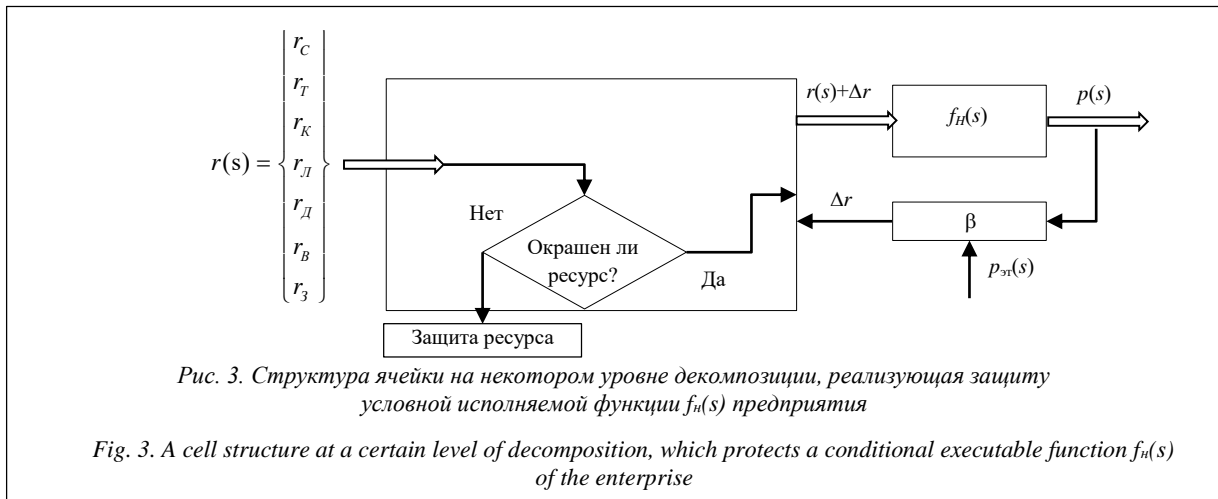
охраны ресурсов) и ликвидация негативных влияний (функция противодействия негативным влияниям).

Внешняя среда любого предприятия – это совокупность предприятий, потребителей, субъектов влияния, производителей со своими функциями назначения (на рисунке 1 внешняя среда – Предприятие 2).



Описание и оценка разработанного подхода

Для определения параметров системы защиты предприятие структурировано путем декомпози-



Структура ячейки, реализующей защищенное исполнение каждой функции предприятия на любом уровне его декомпозиции, показана на рисунке 3. На этом и последующих рисунках приняты обозначения: $r(s)$ – комплементарный ресурс; $f_n(s)$ – исполняемая производственная функция, например назначения; $p(s)$ – фактическое значение основного показателя на выбранном уровне; Δr – ресурсная добавка, вырабатываемая в результате управления; $p_{эт}(s)$ – расчетное (эталонное) значение основного показателя на выбранном уровне; β – решение менеджмента о необходимости ресурсной добавки; «Окрашен ли ресурс?» – оценка, вырабатываемая рубежом охраны ресурса по совокупности индикаторов, на выявление санкционированности управляющего воздействия на комплементарный ресурс. Структура, изображенная на

рисунке 4, состоящая из указанных ячеек, представляет общий случай реализации функции управления предприятием на атомном уровне его декомпозиции. Полная структура предприятия, реализующая многоуровневую среду создания основного показателя деятельности $p(s)$ [10], изображена на рисунке 5.

На рисунке 6 показано взаимодействие одной из ячеек (Яч 1-2) полной структуры защиты и управления предприятием (см. рис. 5) с контроллером РУ (например, на базе PIC-контроллера) атомного уровня исполнения функции $f_n(s)$ (см. рис. 4) с целью повышения достоверности информации о первичном производственном процессе защищаемого предприятия.

Достоверное распознавание каждой ячейкой влияний на ресурсы приблизило программную об-

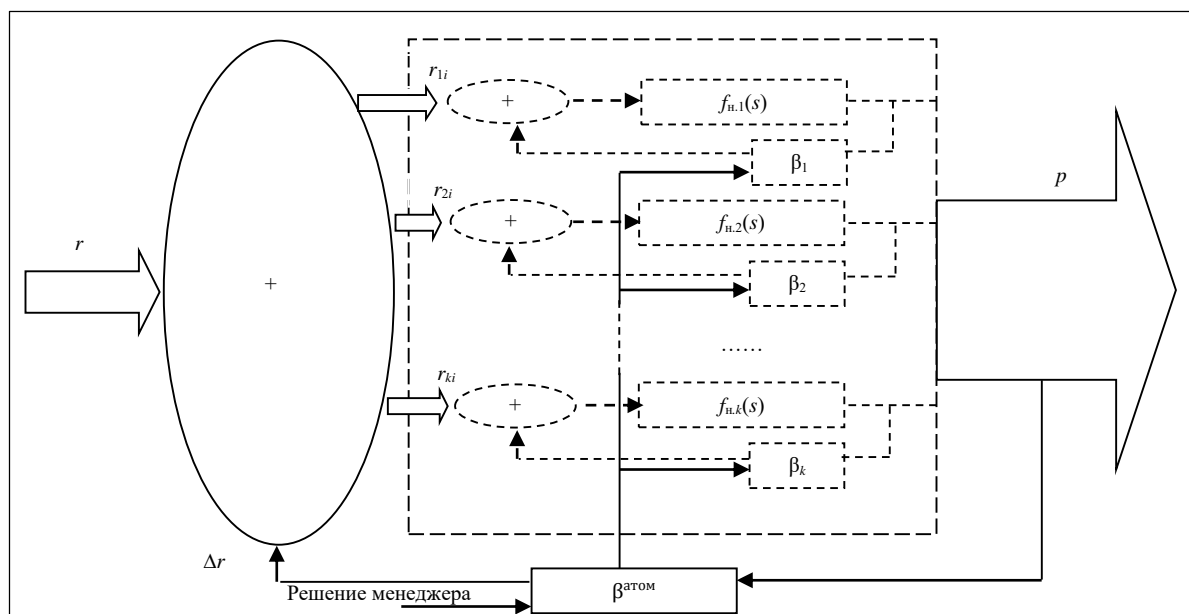


Рис. 4. Структура, реализующая управление исполнением функции $f_n(s)$ на атомном уровне предприятия (пример)

Fig. 4. The structure implementing execution control of function $f_n(s)$ at the atomic level of the enterprise (example)

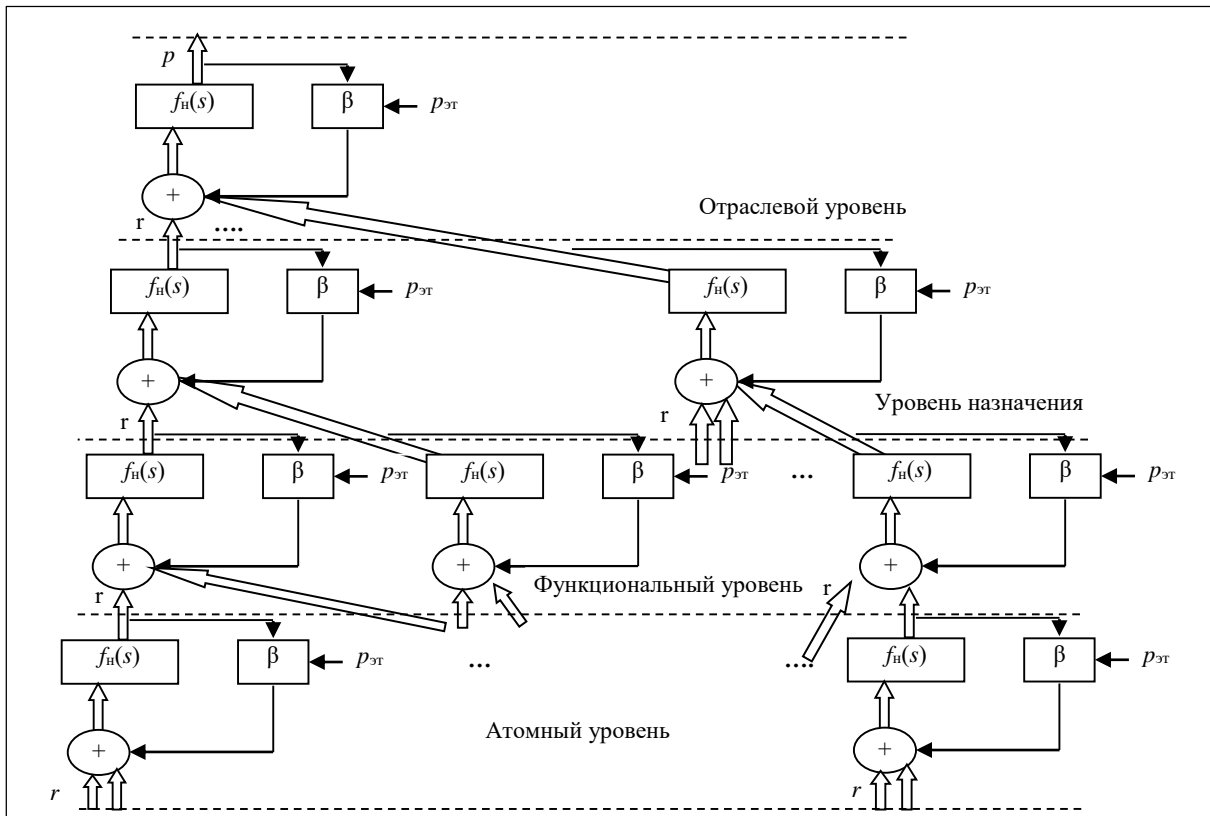


Рис. 5. Полная структура защиты и управления предприятием, состоящая из ячеек

Fig. 5. A full structure of enterprise protection and management consisting of cells

работку информации к первичным процессам и позволило использовать 1 бит для отражения состояния каждой из них в информационной части квитанции, выставляемой контроллеру РУ. Следствием такого приближения программной обработки является прозрачность исполнения функций на всех уровнях управления. Алгоритм квитирования запросов уровневого контроллера представлен по ссылке http://www.swsys.ru/uploaded/image/2017_2/2017-2-dop/5.jpg/.

Существенные отличия функциональных возможностей предложенной системы безопасного управления: 1) каждая ячейка любого уровня имеет обособленную структуру, цель и процесс; 2) ячейка общается с контроллером уровня по протоколу CDDI для повышения надежности информации о

внутренних процессах по разработанной программе квитирования запросов [11]; 3) взаимодействие ячеек соседних уровней происходит посредством защищенного коммуникативного ресурса, что обеспечивает искомое повышение надежности управления предприятием в целом за счет уменьшения вероятности ее катастрофического отказа; 4) система выполняет свои функции, начиная строго с первичных производственных процессов.

Информационная поддержка при принятии управленческих решений реализована путем распределения информации о внутренних процессах, о состоянии его ресурсов на всех уровнях между управленцами, а также организацией информационного обмена между хостом защищаемого предприятия и хостами предприятий-поставщиков сети.

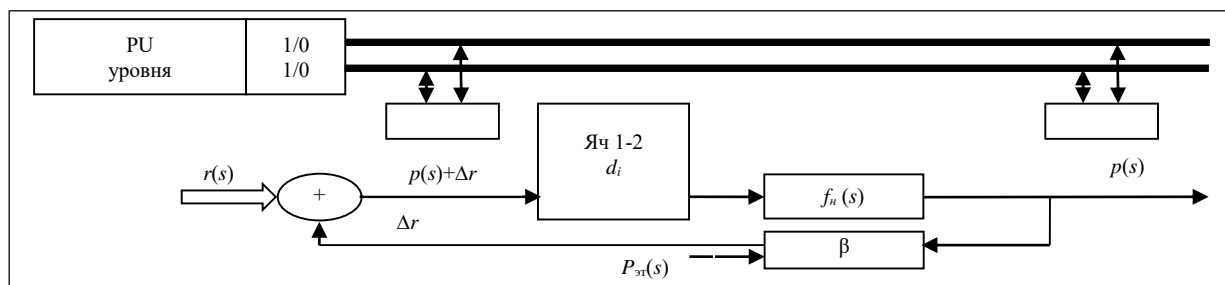


Рис. 6. Реализации взаимодействия ячейки «Яч 1-2» с контроллером РУ уровня

Fig. 6. Implementation of cell interaction with a level controller PU

Обсуждение проблемы

Не вызывает сомнений утверждение: как реальное текущее управление предприятием со стороны менеджмента, так и реальные несанкционированные влияния на его деятельность со стороны внешней среды или субъекта влияния производятся путем воздействия на ресурсы как средства осуществления его функций. Вследствие таких изменений ресурсов исполняемые предприятием функции также изменяются: санкционированно при управлении и несанкционированно при влияниях. Поэтому авторы сфокусировали интерес на определенных границ достаточности защиты предприятия с точки зрения как его внутренних процессов, так и процессов во внешней среде.

Практика деятельности предприятий показывает, что защищенность производственных ресурсов (как собственных, так и привлекаемых извне) недостаточна. Подсистема охраны ресурсов (одна из составных частей системы защиты) выявляет несанкционированное воздействие v_n (v – variety, n – негативное) на них по результату сравнения фактических и расчетных значений показателя $pi(s)$ деятельности на выбранном уровне исполнения функций. Если v_n выявлено, подсистема противодействия (другая составная часть системы защиты) выполняет свою профильную функцию, оказывая ему противодействие a_n (a – anti-variety) с целью достижения некоторого защищенного значения $p_3(s)$. Процедуру противодействия и его количественный результат на этом уровне формализуют уравнение защищенности во влияниях $p_3(s) = a_n v_n r(s) f(s)$, которое совпадает с основным уравнением безопасности на рынке, поэтому является его версией, его уточнением.

Практика показала: уже сейчас несложным для специалиста по защите предприятия является формирование аналитических записей влияний на каждую составляющую ресурса на каждом уровне исполнения функций (рис. 2) в виде $v_n a_n$. Например, для атомного уровня ресурса среды такое влияние v_n с есть появление вредностей в воздушной среде на рабочем месте в количестве, превышающем предельно допустимую концентрацию. Адекватным противодействием a_n с такому превышению является увеличение интенсивности воздухообмена в этой среде путем вентиляции. Аналогичные процедуры обеспечения безопасности выполняются для остальных ресурсных составляющих на остальных уровнях предприятия.

Показателем успешности защиты (охраны ресурсов и противодействия негативным влияниям на них) ресурсной составляющей x авторами принята эффективность: $E_{3,x} = E_{\text{опр } x} E_{n,x}$, количественное наполнение которого не унифицировано для всех уровней предприятия и не установлено на межотраслевом уровне по причине участия в его формировании человеческого фактора. Поэтому в настоя-

щее время он принят в форме минимальных требований к эффективности на основе статистик или экспертным путем.

Таким образом, технический параметр безопасности предприятия можно записать в виде $1 - E_{3,x} = 1 - E_{\text{опр } x} E_{n,x}$. Он количественно характеризует неэффективность защиты, или безнаказанность несанкционированного влияния на ресурсную составляющую x . На его основе можно записать уравнение безопасности ресурсов $r_{\text{безоп}}(s)$: $r_{\text{безоп}}(s) = E_{\text{П } c} E_{\text{опр } c} r_c(s) + E_{\text{П } k} E_{\text{опр } k} r_k(s) + E_{\text{П } t} E_{\text{опр } t} r_t(s) + E_{\text{П } л} E_{\text{опр } л} r_л(s) + E_{\text{П } д} E_{\text{опр } д} r_д(s) + E_{\text{П } в} E_{\text{опр } в} r_в(s) + E_{\text{П } з} E_{\text{опр } з} r_з(s)$, в котором мультипликаты $E_{\text{П}} E_{\text{опр}}$ означают, что ни охрана, ни противодействие не компенсируют друг друга при защите составляющих, то есть не являются взаимодополняемыми.

Полученное выражение для $r_{\text{безоп}}(s)$ дает защищенные (безопасные) значения основного показателя деятельности $p_{\text{безоп}}(s) = f(s) r_{\text{безоп}}(s)$ на выбранном уровне исполнения функции (структуры) предприятия во взаимодействиях.

Найденное уравнение безопасности позволило рассчитывать риск предприятия во взаимодействиях с внешней средой или, другими словами, относительный размер потерь ресурсов из-за несовершенства исполнения функции охраны и исполнения функции противодействия. Величина риска количественно определена, очевидно, разностью между расчетным $p(s)$ (эталонным) и безопасным $p_{\text{безоп}}(s)$ значениями основного показателя деятельности: $risk p(s) = p(s) - p_{\text{безоп}}(s) = p(s) - E_{\text{опр}} E_{\text{П } x} p(s) = (1 - E_{\text{опр}} E_{\text{П } x}) p(s)$, где $(1 - E_{\text{опр}} E_{\text{П}})$ – искомый риск предприятия во взаимодействиях с внешней средой.

Несовершенство современных технических средств защиты вынуждает менеджмент предприятий использовать человека в контуре защиты ресурсов. Попутно отметим: в теории экономических игр априори принятая 100 %-ная эффективность каждой из подсистем защиты ($E_{\text{опр}} = 1$, $E_3 = 1$ или нуль-эффект влияний) заставила отказаться от использования этой теории для решения задачи исследования.

Найденное выражение для риска приводит к количественному определению величины угрозы $Y(s)$ или $th(s)$ (threat – угроза) защищаемому ресурсу предприятия через эффективности $E_{\text{СВ}}$ и E_3 : угроза $Y(s)$ – это риск $(1 - E_{\text{П}} E_{\text{опр}})$, превысивший порог $(1 - E_{\text{П}} E_{\text{опр}})_{\text{пор}}$, установленный экспертным или иным путем. В рассматриваемом влиянии субъекта влияния на предприятие численное значение такого порога дает эффективность $E_{\text{СВ}}$ исполнения субъектом влияния своей функции назначения. Для такого влияния справедливо неравенство $Y(s) > (1 - E_{\text{П}} E_{\text{опр}})_{\text{пор}}$ при $(1 - E_{\text{П}} E_{\text{опр}})_{\text{пор}} = E_{\text{СВ}}$, где $E_{\text{СВ}}$ – эффективность субъекта влияния. Такая найденная в исследовании формула угрозы обобщает различные версии этого термина.

Примеры численных значений риска и угроз для разных видов взаимодействия в таблице 2 показывают: скрытый ущерб влияний (риск) не превращается в явный (угроза) до того момента, когда $r_3 > r_{св}$.

Таблица 2

Численные значения риска и угроз

Table 2

Numerical values of a risk and threats

Взаимодействие	Порог	Риск	Угроза
Землетрясение	3 балла	Меньше 3 баллов	Больше (или равно) 3 баллов
Заболеваемость персонала	30 %	Меньше 30 %	Больше (или равно) 30 %
Эксплуатационная надежность оборудования	Предельное состояние	Эксплуатация до достижения предельного состояния	Эксплуатация после достижения предельного состояния
Заем кредита в банке	10 % численности заемщиков	Меньше 10 % численности заемщиков	Больше (или равно) 10 % численности заемщиков

Заключение

Рассмотренные примеры показывают, что, во-первых, безопасность предприятия достигается защитой каждой отдельной ресурсной составляющей на всех уровнях его структуры даже при нали-

чии во внешней среде негативных влияний, эффективность которых меньше эффективности защиты, а во-вторых, найденное определение угрозы можно распространить на влияние предприятия на себя.

Литература

1. Попов Н.С., Лузгачева Н.В., Чан Минь Тьинь. К методике конструирования экспертной системы оценки промышленной безопасности // Вестн. ТГТУ. 2013. Т. 19. № 1. С. 43–51.
2. Битюков В.К., Емельянов А.Е. Качественный анализ функционирования сетевой системы управления с конкурирующим методом доступа // Вестн. ТГТУ. 2012. Т. 18. № 1. С. 38–46.
3. Битюков В.К., Емельянов А.Е. Обобщенная математическая модель сетевой системы управления с конкурирующим методом доступа // Вестн. ТГТУ. 2012. Т. 18. № 2. С. 319–326.
4. Дякин В.Н. Динамическая модель управления развитием промышленного предприятия // Вестн. ТГТУ. 2013. Т. 19. № 2. С. 304–308.
5. Серов А.Ю., Сморгонский А.В. Действующая компьютерная модель производственного предприятия // Экономика и математические методы. 2009. Т. 45. № 3. С. 40–47.
6. Еремеев А.П. Прототип интеллектуальной системы поддержки принятия решений для управления энергообъектом // Программные продукты и системы. 2002. № 3. С. 38–42.
7. Колесников А.А. Синергетические методы управления сложными системами: теория системного синтеза. М.: Libroком, 2012. 240 с.
8. Литвак Б.Г. Разработка управленческого решения. М.: Дело, 2004. 392 с.
9. Медников В.И., Орехов С.А. Эффективное управление предприятием // Экономика и управление. 2007. № 2. С. 101–106.
10. Mednikov B.V., Mednikov V.I., Mednikov S.V. Commodity market math models // Экономика, статистика и информатика. Вестник УМО. 2015. № 2. С. 194–198.
11. Медников В.И. Квотирование запросов уровневого контроллера. Свид. об офиц. регистр. программы для ЭВМ № 2016619055.2016.

Software & Systems

DOI: 10.15827/0236-235X.118.307-313

Received 26.12.16

2017, vol. 30, no. 2, pp. 307–313

A SOFTWARE AND ALGORITHM COMPLEX OF ENTERPRISE PROTECTION AND MANAGEMENT

V.G. Matveykin¹, Dr.Sc. (Engineering), ProfessorB.S. Dmitrievsky¹, Dr.Sc. (Engineering), Associate ProfessorV.I. Mednikov¹, CandidateS.G. Semerzhinsky¹, Postgraduate Student, ipu@ahp.tstu.ru¹ Tambov State Technical University, Sovetskaya St. 106, Tambov, 392000, Russian Federation

Abstract. The paper presents an enterprise mathematical model interacting with external environment by resource exchange.

Current enterprise management, as well as real unauthorized influence on its activities by external environment or a subject is a result of the impact on resources. Unauthorized actions are detected by comparison of actual and calculated values of performance indicators for a selected level of functions execution. If such action is detected, a countermeasure system becomes active to reach the protected value.

The protection success rate is accepted as minimum performance requirements based on statistics and expert way. As a result, the authors have found a technical parameter of enterprise security that quantitatively describes protection inefficiency.

The built structure of enterprise protection and management system detects and locates unauthorized effect on its internal processes and the processes of interaction with the environment without human intervention. At the same time it organically combines enterprise management and protection and is significantly different from known systems. The protection and control system, which is implemented as software and algorithm complex, makes it possible to describe all production processes.

The paper proposes the means of improving reliability of measurement and obtaining information about resources state. They monitor and identify the external influences on each resource without human intervention. The paper describes the developed means of obtaining quantitative information on resource state and the terms of technical feasibility of the proposed enterprise protection and management system.

The proposed secure management algorithms use a resource protection system that provides reliable information at all management levels. The presented the protection and control system raise the enterprise efficiency in the interactions with the environment.

Keywords: enterprise model, protection structure, protection parameters, risk, productive resources, influence subject, unauthorized influence, protection success rate, resource security equation, threat.

References

1. Popov N.S., Luzgacheva N.V., Chan M.T. To methods of designing expert evaluation system of industrial safety. *Vestn. TGTU* [Trans. of the TSTU]. 2013, vol. 19, no. 1, pp. 43–51 (in Russ.).
2. Bituykov V.K., Emelyanov A.E. Qualitative Analysis of Network Control System with Competing Access Mode. *Vestn. TGTU* [Trans. of the TSTU]. 2012, vol. 18, no. 1, pp. 38–46 (in Russ.).
3. Bituykov V.K., Emelyanov A.E. Generalized Mathematical Model of Network Control System with Competing Access Mode. *Vestn. TGTU* [Trans. of the TSTU]. 2012, vol. 18, no. 2, pp. 319–326 (in Russ.).
4. Dyakin V.N. Dynamic Model of Management of Industrial Enterprise Development. *Vestn. TGTU* [Trans. of the TSTU]. 2013, vol. 19, no. 2, pp. 304–308 (in Russ.).
5. Serov A.Yu., Smorgonsky A.V. Acting computer model of the manufacturing enterprise. *Ekonomika i matematicheskie metody* [Economics and Mathematical Methods]. 2009, vol. 45, no. 3, pp. 40–47 (in Russ.).
6. Ereemeev A.P. The prototype of intellectual decision support system for the management of power facilities. *Programmnye produkty i sistemy* [Software & Systems]. 2002, no. 3, pp. 38–42 (in Russ.).
7. Kolesnikov A.A. *Sinergeticheskie metody upravleniya slozhnymi sistemami. Teoriya sistemnogo sinteza* [Synergetic Control Methods of Complex Systems. System Synthesis Theory]. Moscow, Librokom Publ., 2012, 240 p.
8. Litvak B.G. *Razrabotka upravlencheskogo resheniya* [Development of a Management Solution]. Moscow, Delo Publ., 2004, 392 p.
9. Mednikov V.I., Orekhov S.A. Effective enterprise management. *Ekonomika i upravlenie* [Economics and Management]. 2007, no. 2, pp. 101–106 (in Russ.).
10. Mednikov B.V., Mednikov V.I., Mednikov S.V. Commodity market math models. *Ekonomika, statistika i informatika. Vestnik UMO* [Economics, Statistics and Informatics. Bulletin of UMO]. 2015, no. 2, pp. 194–198 (in Russ.).
11. Mednikov V.I. *Kvitirovanie zaprosov urovnevnogo kontrollera* [Level Controller Challenge Handshake]. Official Registration Certificate of the Computer Program no. 2016612717. 2016.

Примеры библиографического описания статьи

1. Матвейкин В.Г., Дмитриевский Б.С., Медников В.И., Семержинский С.Г. Программно-алгоритмический комплекс защиты и управления предприятием // Программные продукты и системы. 2017. Т. 30. № 2. С. 307–313; DOI: 10.15827/0236-235X.118.307-313.
2. Matveykin V.G., Dmitrievsky B.S., Mednikov V.I., Semerzhinsky S.G. A software and algorithm complex of enterprise protection and management. *Programmnye produkty i sistemy* [Software & Systems]. 2017, vol. 30, no. 2, pp. 307–313 (in Russ.); DOI: 10.15827/0236-235X.118.307-313.