4 Реферати

УДК 004.621.3:519.816

ОЦІНКА ЯКОСТІ ФУНКЦІОНУВАННЯ КОМПЛЕКСНИХ СИСТЕМ ТЕХНІЧНОГО ЗАХИСТУ Й СИСТЕМ ПІДТРИМКИ УХВАЛЕННЯ РІШЕННЯ В ЇХНЬОМУ СКЛАДІ

Володимир Хорошко, Сергій Зибін*

Національний авіаційний університет, Державний Університет Інформаційно-Комунікаційних Технологій

Стаття: ***7 стор., 8 джерел.***

Створення складних систем, а також оцінка якості їх функціонування й працездатності передбачає розв'язання широкого кола різнопланових завдань. Причому інтенсивне застосування засобів обчислювальної техніки й автоматизації в них постійно коректує погляди на діяльність цих систем, до складу яких входять також і системи підтримки ухвалення рішення. Підвищення якості й скорочення часу прийняття рішень при керуванні складними системами різного призначення наразі неможливе без розробки ефективних програмних і апаратних засобів, що забезпечують діяльність обслуговуючого персоналу. Особливо гостро стоїть ця проблема при прийнятті рішень (ПР) у комплексних системах технічного захисту (КСТЗ), що працюють у реальному часі, де дефіцит часу відчувається особливо сильно, а наслідки при несвоєчасному або неправильному ухваленні рішення можуть бути катастрофічними. У зв'язку із цим і з'явилася необхідність у застосуванні систем підтримки прийняття рішень (СППР), основним завданням яких є надання допомоги фахівцям у процесі прийняття раціонального й оптимального рішення в складних ситуаціях, що виникають при функціонуванні КСТЗ у реальному часі. Причому оцінка якості вибору рішень і їх параметрів повинні здійснюватися на базі моделей, які дозволили б оцінювати застосування однієї й тієї ж системи в різних умовах експлуатації.

Підвищення ефективності математичного моделювання КСТЗ можна забезпечити за рахунок моделювання, як комплексної системи, так і підсистем, які входять до її складу. Ця необхідність стимулює розробку моделей і алгоритмів, що допускають вирішення складних завдань керування системою. Тому синтез КСТЗ і СППР для них, створених на основі засобів обчислювальної техніки, повинен здійснюватися відповідно до відомих критеріїв: мікропрограмне керування; модульність побудови; магістральний обмін інформацією; можливість нарощування обчислювальної потужності.

Розробка й дослідження математичних моделей КСТЗ і СППР вимагає значних часових витрат. Тому застосування мереж Петрі (МП) для таких цілей прискорює процес розв'язання цих задач. Метою роботи є розгляд можливості застосування МП для оцінки технічного стану КСТЗ і СППР, а також оцінка якості їх функціонування в різних умовах експлуатації.

За своїм призначенням, структурі й виконуваним функціям СППР є невід'ємною складовою частиною КСТЗ реального часу. Тому питання синтезу СППР слід розглядати з урахуванням взаємодії алгоритмів роботи СППР із алгоритмами функціонування КСТЗ. Для сучасних систем керування КСТЗ, що працюють у реальному часі, найбільш типовою є трирівнева структура обчислювальних засобів. На першому рівні знаходиться універсальна обчислювальна машина, що має великий об'єм пам'яті; на другому – спеціалізовані ЕОМ (міні- або мікро-ЕОМ); на третьому – персональні ЕОМ у складі АРМ або керуюча об'єктом машина.

Реалізація СППР у КСТЗ не змінює основних функцій обчислювальних засобів, пов'язаних з формуванням інформаційної моделі. Імітаційна модель дозволяє оцінити ефективність роботи системи й усувати конфліктні ситуації, тобто функціонування стає ситуаційним.

Для оцінки ефективності функціонування СППР у складі КСТЗ необхідно змоделювати процес її роботи. Його основні цілі – уточнення технічного рішення по вибору засобів обчислювальної техніки і розподіл функцій між ними, перевірка узгодженості функціонування технічних засобів СППР, оцінка ефективності роботи СППР і КСТЗ у цілому.

Таким чином, апарат МЧМП дозволяє будувати досить повні моделі функціонування алгоритмів, що відображають їхню структуру, логіку роботи й часові характеристики.

Для ефективного використання широкого спектра можливостей апаратних мереж Петрі (АМП) необхідне створення на базі АМП системи спеціального математичного забезпечення з набором засобів опису, вводу, трансляції, компонування, налагодження, імітації моделі, обробки результатів моделювання й аналізу.

Одним із способів досягнення компромісу між складністю й вірогідністю математичної моделі є спрощення еквівалентне об'єкту мережі, що проводиться за допомогою маршрутів функціонування системи на основі апарата нечітких відносин у просторі, обумовленому розширюваної базою ділених КСТЗ і СППР. Маршрутна модель із вірогідністю, що заздалегідь задається, дозволяє прогнозувати динаміку розвитку подій навколо КСТЗ із урахуванням СППР і їх стан.

Застосування мереж Петрі для імітаційного моделювання алгоритмів роботи СППР у складі КСЗТ полягає в тому, що кожній структурній схемі алгоритму ставиться у відповідність мережа Петрі. Рух міток у ній моделює процес обчислень, виконуваних алгоритмів. Запропонований метод дозволяє прогнозувати технічний стан і функціонування КСЗТ і СППР на підставі системних оцінок з великою точністю, що дозволяє забезпечити необхідний рівень захищеності.

ОЦЕНКА КАЧЕСТВА ФУНКЦИОНИРОВАНИЯ КОМПЛЕКСНЫХ СИСТЕМ ТЕХНИЧЕСКОЙ ЗАЩИТЫ И СИСТЕМ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЯ В ИХ СОСТАВЕ

Владимир Хорошко, Сергей Зыбин*

Национальный Авиационный Университет, Государственный Университет Информационно-Комуникационных Технологий

Создание сложных систем, а также оценка качества их функционирования и работоспособности предусматривает решение широкого круга разноплановых задач. Причем интенсивное применение средств вычислительной техники и автоматизации в них постоянно корректирует взгляды на деятельность этих систем, в состав которых входят и системы поддержки принятия решения. Повышение качества и сокращение времени принятия решений при управлении сложными системами различного назначения пока невозможно без разработки эффективных программных и аппаратных средств, обеспечивающих деятельность обслуживающего персонала. Особенно остро стоит эта проблема при принятии решений (ПР) в комплексных системах технической защиты (КСТЗ), работающих в реальном времени, где дефицит времени ощущается особенно сильно, а последствия при несвоевременном или неправильном принятии решения могут быть катастрофическими. В связи с этим и появилась необходимость в применении систем поддержки принятия решений (СППР), основной задачей которых является оказание помощи специалистам в процессе принятия рационального и оптимального решения в сложных ситуациях, возникающих при функционировании КСТЗ в реальном времени. Причем оценка качества выбора решений и их параметров должны осуществляться на базе моделей, которые позволили бы оценивать применение одной и той же системы в различных условиях эксплуатации.

Повышение эффективности математического моделирования КСТЗ можно обеспечить за счет моделирования, как комплексной системы, так и подсистем, входящих в ее состав. Эта необходимость стимулирует разработку моделей и алгоритмов, допускающих решения сложных задач управления системой. Поэтому синтез КСТЗ и СППР для них, созданных на основе средств вычислительной техники, должен осуществляться согласно известным критериям: микропрограммное управление; модульность построения; магистральный обмен информацией, возможность наращивания вычислительной мощности.

Разработка и исследование математических моделей КСТЗ и СППР требует значительных временных затрат. Поэтому применение сетей Петри (СП) для таких целей ускоряет процесс решения этих задач. Целью работы является рассмотрение возможности применения СП для оценки технического состояния КСТЗ и СППР, а также оценка качества их функционирования в различных условиях эксплуатации.

По своему назначению, структуре и выполняемым функциям СППР является неотъемлемой составной частью КСТЗ реального времени. Поэтому вопросы синтеза СППР следует рассматривать с учетом взаимодействия алгоритмов работы СППР с алгоритмами функционирования КСТЗ. Для современных систем управления КСТЗ, работающих в реальном времени, наиболее типичной является трехуровневая структура вычислительных средств. На первом уровне находится универсальная вычислительная машина, имеющая большой объем памяти, на втором - специализированные ЭВМ (мини-или микро-ЭВМ), на третьем - персональные ЭВМ в составе АРМ или управляющая объектом машина.

Реализация СППР в КСТЗ не меняет основных функций вычислительных средств, связанных с формированием информационной модели. Имитационная модель позволяет оценить эффективность работы системы и устранять конфликтные ситуации, т.е. функционирование становится ситуационным.

Для оценки эффективности функционирования СППР в составе КСТЗ необходимо смоделировать процесс ее работы. Его основные цели - уточнение технического решения по выбору средств

вычислительной техники и распределение функций между ними, проверка согласованности функционирования технических средств СППР, оценка эффективности работы СППР и КСТЗ в целом.

Таким образом, аппарат МЧМП позволяет строить достаточно полные модели функционирования алгоритмов, отражающих их структуру, логику работы и временные характеристики.

Для эффективного использования широкого спектра возможностей аппаратных СП (АСП) необходимо создание на базе АСП системы специального математического обеспечения с набором средств описания, ввода трансляции, компоновки, наладки, имитации модели, обработки результатов моделирования и анализа.

Одним из способов достижения компромисса между сложностью и вероятностью математической модели является эквивалентное объекту сети упрощение, которое производится с помощью маршрутов функционирования системы на основе аппарата нечетких отношений в пространстве, определяемом расширяемой базой деленных КСТЗ и СППР. Маршрутная модель с предварительно задаваемой вероятностью, позволяет прогнозировать динамику развития событий вокруг КСТЗ с учетом СППР и их состояние.

Применение СП для имитационного моделирования алгоритмов работы СППР в составе КСЗТ заключается в том, что каждой структурной схеме алгоритма ставится в соответствие СП. Движение меток в ней моделирует процесс вычислений, выполняемых алгоритмов. Предложенный метод позволяет прогнозировать техническое состояние и функционирование КСЗТ и СППР на основании системных оценок с большой точностью, что позволяет обеспечить необходимый уровень защищенности.

QUALITY EVALUATION OF OPERATION COMPLEX TECHNICAL SYSTEMS PROTECTION AND SUPPORT SYSTEMS DECISION IN THEIR COMPOSITION

Vladimir Khoroshko, Sergei Zybin*

National Aviation University, State University of Information and Communications Technology

Creating complex systems, and to assess the quality of their functioning and disability involves solving a wide range of diverse tasks. Moreover, the intensive use of computer technology and automation in them constantly corrects views on these systems, which include also the support system decision. Improving the quality and reducing the time of decision making in the management of complex systems for various purposes is currently impossible without the development of effective software and hardware that provide activities staff. Particularly acute is the problem when making decisions (MD) in complex systems technical protection (CSTP) working in real time, where the lack of time is felt particularly strongly, and consequences of untimely or incorrect decision making can be catastrophic. In this regard, and there is a need in the application of decision support systems (DSS), whose main task is to assist professionals in making rational and optimal solutions to complex situations that arise in the operation CSTP in real time. Moreover, the quality assessment of choice making and their parameters must be based on models that would assess the application of the same system in different conditions.

Improving mathematical modeling CSTP can be achieved through simulation of complex systems and subsystems that make up its membership. This agreement encourages the development of models and algorithms that allow solving complex management tasks system. Therefore synthesis CSTP and DSS for them, based on computer technology, must be carried out according to known criteria: firmware control, modular construction; trunk exchange of information, the ability to increase processing power.

Development and study of mathematical models CSTP and DSS requires significant time and resources. Therefore, the use of Petri nets (PN) for such purposes accelerates the resolution of these problems. The aim of the work is to examine the possibility of using IM to evaluate the technical condition CSTP and DSS, and assessing the quality of their operation in different operating conditions.

According to the purpose, structure and Duties DSS is an integral part KSTZ real time. Therefore, the question of synthesis DSS should be considered with regard to interaction with the DSS algorithms algorithms functioning CSTP. For modern control systems CSTP working in real time, the most typical is a three-tier structure of computational tools. On the first level there is a universal computer that has a large amount of memory in a second - specialized computers (mini-or micro-computers) on the third - personal computers in the ECM or control object machine.

Implementation of DSS in CSTP does not change the basic functions of computational tools associated with the formation of the information model. A simulation model to evaluate the effectiveness of the system and eliminate conflicts, ie, the operation becomes situational.

To evaluate the effectiveness of DSS in the CSTP to simulate the process of work. Its main goals - clarifying technical solution on the choice of computer technology and the distribution of functions between them, checking consistency of functioning hardware DSS, evaluation of DSS and CSTP in general.

Thus, the device allows you to build MCHMP fairly complete model of the algorithms that reflect their structure, logic and temporal characteristics.

For efficient use of a wide range of hardware capabilities of Petri nets (HPN) required the establishment of a special HPN system of software with a set of descriptions, input translation, layout, debugging, simulation models, process simulation results and analysis.

One way to achieve a compromise between complexity and reliability of the mathematical model is simplified equivalent network facilities, conducted by route of the system based on fuzzy relations in space, caused expandable base dividend CSTP and DSS. Route model of the probability that the advance is given, allows to predict the dynamics of the events surrounding CSTP taking into account the DSS and their condition.

The use of Petri nets for simulation algorithms in the DSS CSTP is that each block diagram of the algorithm is associated with Petri nets. Movement marks it simulates the process of calculations performed by algorithms. The proposed method allows to predict the technical condition and operation CSTP and DSS based on systematic evaluations with high accuracy, which ensures the necessary level of security.

УДК 004.621.3:681.327

РОЗРОБКА МЕХАНІЗМУ КОНТЕКСТНО-ОРІЄНТОВАНОГО ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Ігор Іванченко

Національний авіаційний університет

Стаття: ***8 стор., 5 джерел.***

Процес створення систем автоматизованого управління є складною науково-технічною проблемою і вимагає відповідного лінгвістичного, програмного та інформаційного забезпечення. Загальною частиною інформаційного забезпечення системи автоматизованого управління є автоматизовані інформаційні ресурси, до складу яких входять інформаційні ресурси та системи управління інформаційними ресурсами. Автоматизовані інформаційні ресурси створюються як обслуговуючі системи систем автоматизованого управління, де інформація зберігається у файлах, а тому користувач немає потреби вивчати деталі фізичного формату їх представлення. Таким чином, системи управління інформаційними ресурсами є не що інше, як спеціалізоване програмне забезпечення, за допомогою якого здійснюється взаємодія користувача з інформацією. Відповідно до цього захищена інформація розділяється на дві категорії: контекстно-залежну й контекстно-незалежну. Тому система обробки та контролю може не зберігати інформацію про попередні звернення до інформаційних ресурсів, оскільки для приймання рішення про можливість доступу до інформації достатньо перевірити зміст регістрів подій поля значень інформації. Подання вимог захисту контекстно-залежної інформації у вигляді орієнтованих графів дає можливість механізму контролю доступу до інформації виявляти порушення захисту.

Застосування алгоритму перетворення до граф-моделі контекстних залежностей в інформаційних ресурсах призводить до лісоподібних структур. Оскільки у початковій структурі граф-моделі відсутні контури, процес її ізоморфних перетворень відбувається без ускладнень і завершується за один етап. Ці структури характерні тим, що взаємозв'язки між елементами, які розміщені на різних рівнях структури, є ієрархічними, але тип загального взаємозв'язку між ними являє собою мережу. Слід зауважити, що в даному випадку ієрархічні взаємозв'язки є частковим випадком взаємозв'язків мережевого типу. Лісоподібні структури з закріпленими коренями та з закріпленим листям мають однакову кількість рівнів ієрархії, але склад числа елементів інформації, розміщеної на однакових рівнях, відрізняється між собою. У випадку необхідності застосування процедур деконтуризації, залежно від числа та типу видалених дуг, можна одержати лісоподібні структури з різним числом рівнів ієрархії. Вказані особливості ізоморфних перетворень граф-моделей контекстних залежностей між елементами інформації необхідно брати до уваги в процесі розробки механізму контекстно-орієнтованого захисту.

Відповідно до цього було сформульовано деякі положення щодо можливостей представлення граф-моделей контекстних залежностей у вигляді лісоподібних ієрархічних структур та розподілу елементів інформації по рівнях ієрархії. Таким чином, запропонована методика дає можливість автоматизувати процес розробки графа контекстних залежностей між елементами даних інформаційних ресурсів, виявлення можливих помилок у початковому формуванні цих залежностей та їх коригування, а також процес

ізоморфних перетворень структур інформаційних ресурсів із механізмом контекстно-орієнтованого захисту інформації як основу для модифікації запитів, залежно від напрямку та змісту попередніх звертань у процесі його функціонування.

РАЗРАБОТКА МЕХАНИЗМА КОНТЕКСТНО-ОРИЕНТИРОВАННОЙ ЗАЩИТЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ

Игорь Иванченко
Национальный авиационный университет

Процесс создания систем автоматизированного управления является сложной научно-технической проблемой и требует соответствующего лингвистического, программного и информационного обеспечения. Общей частью информационного обеспечения системы автоматизированного управления являются автоматизированные информационные ресурсы, в состав которых входят информационные ресурсы и системы управления информационными ресурсами. Автоматизированные информационные ресурсы создаются как обслуживающие системы систем автоматизированного управления, где информация хранится в файлах, а поэтому пользователю нет необходимости изучать детали физического формата их представления. Таким образом, системы управления информационными ресурсами есть не что иное, как специализированное программное обеспечение, с помощью которого осуществляется взаимодействие пользователя с информацией. Согласно этому защищенная информация разделяется на две категории: контекстно-зависимую и контекстно-независимую. Поэтому система обработки и контроля может не хранить информацию о предыдущих обращениях к информационным ресурсам, поскольку для принятия решения о возможности доступа к информации достаточно проверить содержание регистров событий поля значений информации. Представление требований защиты контекстно-зависимой информации в виде ориентированных графов позволяет механизму контроля доступа к информации выявить нарушения защиты.

Применение алгоритма преобразования к граф-модели контекстных зависимостей в информационных ресурсах приводит к лесоподобным структурам. Поскольку в исходной структуре граф-модели отсутствуют контуры, процесс ее изоморфных преобразований происходит без осложнений и заканчивается за один этап. Эти структуры характерны тем, что взаимосвязи между элементами, которые размещены на разных уровнях структуры, являются иерархическими, но тип общей взаимосвязи между ними представляет собой сеть. Следует заметить, что в данном случае иерархические взаимосвязи являются частным случаем взаимосвязей сетевого типа. Лесоподобные структуры с закрепленными корнями и с закрепленными листьями имеют одинаковое количество уровней иерархии, но состав числа элементов информации, размещенной на одинаковых уровнях, отличается между собой. В случае необходимости применения процедур деконтуризации в зависимости от числа и типа удаленных дуг можно получить лесоподобные структуры с различным числом уровней иерархии. Указанные особенности изоморфных преобразований граф-моделей контекстных зависимостей между элементами информации необходимо учитывать в процессе разработки механизма контекстно-ориентированной защиты.

Согласно этому были сформулированы некоторые положения относительно возможностей представления граф-моделей контекстных зависимостей в виде лесоподобных иерархических структур и распределения элементов информации по уровням иерархии. Таким образом, предложенная методика позволяет автоматизировать процесс разработки графа контекстных зависимостей между элементами данных информационных ресурсов, обнаружения возможных ошибок в первоначальном формировании этих зависимостей и их корректировку, а также изоморфные преобразования структур информационных ресурсов с механизмом контекстно-ориентированной защиты информации в качестве основы для модификации запросов в зависимости от направления и содержания предыдущих обращений в процессе его функционирования.

DEVELOPING MECHANISM FOR CONTEXT-BASED INFORMATION RESOURCES PROTECTION

Igor Ivanchenko
National Aviation University

The process of creation of automated control systems is a complex scientific and technical challenge and will require a linguistic, software and information. Common part of the information management system of automated controls are automated information resources, which include information resources and information management systems. Automated information resources are created as servicing systems of automated control systems, where the information is stored in files, so the user does not need to study the details of the physical format of presentation.The content management system is nothing more than a special software through which the user interacts with information. According to that protected information is divided into two categories: context-sensitive and context-independent. Before the system processing and control cannot store information about previous calls to the information resources, since the decision on access to information sufficient to verify the contents of the event register value field information. Representation of the protection requirements of context-sensitive information in the form of directed graphs allows the access control mechanism to identify information security breaches.

Algorithm to transform a graph model of context dependency in information resources leads to structure similarity woods structures. Since the initial structure of the graph model has no contours, the process of transformation is isomorphic with no complications and ends with a single step. These structures are characterized by the fact that the relationship between the elements, which are placed at different levels of the structure, are hierarchical, but the type of the overall relationship between the two is a network. Note that in this case the hierarchical relationships are special case of the relationship of network type. The structure similarity woods structure with fixed roots and leaves have the same fixed number of levels in the hierarchy, but the composition of the pieces of information placed on the same level, different among themselves. If necessary, use separation procedures, depending on the number and type of remote arcs can be structure similarity woods structures with different numbers of levels in the hierarchy. These features of the isomorphic graph transformation model of contextual relationships between pieces of information should be considered in the development of context-oriented mechanism of protection.

According to that formulated some provisions for possible submission to the graph models in the form of context-sensitive structure similarity woods hierarchical structures and the distribution of items of information on the levels of the hierarchy. That why the proposed methodology automates the process of developing a graph of contextual relationships between data elements of information resources, to detect possible errors in the initial formation of these functions and their adjustment, and isomorphic transformation of structures of information resources with the mechanism of context-oriented information security as a basis for modifying queries , depending on the direction and content of previous calls during its functioning.

УДК 004.681.003

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОБ'ЄКТА

Юлія Хохлачова
Національний Авіаційний Університет

Стаття: ***6 стор., 3 джерела.***

Метою розробки офіційної політики інформаційної безпеки (ПІБ) конкретного об’єкта в області інформаційної безпеки є визначення правильного способу використання обчислювальних і комунікаційних ресурсів, а також розробка процедур, що запобігають чи реагують на порушення режиму безпеки. Для досягнення цієї мети варто відштовхуватися від стандартних канонів розробки ПІБ, але й, звичайно ж, враховувати специфіку конкретного об’єкта. Один з головних спонукальних мотивів розробки ПІБ об’єкта полягає в одержанні впевненості, що діяльність з захисту інформації побудована економічно і технічно виправданим способом. Політика звичайно складається з двох частин: загальних принципів і конкретних правил роботи. Інформаційну систему об’єкта захисту можна вважати захищеною, якщо всі операції виконуються згідно зі строго визначеними правилами, що забезпечують безпосередній захист об’єктів, ресурсів і операцій.

Основу для формування вимог до захисту складає список загроз. Коли такі вимоги відомі, можуть бути визначені відповідні правила забезпечення захисту, що визначають необхідні функції і засоби захисту. Чим

суворіші вимоги до захисту і більше відповідних правил, тим ефективніші її механізми і тим більше захищеною виявляється інформаційна система.

Захист інформації на інформаційному об'єкті буде ефективним, коли проектування та реалізація системи захисту інформаційного об'єкта відбувається згідно з етапами: аналіз ризиків; реалізація політики безпеки; підтримка політики безпеки.

Організаційна ПІБ описує порядок надання і використання прав доступу користувачів, а також вимоги звітності користувачів за свої дії в питаннях безпеки.

Для інформаційних мереж можна виділити випадкові та навмисно створювані ймовірні загрози, які необхідно враховувати при визначенні ПІБ.

На підставі вище зазначеного розроблено зразковий алгоритм роботи з оцінки інформаційних ризиків.

Реалізація ПІБ об'єкта починається з проведення розрахунку фінансових втрат і вибору відповідних засобів для виконання цих задач. При цьому необхідно врахувати такі фактори як безконфліктність роботи обраних засобів, репутація постачальників засобів захисту, можливість одержання повної інформації про механізми захисту і надані гарантії.

При підтримці ПІБ потрібно постійне спостереження за вторгненнями зловмисників, виявлення вад і "дір" у системі захисту об'єкта інформації, облік випадків несанкціонованого доступу до конфіденційних даних. При цьому основна відповідальність за підтримку ПІБ мережі (об'єкта інформації) лежить на системному адміністраторі.

Необхідно заздалегідь визначити характер дій, що починаються у випадку виявлення порушень ПІБ. Щоб ці дії були швидкими й правильними варто організувати розслідування. Після цього потрібно внести корективи в систему захисту. Тип і серйозність коректив залежить від типу порушення, яке сталося.

Таким чином, послідовність відповідних дій залежить не тільки від типу порушення, але й від виду порушника; вона повинна бути продумана задовго до першого інциденту.

Кожний об'єкт повинен заздалегідь визначити набір адміністративних санкцій, застосованих до місцевих користувачів, які порушують ПІБ сторонньої організації чи об'єкта. Крім того, необхідно подбати про захист від відповідних дій сторонньої організації. При розробці ПІБ варто враховувати всі юридичні положення, які застосовуються до подібних ситуацій.

Політика безпеки об'єкта повинна мати процедури для взаємодії з зовнішніми організаціями, у число яких входять правоохоронні органи, інші організації, команди "швидкого реагування", засобів масової інформації. У процедурах повинно бути визначено, хто має право на такі контакти, і як саме вони відбуваються. Крім політичних положень, необхідно продумати й описати процедури, що виконуються у випадку виявлення порушень режиму безпеки. Для всіх видів порушень мають бути заготовлені відповідні процедури.

ПІБ об'єкта має доповнюватися і змінюватися згідно з усіма перерахованими критеріями змін і цінності інформації, що підлягає захисту.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТА

Юлия Хохлачова

Национальный Авиационный Университет

Целью разработки официальной политики информационной безопасности (ПИБ) конкретного объекта в области информационной безопасности является определение правильного способа использования вычислительных и коммуникационных ресурсов, а также разработка процедур, которые предотвращают или реагируют на нарушения режима безопасности. Для достижения этой цели следует отталкиваться от стандартных канонов разработки ПИБ, но и, конечно же, учитывать специфику конкретного объекта. Один из главных побудительных мотивов разработки ПИБ объекта заключается в получении уверенности, что деятельность по защите информации построена экономически и технически оправданным способом. Политика обычно состоит из двух частей: общих принципов и конкретных правил работы. Информационную систему объекта защиты можно считать защищенной, если все операции выполняются согласно строго определенным правилам, обеспечивающим непосредственную защиту объектов, ресурсов и операций.

Основу для формирования требований к защите составляет список угроз. Когда такие требования известны, могут быть выделены соответствующие правила обеспечения защиты, определяющие необходимые функции и средства защиты. Чем строже требования к защите и больше соответствующих правил, тем эффективнее ее механизмы и тем более защищенной оказывается информационная система.

Защита информации на информационном объекте будет эффективным, когда проектирование и реализация системы защиты информационного объекта происходит согласно этапам: анализ рисков; реализация политики безопасности, поддержка политики безопасности.

Организационная ПИБ описывает порядок предоставления и использования прав доступа пользователей, а также требования отчетности пользователей за свои действия в вопросах безопасности.

Для информационных сетей можно выделить случайные и намеренно создаваемые вероятные угрозы, которые необходимо учитывать при определении ПИБ.

На основании выше указанного разработан примерный алгоритм работы по оценке информационных рисков.

Реализация ПИБ объекта начинается с проведения расчета финансовых потерь и выбора соответствующих средств для выполнения этих задач. При этом необходимо учесть такие факторы как бесконфликтность работы выбранных средств, репутация поставщиков средств защиты, возможность получения полной информации о механизмах защиты и предоставленные гарантии.

При поддержке ПИБ требуется постоянное наблюдение за вторжениями злоумышленников, выявления недостатков и "дыр" в системе защиты объекта информации, учет случаев несанкционированного доступа к конфиденциальным данным. При этом основная ответственность за поддержание ПИБ сети (объекта информации) лежит на системном администраторе.

Необходимо заранее определить характер действий, которые начинаются в случае выявления нарушений ПИБ. Чтобы эти действия были быстрыми и правильными следует организовать расследование. После этого нужно внести коррективы в систему защиты. Тип и серьезность корректив зависит от типа нарушения, которое произошло.

Таким образом, последовательность соответствующих действий зависит не только от типа нарушения, но и от вида нарушителя, она должна быть продумана задолго до первого инцидента.

Каждый объект должен заранее определить набор административных санкций, примененных к местным пользователям, нарушающим ПИБ посторонней организации или объекта. Кроме того, необходимо позаботиться о защите от ответных действий посторонней организации. При разработке ПИБ следует учитывать все юридические положения, применимые к подобным ситуациям.

Политика безопасности объекта должна иметь процедуры для взаимодействия с внешними организациями, в число которых входят правоохранительные органы, другие организации, команды "быстрого реагирования", средства массовой информации. В процедурах должно быть определено, кто имеет право на такие контакты, и как именно они происходят. Кроме политических положений, необходимо продумать и описать процедуры, выполняемые в случае выявления нарушений режима безопасности. Для всех видов нарушений должны быть заготовлены соответствующие процедуры.

ПИБ объекта должна дополняться и изменяться согласно со всеми перечисленными критериями изменений и ценности информации, подлежащей защите.

INFORMATION SECURITY POLICY OBJECT

Julia Hohlachova
National Aviation University

The aim of developing an official information security policy (ISP) of a particular object in the field of information security is to determine the proper way to use computing and communication resources, and to develop procedures to prevent or respond to violations of safety. To achieve this goal, we should start from the standard canons development ISP, but, of course, be specific to a particular item. One of the main motivations Development ISP object is to obtain assurance that the activities of protection built economically and technically sound manner. Politics usually consists of two parts: general principles and specific rules of work. Information system security object can be considered secure if all operations are performed in accordance with strictly defined rules to ensure immediate protection of facilities, resources and operations.

The basis for the formation protection requirements is a list of threats. When these requirements are known, can be identified by appropriate rules to protect that define the functionality and protection. The more stringent requirements to protect the more relevant rules, the more effective its mechanisms and the more secure is information system.

Data Security information objects will be effective when the design and implementation of an information security system is an object according to stages: risk analysis, implementation of security policies, support for security policy.

Organizational ISP describes the procedure for granting and use of user access and user reporting requirements for their actions in matters of security.

For information networks are the random and deliberately created a credible threat that must be considered when determining the ISP.

Based on the above-mentioned exemplary algorithm developed to assess the risk of information.

Implementing Object ISP begins with calculation of financial losses and the selection of appropriate tools to perform these tasks. It is necessary to take into account such factors as the absence of conflict of selected products, suppliers reputation protection, the possibility of obtaining information about safeguards and guarantees provided.

With the support of ISP need constant monitoring incursions intruders, detect flaws and "holes" in the system of protection of object information record cases of unauthorized access to sensitive data. Thus the primary responsibility for maintaining the network ISP (facility information) on the system administrator.

Necessary to determine the nature of activities that begin in case of violations ISP. For these actions were swift and accurate should organize an investigation. Then you have to make adjustments to the system of protection. The type and severity of adjustment depends on the type of violation that happened.

Thus, the sequence of the response depends not only on the type of violation, but also on the type of offender, it should be thought out well before the first incident.

Each object must predefine set of administrative sanctions applied to local users who violate third party's ISP or object. In addition, care must be taken appropriate action to protect third party. In developing the ISP should consider all the legal provisions applicable to such situations.

Policy object must have procedures for interacting with external organizations, which include law enforcement agencies, other organizations, teams "quick response" media. In proceedings must be determined who is entitled to such contacts, and how they occur. Apart from the political provisions necessary to consider and describe the procedures to be performed in case of violations of security. For all types of violations should be harvested procedures.

ISP of the object must be complemented and are in compliance with all criteria listed changes and value of the information to be protected.

УДК: 343.9.02.005.334 (477)

ОЦІНЮВАННЯ РИЗИКІВ ТА ЗАГРОЗ ЗЛОЧИННОСТІ У ЗАБЕЗПЕЧЕННІ КРИМІНОЛОГІЧНОЇ БЕЗПЕКИ

Дарія Прокоф'єва-Янчиленко
Служба безпеки України

Стаття: ***5 стор., 9 джерел.***

Набуття злочинністю в сучасному світі статусу однієї з найбільш істотних загроз національній безпеці на загальнодержавному та міжнародному рівні вимагає нових підходів у дослідженні злочинності та її конкретизованих проявів, а також нових стратегій протидії зазначеним негативним явищам. Враховуючи, що суспільство фактично існує в умовах ризику злочинності, видається перспективним застосування до оцінки та прогнозування динаміки злочинності методології ризик-менеджменту та превентивного управління системою кримінологічної безпеки.

Оскільки у сфері кримінологічної безпеки наслідки настання певної події (реалізації кримінальної загрози) розглядаються з негативної точки зору, управління ризиками в даному випадку має приділяти основну увагу превентивним заходам або заходам, що зменшують розміри негативних наслідків. Основою для відповідних заходів (як і заходів щодо забезпечення кримінологічної безпеки в цілому) слугує оцінювання ризиків та загроз злочинності як процес збору та аналізу інформації про: характер і масштаби загроз кримінологічній безпеці; слабкі сторони систем і засобів забезпечення кримінологічної безпеки, а також інших особливостей юрисдикції, які роблять її привабливою для осіб, втягнених у злочинну діяльність (насамперед у її організованих формах). Метою оцінювання ризиків кримінологічної безпеки є виявлення методів злочинної діяльності (насамперед у її організованих формах) у межах юрисдикції, визначення частоти використання цих методів, їх ефективності й пошуку «слабких місць» у системах і засобах здійснення злочинної діяльності. Оцінювання ризиків та загроз злочинності реалізується в рамках системи управління ризиком, яка базується на комплексному процесному підході. До складу процесів системи входять: ідентифікація ризику; аналіз ризику; визначення ступеня (оцінювання) ризику; обробка ризику; комунікація ризику; постійне поліпшення системи оцінювання ризиків.

Система управління ризиками злочинності має бути впроваджена в усі правоохоронні практики, адже процеси управління ризиками мають стати частиною процесів забезпечення кримінологічної безпеки й національної безпеки України в цілому. Зокрема, ризик-менеджмент має бути впроваджений у політику розвитку, оцінку стратегічного планування протидії злочинності, а також у процеси управління соціальними змінами. На перший план при цьому виходить проблема інформаційної причинності, адже пізнання та використання в науках кримінального циклу та правоохоронній практиці закономірностей існування інформаційних взаємозв'язків відкриває нові перспективи в досягненні їх основної спільної мети – забезпечення кримінологічної безпеки, а також привносить нові ідеї щодо співвідношення загальної детермінації та свободи волі при вчиненні злочину, розуміння причин та умов злочинності, причинно-наслідкового зв'язку в механізмі злочину, так званого «елементу вірогідності», відображення механізму злочину, прогностичних можливостей правоохоронних органів тощо.

УДК: 343.9.02.005.334 (477)

ОЦЕНКА РИСКОВ И УГРОЗ ПРЕСТУПНОСТИ В ОБЕСПЕЧЕНИИ КРИМИНОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ

Дария Прокофьева-Янчиленко
Служба безопасности Украины

Получение преступностью в современном мире статуса одной из наиболее существенных угроз национальной безопасности на общегосударственном и международном уровне требует новых подходов в исследовании преступности и ее конкретизированных проявлений, а также новых стратегий противодействия указанным негативным явлениям. Учитывая, что общество фактически существует в условиях риска преступности, представляется перспективным применение к оценке и прогнозированию динамики преступности методологии риск-менеджмента и превентивного управления системой криминологической безопасности.

Поскольку в сфере криминологической безопасности последствия наступления определенного события (реализации криминальной угрозы) рассматриваются с негативной точки зрения, управление рисками в данном случае должно уделять основное внимание превентивным мерам или мероприятиям, уменьшающие размеры негативных последствий. Основой для соответствующих мероприятий (как и мер по обеспечению криминологической безопасности в целом) служит оценка рисков и угроз преступности как процесс сбора и анализа информации, при котором исследуются: характер и масштабы угроз криминологической безопасности; слабые стороны систем и средств обеспечения криминологической безопасности, а также других особенностей юрисдикции, которые делают ее привлекательной для лиц, вовлеченных в преступную деятельность (прежде всего в ее организованных формах). Целью оценки рисков криминологической безопасности является выявление методов преступной деятельности (прежде всего в ее организованных формах) в пределах юрисдикции, определение частоты использования этих методов, их эффективности и поиска «слабых мест» в системах и средствах осуществления преступной деятельности. Оценка рисков и угроз преступности реализуется в рамках системы управления риском, которая базируется на комплексном процессном подходе. В состав процессов системы входят: идентификация риска, анализ риска, определение степени (оценки) риска; обработка риска; коммуникация риска; постоянное улучшение системы оценки рисков.

Система управления рисками преступности должна быть внедрена во все правоохранительные практики, а процессы управления рисками должны стать частью процессов обеспечения криминологической безопасности и национальной безопасности Украины в целом. В частности, риск-менеджмент должен быть внедрен в политику развития, оценку стратегического планирования противодействия преступности, а также в процессы управления социальными изменениями. На первый план при этом выходит проблема информационной причинности, поскольку познание и использование в науках криминального цикла и правоохранительной практике закономерностей существования информационных взаимосвязей открывает новые перспективы в достижении их основной общей цели–обеспечения криминологической безопасности, а также привносит новые идеи относительно соотношения общей детерминации и свободы воли при совершении преступления, понимания причин и условий преступности, причинно-следственной связи в механизме преступления, так называемого «элемента вероятности», отражения механизма преступления, прогностических возможностей правоохранительных органов и т. д.

EVELUATION OF RISK AND CRIME THREAT IN CRIMINOLOGICAL SECURITY GUARANTEE

Daria Prokof'eva-Yanchilenko
Service safety of Ukraine

In the modern world the status of one of the most significant threats to national security at the national and international level was given to the criminality and it requires new approaches in the study of crime and its manifestations concretized, and new strategies to counter these negative phenomena. Consider that society actually exist at risk of crime, a promising application to the estimation and prediction of the dynamics of crime methodology of risk management and control system of preventive security criminology.As in the field of criminological security implications a certain event (realization criminal threat) are considered from a negative point of view, risk management in this case should focus on preventive measures or measures that reduce the size of negative consequences. The basis for the relevant activities (as well as measures to ensure the safety of criminology in general) is the assessment of the risks and threats of crime as a process of information gathering and analysis, which examines: the nature and extent of threats criminological security weaknesses of the systems and means of criminological security and other features of the jurisdiction that make it attractive to people involved in criminal activity (especially in its organized forms). The purpose of risk assessment is to identify security criminological methods of criminal activity (especially in its organized forms) within the jurisdiction to determine the frequency of use of these methods, their effectiveness and search for "weak spots" in the systems and means of criminal activity. Assessment of risks and threats of crime is realized in the framework of risk management, which is based on an integrated process approach. The structure of system processes include: risk identification, risk analysis, determination of (estimated) risk, risk treatment, risk communication and continual improvement of the system of risk assessment.The risk management system of crime should be embedded in all law enforcement practices, and risk management processes should be part of the processes to ensure safety and criminological Ukraine's national security in general. In particular, risk management should be incorporated into policy development, evaluation of strategic planning to crime, as well as in the management of social change. At the forefront of the yield of the problem of information causality, because the knowledge and use of science in criminal cycle and law practice patterns of existence interconnectivity opens new prospects to achieve their main common goal-ensuring criminological security, and brings new ideas on ratio of total determination and freedom of will during the commitment of the crime, understanding the causes and conditions of crime causation in the mechanism of the crime, the so-called "element of probability", reflections crime mechanism, predictive capability of law enforcement agencies, etc.

УДК 343.96+343.326+343.341

ПЕРСПЕКТИВИ НОРМАТИВНО-ПРАВОВОГО ВРЕГУЛЮВАННЯ ЗНЯТТЯ ІНФОРМАЦІЇ З ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ ТА ЕЛЕКТРОННИХ ІНФОРМАЦІЙНИХ СИСТЕМ У НОВОМУ КПК УКРАЇНИ

Дмитро Мельник
Служба безпеки України

Стаття: ***6 стор., 8 джерел.***

В Україні сьогодні на законодавчому рівні не передбачено прозорого порядку створення та впровадження систем перехоплення телекомунікацій, не визначено організаційно-технічних вимог, які повинні забезпечувати контроль перехоплення телекомунікацій, не зважаючи на актуальність правового забезпечення проведення пошукових та оперативно-технічних заходів на каналах зв'язку правоохоронними органами в умовах стрімкого розвитку інформаційного середовища. Спробу законодавчого врегулювання проведення оперативно-технічних заходів в мережах телекомунікацій та електронних інформаційних системах зроблено у новому КПК України від 13. 04. 2012 р., яким передбачено зняття інформації з транспортних телекомунікаційних мереж та електронних інформаційних систем. Однак при цьому норми вітчизняного законодавства потребують приведення у відповідність до положень Конвенції про кіберзлочинність; необхідним є створення умов, які б покращували можливості уповноважених органів у сфері протидії комп'ютерній злочинності. Ефективній реалізації положень КПК України щодо зняття інформації з

транспортних телекомунікаційних мереж та електронних інформаційних систем сприятиме прийняття Закону України «Про перехоплення телекомунікацій», внесення необхідних змін до законів України «Про телекомунікації», «Про оперативно-розшукову діяльність», «Про контррозвідувальну діяльність».

ПЕРСПЕКТИВЫ НОРМАТИВНО-ПРАВОВОГО РЕГУЛИРОВАНИЯ СНЯТИЯ ИНФОРМАЦИИ С ТЕЛЕКОМУНИКАЦИОННЫХ СЕТЕЙ И ЭЛЕКТРОННЫХ ИНФОРМАЦИОНЫХ СИСТЕМ В НОВОМ КПК УКРАИНЫ

Дмитрий Мельник
Служба безопасности Украины

В Украине сегодня на законодательном уровне не предусмотрен прозрачный порядок создания и внедрения систем перехвата телекоммуникаций, не определены организационно-технические требования, которые должны обеспечивать контроль перехвата телекоммуникаций, не смотря на актуальность правового обеспечения проведения поисковых и оперативно-технических мероприятий на каналах связи правоохранительными органами в условиях стремительного развития информационной среды. Попытка законодательного урегулирования проведения оперативно-технических мероприятий в сетях телекоммуникаций и электронных информационных системах осуществлена в новом КПК Украины от 13. 04. 2012 г., которым предусмотрено снятие информации из транспортных телекоммуникационных сетей и электронных информационных систем. Однако при этом нормы отечественного законодательства нуждаются в приведении в соответствие с положением Конвенции о кибер-преступности; необходимым есть создание условий, которые бы улучшали возможности уполномоченных органов в сфере противодействия компьютерной преступности. Эффективной реализации положений КПК Украины о снятии информации с транспортных телекоммуникационных сетей и електронных информационных систем будет содействовать принятие Закона Украины «О перехвате телекоммуникаций», внесение изменений в законы Украины «О телекоммуникациях», «Об оперативно-розыскной деятельности», «О контрразве-дывательной деятельности».

PERSPECTIVES OF LAW REGULATION REMOVALS OF THE INFORMATION FROM TRANSPORT TELECOMMUNICATION NETWORKS AND ELECTRONIC INFORMATION SYSTEMS

Dmitro Melnik
Service safety of Ukraine

In Ukraine today at legislative level the transparent order of creation and introduction of interception systems on the telecommunications is not provided, are not defined organizational-technical requirements which should provide the control of interception of telecommunications, without reckoning with an urgency of legal maintenance of carrying out of search and operating-technical actions on communication channels for law enforcement bodies in conditions steep of development of the information environment. Attempt of legislative settlement of carrying out of operating-technical actions in networks of telecommunications and electronic information systems it is made in the new Criminal remedial code (CRC) of Ukraine from 13. 04. 2012 by which it is provided removals of the information from transport telecommunication networks and electronic information systems. However thus norms of the domestic legislation require reduction in conformity to positions of Cybercrime convention, necessary there are creations of conditions which would improve possibilities of the authorised bodies in sphere of counteraction of computer criminality. Effective realisation of positions of a CRC of Ukraine concerning information removal from transport telecommunication networks and electronic information systems will be assisted by adoption of law "About interception of telecommunications", changes into the laws "About telecommunication", "About operatively-search activity", "About counterintelligence activity".

УДК 004.056.5; 338.516.2

МОДЕЛЬ ЦІНОУТВОРЮЮЧИХ ЧИННИКІВ НАДАННЯ ПОСЛУГ У СФЕРІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Володимир Кононович, Юрій Копитін*, Марина Копитіна

*Одеська національна академія зв'язку ім. О.С. Попова, *КП «Обласний інформаційно-аналітичний центр» Одеської обласної ради*

Стаття: ***9 стор., 17 джерел, 2 рис.***

В роботі зазначається, що з підвищенням значущості і цінності інформаційно-комунікаційних технологій зростає важливість надання якісно нових послуг у сфері забезпечення інформаційної безпеки (СЗІБ). Ринок постачальників послуг у СЗІБ складають вітчизняні постачальники послуг та філії міжнародних компаній. Однак, ціна та якість однакових послуг може досить суттєво відрізнятися.

Пропонується наступна класифікація послуг у СЗІБ: виробництво пристроїв, розробка критеріїв ІБ, впровадження механізмів ІБ, додаткові та спеціалізовані послуги.

Відображено основні чинники, що впливають на процес ціноутворення надання послуг у СЗІБ у вигляді моделі. Перший рівень моделі складають фундаментальні чинники ціноутворення на послуги у СЗІБ, другий рівень – самі послуги у СЗІБ, третій рівень – критерії формування цін на певну послугу.

Проведений аналіз ціноутворюючих чинників процесу надання послуг у СЗІБ свідчить про недостатній розвиток нормативно-правової бази, відсутність критеріїв оцінки якості послуг, недостатній стимулюючий вплив регуляторів і, як наслідок, низьку конкурентоспроможність вітчизняних постачальників послуг. Побудована модель – це лише один із кроків вирішення проблем, пов'язаних з наданням послуг у СЗІБ, та в подальшому може бути відправною точкою для розрахунку собівартості надання послуг.

МОДЕЛЬ ЦЕНООБРАЗУЮЩИХ ФАКТОРОВ ПРЕДОСТАВЛЕНИЯ УСЛУГ В СФЕРЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Владимир Кононович, Юрий Копытин*, Марина Копытина

*Одесская национальная академия связи им. А.С. Попова, *КП «Областной информационно-аналитический центр» Одесского областного совета*

В работе отмечается, что с повышением значимости и ценности информационно-коммуникационных технологий возрастает важность предоставления качественно новых услуг в сфере обеспечения информационной безопасности (СОИБ). Рынок поставщиков услуг в СОИБ составляют отечественные поставщики и филиалы международных компаний. Однако, цена и качество одинаковых услуг может довольно существенно отличаться.

Предлагается следующая классификация услуг в СОИБ: производство устройств, разработка критериев ИБ, внедрение механизмов ИБ, дополнительные и специализированные услуги.

Отражены основные факторы, влияющие на процесс ценообразования предоставления услуг в СОИБ в виде модели. Первый уровень модели составляют фундаментальные факторы ценообразования на услуги в СОИБ, второй уровень – сами услуги в СОИБ, третий уровень – критерии формирования цен на определенную услугу.

Проведенный анализ ценообразующих факторов процесса предоставления услуг в СОИБ свидетельствует о недостаточном развитии нормативно-правовой базы, отсутствии критериев оценки качества услуг, недостаточном стимулирующем влиянии регуляторов и, как следствие, низкой конкурентоспособности отечественных поставщиков услуг. Построенная модель – это лишь один из шагов решения проблем, связанных с предоставлением услуг в СОИБ, и в дальнейшем может быть отправной точкой для расчета себестоимости предоставления услуг.

MODEL OF PRICING FACTORS PROVIDE SERVICES IN THE SECTOR OF INFORMATION SECURITY

Volodymyr Kononovich, Yurii Kopytin*, Maryna Kopytina
*Odessa National Academy of communications named after A.S. Popov, *«Regional information-analytical center» Odessa Regional Council*

The paper states that with increasing importance and value of ICT relatively increases the importance providing of high quality new services in the sector of information security (SIS). Market providers of services in SIS constitute local service providers and affiliates of international companies. However, the price and quality of similar services may vary quite significantly.

The classification of services SIS is proposed following: production of devices, development criteria of information security, implementation of information security mechanisms, additional and specialized services.

A model of the main factors that affect the pricing of services SIS is displayed. The first level of the model are fundamental factors in the pricing of services in SIS, the second level – the services in SIS, third level – criteria pricing for certain services.

The analysis of the pricing factors of process providing services in SIS is conducted and demonstrated an insufficient development of the legal framework, the lack of criteria for assessing the quality of services, insufficient stimulating effect of regulators and, consequently, low competitiveness of domestic service providers. The model is only one of the steps of solving problems associated with the provision of services in SIB and in the future can be a starting point for calculating the cost of providing services.

УДК 004.056.53(045)

СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НА БАЗІ МІЖНАРОДНИХ СТАНДАРТІВ СЕРІЇ ISO

Анна Чунарьова, Андрій Чунарьов
Національний авіаційний університет

Стаття: ***4 стор., 4 джерел.***

Для ефективного функціонування організації доводиться ідентифікувати та управляти багатьма процесами, а саме процесом управління ризиками інформаційного об’єкту. Оцінювання ризиків організації є первинним етап при розробці та експлуатації захищених інформаційних систем. Через оцінки ризиків ідентифікуються загрози активам, оцінюються їх уразливість й імовірність виникнення загроз, а також можливий руйнівний вплив під час реалізації несанкціонованих дій. В даній статті запропоновано сценарій управління ризиками інформаційного об’єкту.

Запропонований сценарій розрахунку ризиків складається з наступних базових складових, а саме:

−визначення методології оцінювання ризику для інформаційної системи;

−розроблення критеріїв ухвалення ризиків та визначення прийнятого рівня ризику;

−визначення активів;

−виявлення небезпеки для активів;

−виявлення вразливих місць в системі захисту;

−виявлення дій, які порушують конфіденційність, цілісність та доступність активів та інформаційної ситсеми;

−визначення ймовірності провалу системи безпеки за наявності вразливостей;

−оцінювання рівнів ризику;

−визначення прийнятності ризику або проведення процедури скорочення, використовуючи встановлені критерії допустимості та прийнятності ризику;

−вибір завдань та засобів управління для скорочення ризиків з умов забезпечення ефективності захисту.

Також, в статті виділено ряд переваг застосування системи управління інформаційною безпекою на базі міжнародних стандартів серії ISO в сучасних інформаційно-комунікаційних системах та мережах. На основі запропонованого сценарію розроблена структурна схема оцінювання інформаційних ризиків.

СИСТЕМА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ НА БАЗЕ МЕЖДУНАРОДНЫХ СТАНДАРТОВ СЕРИИ ISO

Анна Чунарева, Андрей Чунарев
Национальный авиационный університет

Для эффективного функционирования организации приходится идентифицировать и управлять многими процессами, а именно процессом управления рисками информационного объекта. Оценка рисков организации является первичным этап при разработке и эксплуатации защищенных информационных систем. Через оценки рисков идентифицируются угрозы активам, оцениваются их уязвимость и вероятность возникновения угроз, а также возможное разрушительное воздействие при реализации несанкционированных действий. В данной статье предложен сценарий управления рисками информационного объекта.

Предложенный сценарий расчета рисков состоит из следующих базовых составляющих, а именно:

–определение методологии оценки риска для информационной системы;

–разработка критериев принятия рисков и определения принятого уровня риска;

–определение активов;

–выявление опасности для активов;

–выявление уязвимых мест в системе защиты;

–выявление действий, нарушающих конфиденциальность, целостность и доступность активов и информационной ситсемы;

–определение вероятности провала системы безопасности при наличии уязвимостей;

–оценка уровня риска;

–определение приемлемости риска или проведения процедуры сокращения, используя установленные критерии допустимости и приемлемости риска;

–выбор задач и средств управления для сокращения рисков из условий обеспечения эффективности защиты.

Также, в статье выделен ряд преимуществ применения системы управления информационной безопасностью на базе международных стандартов серии ISO в современных информацийно-коммуникационных системах и сетях. На основе предложенного сценария разработана структурная схема оценки информационных рисков.

INFORMATION SECURITY MANAGEMENT SYSTEM BASED ON INTERNATIONAL STANDARDS OF ISO

Anna Chunareva, Andrew Chunarev
National Aviation University

For effective functioning the organization it is necessary to identify and operate many processes, namely managerial process by risks of information object. The assessment of risks of the organization is primary a stage by development and operation of the protected information systems. Through assessments of risks threats to actives are identified, their vulnerability and probability of occurrence of threats, as well as possible destructive influence of in using not authorized actions are estimated. In given article the script of management is offered by risks of information object.

The offered script of calculation of risks will consist of following base components, namely:

definition of methodology of an assessment of risk for information system;

development of criteria of acceptance of risks and definitions of the accepted risk level;

–definition of actives;

–revealing danger to actives;

–revealing critical areas in system of protection;

–revealing the actions breaking confidentiality, integrity and availability of actives and information ситсемы;

−definition of probability of a failure of system of a security at availability уязвимостей;

−an assessment of a risk level;

−definition of an acceptability of risk or carrying out of procedure of reduction, using the installed criteria of an admissibility and an acceptability of risk;

−a choice of problems and control facilities for reduction of risks from conditions of maintenance of efficiency of protection.

Also, in article a number of advantages is allocated of application of a control system by an information security on the basis of the international standards of set ISO in modern information-communication systems and networks is allocated. On the basis of the offered script developed the block diagram of an assessment of information risks.

УДК 621.391.7

СПЕЦІАЛІЗОВАНІ ПРОЦЕСОРИ АСИМЕТРИЧНОГО ШИФРУВАННЯ ІНФОРМАЦІЇ НА ОСНОВІ РЕКУРЕНТНИХ ПОСЛІДОВНОСТЕЙ

Юрій Яремчук

Вінницькій національний технічний університет

Стаття: ***6 стор., 6 джерел.***

У роботі розглянуто математичний апарат рекурентних V_k^+ – та U_k –послідовностей та на його основі представлено метод асиметричного шифрування інформації, суть якого полягає в заміні піднесення до степеня обчисленням певного елементу U_k –послідовності. Особливість представленого методу шифрування полягає в тому, що усі процедури в ньому виконуються принципово послідовно, тому запропоновано спеціалізований процесор для шифрування (дешифрування), який містить один пристрій для обчислення елементів V_k^+ – та U_k –послідовностей. Організація пам'яті для спрощення реалізується у вигляді окремих блоків пам'яті для зберігання різних даних. Порівняння процесорів, що реалізують запропонований метод та відомий метод Ель-Гамаля показує, що перші забезпечують майже однаковий час шифрування–дешифрування при $k = 2$ та більший час при $k > 2$. Однак суттєвою перевагою запропонованого методу є те, що він дозволяє встановлювати необхідну криптостійкість залежно від параметру k. Також перевагою розроблених спеціалізованих процесорів асиметричного шифрування на основі рекурентних V_k^+ – та U_k – послідовностей може бути те, що принципи їх організації можуть стати основою для побудови спеціалізованих процесорів різного криптографічного призначення, що реалізують технологію відкритого ключа, зокрема, в задачах автентифікації або цифрового підписування, де переваги в швидкості криптографічних перетворень на основі V_k^+ – та U_k –послідовностей можуть бути більш суттєвими і важливими.

СПЕЦИАЛИЗИРОВАННЫЕ ПРОЦЕССОРЫ АССИМЕТРИЧНОГО ШИФРОВАНИЯ ИНФОРМАЦИИ НА ОСНОВЕ РЕКУРРЕНТНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Юрий Яремчук

Винницкий национальный технический університет

В работе рассмотрен математический аппарат рекуррентных V_k^+ – и U_k –последовательностей и на его основе представлен метод ассиметричного шифрования информации, суть которого состоит в замене возведения в степень вычислением определённого элемента U_k –последовательности. Особенность представленного метода шифрования состоит в том, что все процедуры в нём выполняются принципиально последовательно, поэтому предложен специализированный процессор для шифрования (дешифрования), который содержит одно устройство для вычисления элементов V_k^+ – и U_k –последовательностей. Организация памяти для упрощения реализуется в виде отдельных блоков памяти для хранения различных

данных. Сравнения процессоров, реализующих предложенный метод и известный метод Эль-Гамаля показывают, что первые обеспечивают почти одинаковое время шифрования – дешифрования при $k = 2$ и большее время при $k > 2$. Однако существенным преимуществом предложенного метода является то, что он позволяет устанавливать необходимую криптостойкость в зависимости от параметра k. Также преимуществом разработанных специализированных процессоров ассиметричного шифрования на основе рекуррентных V_k^+ – и U_k –последовательностей может быть то, что принципы их организации могут стать основой для построения специализированных процессоров различного криптографического назначения, реализующих технологию открытого ключа, в частности, в задачах аутентификации или цифровой подписи, где преимущества по скорости криптографических преобразований на основе V_k^+ – и U_k – последовательностей могут быть более существенными и важными.

SPECIALIZED PROCESSORS OF ASYMMETRIC ENCRYPTION INFORMATION BASED ON RECURRENT SEQUENCES

Iurii Iaremchuk
Vinnytsia national technical university

The paper deals with the mathematical apparatus of recurrent V_k^+ - and U_k –sequences, on whose basis a method of asymmetric encryption information is presented, the essence of which is to replace the exponentiation via calculation of a certain element of U_k –sequence. The peculiarity of the presented method of encryption is that all the procedures are carried out consistently, so a specialized processor was offered for encryption (decryption) containing one device for calculating elements of V_k^+ - and U_k –sequences. To simplify the organization of memory, it is implemented as a separate memory block for storage of various data. A comparison of processors that implement the proposed method and the known Al Gamal method shows that the former offer almost the same time of encryption - decryption at $k = 2$ and more time at $k > 2$. However, a significant advantage of this method is that it allows setting the desired cryptographic reliability depending on the parameter k. Also, the advantage of the developed specialized processors of asymmetric encryption based on recurrent V_k^+ - and U_k –sequences may be the principles of their organization that can become the basis for construction of specialized processors of different cryptographic purpose that implement the public key technology, in particular in authentication or digital signature tasks, where the speed advantages of cryptographic transformations based on V_k^+ - and U_k –sequences may be more significant and important.

УДК 681.3.06(075.8)

АНОНІМНІСТЬ ЯК КРИТЕРІЙ ОЦІНКИ ЗАХИЩЕНОСТІ ПРОТОКОЛІВ СЛІПОГО ЕЛЕКТРОННОГО ЦИФРОВОГО ПІДПИСУ

Галина Козіна, Геннадій Нікуліщев
Запорізький національний технічний університет

Стаття: ***8 стор., 5 джерел.***

На часі разом із завданнями реалізації стандартних схем електронного цифрового підпису (ЕЦП) практичну актуальність і значущість мають реалізації інших схем, зокрема, сліпого підпису. Сліпий ЕЦП дозволяє авторові документа довести його юридичну значимість, не розкриваючи власної особи. Це може знадобитися, зокрема, при проведенні електронного голосування чи розрахунку електронними грошима. В типовій схемі сліпого підпису, як правило, приймають участь три сторони – емітент документу, підписувач та валідатор.

Таким чином, у випадку сліпого ЕЦП до критеріїв захищеності схеми підпису додається анонімність – неможливість відстежити за підписаним документом його автора і однозначно їх пов'язати. Втім, в деяких схемах у підписувача може виявитись можливість порушити анонімність, оскільки в процесі формування

остаточного підпису він обмінюється з емітентом документа додатковими параметрами, передбаченими схемою підпису. Якщо підписувач збереже ці параметри, пов'язавши їх з конкретним емітентом, а в подальшому зможе отримати доступ до документу із власним підписом у відкритому вигляді, то він зможе спробувати вирахувати його автора за допомогою збережених параметрів. Обчисливши маскуючі параметри, які використовував емітент, підписувач зможе однозначно пов'язати його із документом, що призведе до порушення анонімності.

Для перевірки схеми сліпого ЕЦП за критерієм анонімності необхідно з'ясувати, чи є у підписувача можливість обчислити підпис в не замаскованому вигляді за допомогою бази даних проміжних значень, яку він створює при постановці підпису. В статті розглянуті 3 протоколи сліпого підпису. Для двох показано, що вони не забезпечують захищеність підписаного повідомлення за критерієм анонімності. Для третьої схеми доведено стійкість за цим критерієм. Наведені приклади розрахунків за всіма протоколами.

АНОНИМНОСТЬ КАК КРИТЕРИЙ ОЦЕНКИ ЗАЩИЩЕННОСТИ ПРОТОКОЛОВ СЛЕПОЙ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Галина Козина, Геннадий Никулищев
Запорожский национальный технический университет

Сейчас наряду с задачами реализации стандартных схем электронной цифровой подписи (ЭЦП) практическую актуальность и значимость имеют реализации других схем, в частности, слепой подписи. Слепая ЭЦП позволяет автору документа доказать его юридическую значимость, не раскрывая своей личности. Это может понадобиться, в частности, при проведении электронного голосования или расчета электронными деньгами. В типичной схеме слепой подписи, как правило, принимают участие три стороны - эмитент документа, подписчик и валидатор.

В случае слепой ЭЦП к критериям защищенности схемы подписи добавляется анонимность - невозможность отследить по подписанному документу его автора и однозначно их связать. Однако, в некоторых схемах у подписчика может оказаться возможность нарушить анонимность, поскольку в процессе формирования окончательной подписи он обменивается с эмитентом документа дополнительными параметрами, предусмотренными схемой подписи. Если подписчик сохранит значения этих параметров, связав их с конкретным эмитентом, а в дальнейшем сможет получить доступ к документу с собственной подписью в открытом виде, то он сможет попробовать вычислить его автора при помощи хранимых параметров. Вычислив маскирующие параметры, которые использовал эмитент, подписчик сможет однозначно связать его с документом, что приведет к нарушению анонимности.

Для проверки схемы слепой ЭЦП по критерию анонимности необходимо выяснить, есть ли у подписчика возможность вычислить подпись в открытом виде с помощью базы данных промежуточных значений, которую он создает при постановке подписи. В статье рассмотрены 3 протокола слепой подписи. Для двух показано, что они не обеспечивают защищенность подписанного сообщения по критерию анонимности. Для третьей схемы доказана устойчивость по этому критерию. Приведены примеры расчетов по каждому протоколу.

ANONYMITY AS A CRITERION FOR EVALUATING SECURITY PROTOCOLS BLIND ELECTRONIC DIGITAL SIGNATURE

Galina Kozina, Gennady Nikulischev
Zaporizhzhya National Technical University

Now, along with the tasks of implementing the standard digital signature schemes, the implementation of other schemes, in particular, the blind signature have practical relevance and importance. Blind signature allows the author of the document to prove its legal value, without disclosing his identity. It may be necessary in electronic voting or electronic money. Typical blind signature scheme usually involves three parties - the issuer of the document, the signer and the validator.

Blind signature schemes have one more security criterion - anonymity of the signature. It means the inability to trace the document signed by the author and associate them uniquely. However, in some schemes the signer may have an opportunity to break anonymity due to the process of final signature formation. While communicating with the issuer of the document the signer can record additional parameters, used in the scheme. If the signer will retain

the values of these parameters by relating them to a specific issuer, and in the future be able to get access to the document with his signature, he can try to calculate its author with the help of stored values. If the signer can calculate the masking parameters, which are used by the issuer, he will be able to uniquely associate him with the document, that will lead to a breach of anonymity.

To evaluate the blind signature scheme by anonymity criterion it is necessary to determine whether a signer can compute the clear signature with the help of an intermediate values database, which he created while setting a masked signature. The article deals with two blind signature protocols, that does not provide a signed message security by anonymity, and a scheme that is stable by this criterion.

УДК 681.3.06

ВДОСКОНАЛЕННЯ АЛГОРИТМУ НАВЧАННЯ БАГАТОШАРОВОГО ПЕРСПЕТРОНУ ПРИЗНАЧЕНОГО ДЛЯ РОЗПІЗНАВАННЯ МЕРЕЖЕВИХ АТАК

Ігор Терейковський
Кафедра спеціалізованих комп'ютерних систем НТУУ "КПІ"

Стаття: ***6 стор., 7 джерел.***

На протязі декількох останніх років розпізнавання атак на інформацію комп'ютерних систем та мереж являється однією із найбільш важливих та актуальних проблем в галузі захисту інформації. Складність проблеми обумовлена багатофакторною динамікою функціонування означених систем, великою різноваріантністю відомих та постійним виникненням нових видів атак. По цим причинам розпізнати атаку за допомогою методів, які базуються на класичному аналізі статистики функціональних параметрів комп'ютерних систем та мереж в багатьох випадках практично неможливо. Як наслідок знаходять застосування різноманітні альтернативні математичні теорії, в тому числі і теорія штучних нейронних мереж, що довела свою ефективність в задачах аналізу багатопараметричних, зашумлених даних. Відомі вдалі спроби розпізнавати за допомогою нейронних мереж віддалені мережеві атаки, комп'ютерні віруси, приховані факти передачі зашифрованих даних, спам-листи електронної пошти.

Більшість сучасних нейромережевих методів розпізнавання атак на комп'ютерні системи та мережі базуються на використанні багатошарового перспетрону, основною задачею якого є визначення допустимості відхилень параметрів поточного функціонування від параметрів функціонування в нормальних умовах. При цьому одним із найбільш значимих недоліків використання багатошарового перспетрону є висока відносна похибка навчання при вирішенні задачі апроксимації заданої табличної функції, мінімальні та максимальні значення якої значно відрізняються між собою в області мінімальних значень функції. Відносно задач розпізнавання атак це призводить до низької достовірності визначення допустимості відхилень параметрів поточного функціонування в області їх мінімальних значень, що в свою чергу може значно зменшити ефективність розпізнавання мережевих атак, коли необхідно визначити допустимість відхилення контролюємих параметрів від шаблону нормальної поведінки, або від шаблону атаки. Показано, що вказаний недолік спричинений неадекватністю цільового функціоналу алгоритму зворотнього поширення помилки, який застосовується для навчання багатошарового перспетрону.

Для виправлення вказаного недоліку запропоновано вдосконалити алгоритм зворотнього поширення помилки за рахунок застосування цільового функціоналу у вигляді квадратичної приведеної помилки навчання. Розроблене відповідне математичне забезпечення корекції вагових коефіцієнтів синаптичних зв'язків.

Перспективним шляхом підвищення ефективності застосування нейромережевих методів розпізнавання атак є розробка методики оптимізації структури багатошарового перспетрону відповідно умов конкретних задач.

УСОВЕРШЕНСТВОВАНИЕ АЛГОРИТМА ОБУЧЕНИЯ МНОГОСЛОЙНОГО ПЕРСПЕТРОНА ПРЕДНАЗНАЧЕНО ДЛЯ РАСПОЗНАВАНИЯ СЕТЕВЫХ АТАК

Игорь Терейковский
Кафедра специализированных компьютерных систем НТУУ "КПИ"

На протяжении нескольких последних лет распознавания атак на информацию компьютерных систем и сетей является одной из наиболее важных и актуальных проблем в области защиты информации. Сложность проблемы обусловлена многофакторной динамикой функционирования указанных систем, большой разновариантность известных и постоянным возникновением новых видов атак. По этим причинам распознать атаку с помощью методов, основанных на классическом анализе статистики функциональных параметров компьютерных систем и сетей во многих случаях практически невозможно. Как следствие находят применение различные альтернативные математические теории, в том числе и теория искусственных нейронных сетей, которая доказала свою эффективность в задачах анализа многопараметрических, зашумленных данных. Известны удачные попытки распознавать с помощью нейронных сетей отдаленные сетевые атаки, вирусы, скрытые факты передачи зашифрованных данных, спам-письма электронной почты.

Большинство современных нейросетевых методов распознавания атак на компьютерные системы и сети базируются на использовании многослойного персптрона, основной задачей которого является определение допустимости отклонений параметров текущего функционирования от параметров функционирования в нормальных условиях. При этом одним из наиболее значимых недостатков использования многослойного персптрона является высокая относительная погрешность обучения при решении задачи аппроксимации заданной табличной функции, минимальные и максимальные значения которой значительно отличаются между собой в области минимальных значений функции. Относительно задач распознавания атак это приводит к низкой достоверности определения допустимости отклонений параметров текущего функционирования в области их минимальных значений, что в свою очередь может значительно снизить эффективность распознавания сетевых атак, когда необходимо определить допустимость отклонения контролируемых параметров от шаблона нормального поведения, или от шаблона атаки. Показано, что указанный недостаток вызван неадекватностью целевого функционала алгоритма обратного распространения ошибки, который применяется для обучения многослойного персптрона.

Для исправления указанного недостатка предложено усовершенствовать алгоритм обратного распространения ошибки за счет применения целевого функционала в виде квадратичной приведенной ошибки обучения. Разработано соответствующее математическое обеспечение коррекции весовых коэффициентов синаптических связей.

Перспективным путем повышения эффективности применения нейросетевых методов распознавания атак является разработка методики оптимизации структуры многослойного персптрона в соответствии с условиями конкретных задач.

ENHANCED LEARNING ALGORITHM MULTILAYER PERCEPTRON DEVOTED FOR RECOGNIZING NETWORK ATTACKS

Igor Terejkowski
Department of specialized computer systems "KPI"

Over the past few years, recognition of attacks on information systems and computer networks is one of the most important and urgent problems in the field of information security. The complexity of the problem is caused by the dynamics of multi functioning of these systems, large raznovariantnost known and constant emergence of new types of attacks. For these reasons, to recognize an attack using methods based on classical statistical analysis of the functional parameters of computer systems and networks, in many cases almost impossible. As a consequence, are used various alternative mathematical theories, including the theory of artificial neural networks, has proven successful in the multivariable analysis tasks, noisy data. There are successful attempts to identify with the help of neural networks remote network attacks, viruses, hidden facts of the transfer of encrypted data, the spam email.

Most modern methods of pattern recognition neural network attacks on computer systems and networks based on the use of multi-layer perceptron, whose main task is to determine the tolerance parameters of the current functioning of the parameters of the operation under normal conditions. At the same time one of the most significant disadvantages of using a multilayer perceptron is a high relative error of training in solving the problem of approximation of a given table function, the minimum and maximum values which significantly differ in the minimum values of the function. With regard to problems of recognition of attacks, this leads to low reliability of the parameters determining the admissibility of the deviations of the current functioning of their minimum values, which in turn can significantly reduce the efficiency of detection of network attacks, when it is necessary to determine the

admissibility of the deviations of monitored parameters from the normal pattern of behavior or pattern of attack. It is shown that this deficiency is caused by the inadequacy of the objective functional backpropagation algorithm, which is used for training a multilayer perceptron.

To remedy this defect suggested to improve the back-propagation algorithm for error due to application of the objective function given in the form of a quadratic error learning. Developed by the appropriate software correction weights of synaptic connections.

Promising way of improving the application of neural network methods for detection of attacks is to develop methods of optimizing the structure of multilayer perceptron in accordance with the terms of specific tasks.

УДК 004.4.5, 681.030

АВТОМАТИЧНЕ НАЛАШТУВАННЯ І ПЕРЕВІРКА НАЛАШТУВАНЬ СЛУЖБ ОПЕРАЦІЙНОЇ СИСТЕМИ ПРИ ВИКОРИСТАННІ КОМПЛЕКСНИХ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ

Денис Танцюра
НДЦ"ТЕЗІС" (НТУУ "КПІ")

Стаття: ***11 стор, 26 джерел.***

Налаштування і перевірка налаштувань служб операційної системи є необхідною складовою при створенні комплексної системи захисту в автоматизованій системі, а також при проведенні її експертизи, що може займати значний обсяг часу. Автором розглянуті можливі варіанти для швидкого, надійного та зручного виконання цих операцій і розроблені такі варіанти для налаштування служб операційної системи Windows XP. Також були проведені експерименти по застосованості запропонованих і розроблених варіантів для різних комплексів засобів інформації в автоматизованих системах класу 1 на різних операційних системах Windows.

АВТОМАТИЧЕСКАЯ НАСТРОЙКА И ПРОВЕРКА НАСТРОЕК СЛУЖБЫ ОПЕРАЦИОННОЙ СИСТЕМЫ ПРИ ИСПОЛЬЗОВАНИИ КОМПЛЕКСНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

Денис Танцюра
НИЦ "ТЕЗИС" (НТУУ "КПИ")

Настройка и проверка настройки служб операционной системы является необходимой составляющей при создании комплексной системы защиты информации в автоматизированной системе, а также при проведении ее экспертизы, что может занимать значительный объем времени. Автором рассмотрены возможные варианты для быстрого, надежного и удобного выполнения этих операций и разработаны такие варианты для настройки служб операционной системы Windows XP. Также были проведены эксперименты по применимости предложенных и разработанных вариантов для различных комплексов средств защиты информации в автоматизированных системах класса 1 на различных операционных системах Windows.

AUTOMATIC ADJUSTMENT AND VERIFICATION OF CONFIGURATION SERVICES OPERATING SYSTEM USING COMPLEX INFORMATION SECURITY TOOLS IN AUTOMATED SYSTEMS

Denis Tantsyura
SRCof TPI "TESIS" (NTUU "KPI")

Configuration and verifying configuration services operating system is a necessary part to create complex security system in the automated system, as well as fulfillment examination, which can take a considerable amount of time. Author reviewed possible options for fast, reliable and friendly execution of these operations. Author developed the solutions to the problem for automatic configuring services of the operating system Windows XP. Also, the author has performed experiments on the applicability proposed and developed variants solution for different complexes of information security in automated systems class 1 on different Windows operating systems.

УДК 654.924

АНАЛІЗ ЕФЕКТИВНОСТІ ОХОРОННИХ СПОВІЩУВАЧІВ ПРИ ПАСИВНОМУ ВПЛИВУ ПОРУШНИКА

Володимир Волхонскій, Роберт Трапш

Санкт-Петербурзький національний дослідницький університет інформаційних технологій, механіки та оптики

Стаття: ***5 стор., 3 джерела***

Розробка та аналіз ефективності системи охоронної сигналізації вимагає оцінки ймовірності виявлення (ВО) несанкціонованого проникнення, особливо при охороні важливих об'єктів через зростання ймовірності застосування порушником методів і засобів, що знижують можливість його виявлення. Доцільно розглянути вплив на датчики охоронної сигналізації і різні варіанти їх структур різних напрямків руху порушника. В якості критерію оцінки ефективності розглянутих структур використовуємо критерій неспільних ефективних впливів на датчики.Для одиночних датчиків з неперекривающіеся зонами виявлення (ЗО) умисне переміщення порушника в радіальному напрямку для пасивного інфрачервоного датчика (ПІК) і для радіохвильового (РВ) в тангенціальному може призводити до суттєвого зменшення ВО. Цей прийом може використовуватися порушником і для окремих каналів комбінованих датчиків. А також і для суміщених.При використанні пар одиночних рознесених датчиків з перекриваються ЗО, розташованих в різних місцях і осями діаграм спрямованості розгорнутими по відношенню один до одного на 90^0, буде напрямок руху НП, однаково ефективно для виявлення обома датчиками. Але також буде і напрямок (радіальне для ПІК і тангенціальне для РВ датчика), при русі порушника в якому ВО буде мала.Зниження ВО при русі порушника в довільному напрямку можна уникнути, використовуючи дві пари згаданих рознесених датчиків, кожна з яких розгорнута на 900 відносно один одного. Це дозволить ефективно виявити порушника при русі у всіх напрямках. Використання алгоритму «І» для пристроїв кожної пари дозволить зберегти низьку ймовірність помилкової тривоги.

АНАЛИЗ ЭФФЕКТИВНОСТИ ОХРАННЫХ ИЗВЕЩАТЕЛЕЙ ПРИ ПАССИВНЫХ ВОЗДЕЙСТВИЯХ НАРУШИТЕЛЯ

Владимир Волхонский, Роберт Трапш

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Разработка и анализ эффективности системы охранной сигнализации требует оценки вероятности обнаружения (ВО) несанкционированного проникновения, особенно при охране важных объектов из-за роста вероятности применения нарушителем методов и средств, снижающих возможность его обнаружения. Целесообразно рассмотреть влияние на датчики охранной сигнализации и различные варианты их структур разных направлений движения нарушителя. В качестве критерия оценки эффективности рассматриваемых структур используем критерий несовместности эффективных воздействий на датчики.

Для одиночных датчиков с неперекрывающиеся зонами обнаружения (ЗО) умышленное перемещение нарушителя в радиальном направлении для пассивного инфракрасного датчика (ПИК) и для радиоволнового (РВ) в тангенциальном может приводить к существенному уменьшению ВО. Этот прием может использоваться нарушителем и для отдельных каналов комбинированных датчиков. А также и для совмещенных.

При использовании пар одиночных разнесенных датчиков с перекрывающимися ЗО, расположенных в разных местах и осями диаграмм направленности развернутыми по отношению друг к другу на 90^0, будет направление движения НП, одинаково эффективно обнаруживаемое обоими датчиками. Но также будет и

направление (радиальное для ПИК и тангенциальное для РВ датчика), при движении нарушителя в котором ВО будет мала.

Снижения ВО при движении нарушителя в произвольном направлении можно избежать, используя две пары упомянутых разнесенных датчиков, каждая из которых развернута на 90^0 относительно друг друга. Это позволит эффективно обнаружить нарушителя при движении во всех направлениях. Использование алгоритма «И» для устройств каждой пары позволит сохранить низкую вероятность ложной тревоги.

ANALYZIZ OF SECURITY DETECTORS EFFECTIVENESS UNDER PASSIVE INFLUENCE OF INTRUDER

Vladimir Volkhonski, Robert Trapsh
Saint-Petersburg National Research University of Information Technology, Mechanics and Optics

Development and analyzes of alarm security system effectiveness required estimation of probability detection (PD) of intruder penetration. Especially for critical infrastructure protection due to opportunity of application by intruder special modes for decreasing of PD. So it makes sense to research influence of different movement direction of intruder upon alarm security detectors and their structures. As criterion of effectiveness could be used criterion of influence intruder incompatibility.

For single detectors with non overlap of detection pattern movement direction of intruder in radial direction for passive infrared (PIR) and tangential direction for microwave (MW) detectors will lead to decreasing of PD.

In case single detectors with overlap of detection pattern which are installed into different places and has detection patterns with axes oriented on 90^0 there will be movement direction of intruder with effective detection by both detectors. But there will be also direction (radial for PIR and tangential for MW) with low PD.

In order to keep high PD for any movement direction of intruder could be used double pair of single detectors with overlap of detection pattern which placed into different corners and has detection patterns with axes orientation onto 90^0 between each of detectors and each pair. Decision algorithm “AND” for each pair of detectors will lead to low false alarm in addition.

УДК 621.395

СИНТЕЗ РАЦІОНАЛЬНОЇ СТРУКТУРИ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ ЗА ЗАДАНИМИ ПОКАЗНИКАМИ

Валерій Правило
ВІТІ НТУУ “КПІ”

Стаття: ***8 стор, 5 джерел.***

Метою статті є розгляд методики синтезу структури телекомунікаційної мережі (ТКМ) за показниками мінімальної вартості та структурної надійності, аналіз і обґрунтування алгоритмів та методів синтезу ТКМ, представлення блок-схеми алгоритму синтезу структури ТКМ. Актуальність даної статті визначається необхідністю рішення завдання знаходження різних раціональних первісних топологічних структур ТКМ і вибору прийнятного результату з отриманої безлічі рішень.

Виділяють два класи алгоритмів для вирішення завдань синтезу структури ТКМ: алгоритми строгої оптимізації та алгоритми евристичного пошуку. Найбільше поширення одержали евристичні алгоритми, які в умовах обмеження часу дозволяють при покроковій зміні заданої первісної структури мережі одержати вузький діапазон структур, що задовольняють заданим вимогам.

Особливістю представленої методики є те, що синтез структури ТКМ запропоновано здійснювати у два етапи. На першому етапі, для звуження області пошуку, синтезувати початкову структуру мережі, використовуючи алгоритм Краскала. Даний алгоритм вже на початкових етапах синтезу дозволяє одержати структуру, яка задовольняє поставленим вимогам. На другому етапі для визначення раціональної структури мережі за критерієм мінімальної вартості мережі при виконанні вимог до значень показників структурної надійності запропоновано використати метод насичених перетинів.

Представлена блок-схема алгоритму більш наочно пояснює реалізацію запропонованої методики синтезу структури ТКМ за показниками мінімальної вартості й структурної надійності.

СИНТЕЗ РАЦИОНАЛЬНОЙ СТРУКТУРЫ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ ПО ЗАДАННЫМ ПОКАЗАТЕЛЯМ

Валерий Правило
ВИТИ НТУУ "КПИ"

Целью статьи является рассмотрение методики синтеза структуры телекоммуникационной сети (ТКС) по показателям минимальной стоимости и структурной надежности, анализ и обоснование алгоритмов и методов синтеза ТКС, представление блок-схемы алгоритма синтеза структуры ТКС. Актуальность данной статьи определяется необходимостью решения задачи нахождения различных рациональных первоначальных топологических структур ТКС и выбора приемлемого результата из полученного множества решений.

Выделяют два класса алгоритмов для решения задач синтеза структуры ТКС: алгоритмы строгой оптимизации и алгоритмы эвристического поиска. Наибольшее распространение получили эвристические алгоритмы, которые в условиях ограничения времени позволяют при пошаговом изменении заданной первоначальной структуры сети получить узкий диапазон структур, удовлетворяющих заданным требованиям.

Особенностью представленной методики является то, что синтез структуры ТКС предложено осуществлять в два этапа. На первом этапе, для сужения области поиска, синтезировать начальную структуру сети, используя алгоритм Краскала. Данный алгоритм уже на начальных этапах синтеза позволяет получить структуру, которая удовлетворяет поставленным требованиям. На втором этапе, для определения рациональной структуры сети по критерию минимальной стоимости, при выполнении требований к значениям показателей структурной надежности, предложено использовать метод насыщенных сечений.

Представленная блок-схема алгоритма более наглядно объясняет реализацию предложенной методики синтеза структуры ТКС по показателям минимальной стоимости и структурной надежности.

SYNTHESIS OF RATIONAL STRUCTURE OF THE TELECOMMUNICATION NETWORK ON SPECIFIED INDEXES

Valeriy Pravilo
MITI NTUU "KPI"

The purpose of given article is reviewing of a technique of synthesis of structure of a telecommunication network (TCN) on indexes of the minimum cost and structural reliability, the analysis and a substantiation of algorithms and methods of synthesis of TCN, representation of a block diagram of a synthesis algorithm of structure of TCN. The urgency of given article is defined by necessity of the solving of the task of a finding of various rational initiating topological structures of TCN and a choice of comprehensible result from the received set of decisions.

There are two classes of algorithms for solving of tasks of synthesis of structure TCN: algorithms of strict optimization and algorithms of heuristic search. The greatest propagation was received by heuristic algorithms which in the conditions of time restriction allow at step by step change of the given initial structure of a network, to receive narrow range of structures which satisfies the given requirements.

Singularity of the presented technique is that synthesis of TCN structureis offered for carrying out in two stages. At the first stage, for search area narrowing, we have to synthesize initial structure of a network, using algorithm of Kraskala. The given algorithm at the very begenning of the synthesis allows to receive structure which meets the case. At the second stage, for determination of rational structure of a network by criterion of the minimum cost, at performance of requirements to values of indexes of structural reliability, it is offered to use a method of saturated sections.

The presented block diagram of algorithm explains implementation of the offered technique of synthesis of structure TCN on indexes of the minimum cost and structural reliability more visually.

УДК 638.235.231

ІДЕНТИФІКАЦІЯ НЕЛІНІЙНИХ РОЗСІЮВАЧІВ ЗА РІВНЕМ ОДНІЄЇ ГАРМОНІКИ

Максим Зінченко, Юрій Зіньковський, Михайло Прокофьєв
НДЦ «ТЕЗІС» НТУУ «КПІ»

Стаття: ***9 стор, 15 джерел.***

Перспективним напрямком вдосконалення нелінійних радіолокаторів (НР) є дослідження вторинних демаскуючих ознак напівпровідникових нелінійних розсіювачів (НРс), що безпосередньо покращать ефективність використання засобів нелінійної радіолокації в процесі пошуку закладних пристроїв. Дослідження вторинних демаскуючих ознак стає можливим завдяки аналізу внутрішніх ефектів у напівпровідникових структурах НРс під час дії відносно потужного зондуючого сигналу (ЗС) нелінійного радіолокатора. Складний напівпровідниковий НРс під час зондування відносно потужним ЗС НР здатен перевипромінювати у навколишнє середовище крім кратних гармонік частоти ЗС (у випадку моногармонічного ЗС або комбінаційних частот у випадку бігармонічного ЗС) власні коливання, що в більшості випадків є некратними гармоніками частоти ЗС НР. Це пов'язано з тим, що під час зондування відносно потужним ЗС НР на ВАХ нелінійних структур напівпровідникових НРс з'являються ділянки з негативним диференціальним опором, які в поєднанні з присутніми зворотними зв'язками призводять до самозбудження системи. Частота будь-якої некратної гармоніки є випадковою величиною, яка достатньо швидко змінюється в часі, оскільки величини параметрів більшості елементів еквівалентної коливальної системи постійно флуктують при дії відносно потужного НВЧ поля. Наслідком інерційності процесу генерування некратних гармонік є поява області петлеутворення на функціональній залежності рівня (амплітуди) другої гармоніки в розсіяному НРс сигналі відгуку від рівня потужності ЗС НР. Розглянута властивість характерна лише для напівпровідникових НРс, а тому її можна використовувати для виявлення, ідентифікації та локалізації НРс у нелінійній радіолокації. Підвищення ефективності використання НР досягається за рахунок зведення до мінімуму значущостей впливу таких факторів як: присутність у досліджуваному середовищі завадових МОМ-структур; суб'єктивність оператора; присутність паразитних пелюсток діаграми спрямованості випромінюючої антени (за рахунок обмеження рівня потужності ЗС НР).

ИДЕНТИФИКАЦИЯ НЕЛИНЕЙНЫХ РАССЕИВАТЕЛЕЙ ПО УРОВНЮ ОДНОЙ ГАРМОНИКИ

Максим Зинченко, Юрий Зиньковский, Михаил Прокофьев
НИЦ «ТЕЗИС» НТУУ «КПИ»

Перспективным направлением совершенствования нелинейных радиолокаторов (НР) является исследование вторичных демаскирующих признаков полупроводниковых нелинейных рассеивателей (НРс), что непосредственно улучшит эффективность использования средств нелинейной радиолокации в процессе поиска закладных устройств. Исследование вторичных демаскирующих признаков становится возможным благодаря анализу внутренних эффектов в полупроводниковых структурах НРс во время действия относительно мощного зондирующего сигнала (ЗС) нелинейного радиолокатора. Сложный полупроводниковый НРс во время зондирования относительно мощным ЗС НР способен переизлучать в окружающую среду кроме кратных гармоник частоты ЗС (в случае моногармонического ЗС или комбинационных частот в случае бигармонического ЗС) собственные колебания, что в большинстве случаев являются некратными гармониками частоты ЗС НР. Это связано с тем, что во время зондирования относительно мощным ЗС НР на ВАХ нелинейных полупроводниковых структур НРс появляются участки с отрицательным дифференциальным сопротивлением, которые в сочетании с присутствующими обратными связями приводят к самовозбуждению системы. Частота любой некратной гармоники является случайной величиной, которая достаточно быстро изменяется во времени, поскольку величины параметров большинства элементов эквивалентной колебательной системы постоянно флуктуируют при действии относительно мощного СВЧ поля. Следствием инерционности процесса генерирования некратных гармоник является появление области петлеобразования на функциональной зависимости уровня (амплитуды) второй гармоники в рассеянном НРс сигнале отклика от уровня мощности ЗС НР. Рассмотренное свойство характерно лишь для полупроводниковых НРс, а потому его можно использовать для обнаружения,

идентификации и локализации НРс в нелинейной радиолокации. Повышение эффективности использования НР достигается за счет сведения к минимуму значимости влияния таких факторов как: присутствие в исследуемой среде помеховых МОМ-структур; субъективность оператора; присутствие паразитных лепестков диаграммы направленности излучающей антенны (за счет ограничения уровня мощности ЗС НР).

IDENTIFICATION OF NONLINEAR SCATTERERS AFTER THE LEVEL OF ONE HARMONIC

Maxim Zinchenko, Yuriy Zinkovskiy, Mikhail Prokofiev
SRC "THESIS" OF NTUU "KPI"

Perspective direction of perfection of nonlinear radio-locators (NR) is research of secondary unmasking features of semiconductor nonlinear scatterers (NS), that directly will improve efficiency of the usage of facilities of nonlinear radar in the process of search of the mortgaged devices in the field of technical guarding. Research of secondary unmasking features becomes possible due to the analysis of internal effects in the semiconductor structures of NS during the action of relative powerful sounding signal (SS) of nonlinear radio-locator. Difficult semiconductor NS during sounding by relatively powerful SS of NR is capable to re-emit in an environment eigen oscillations except from the multiple harmonics of frequency of SS in the case of monoharmonic SS or combinational frequencies in case of biharmonic SS, that in most cases are the aliquant harmonics of frequency of SS of NR. It is related to that during sounding by relatively powerful SS of NR the areas with negative differential resistance, which in combination with present feedbacks give rise to self-excitation of the system, appear on current-voltage diagram of nonlinear semiconductor structures of NS. Frequency of any aliquant harmonic is a casual value which quickly changes in time, as values of parameters of most elements of the equivalent oscillating system constantly fluctuate at an action of relative powerful ultrahigh field. The appearance of area of looping on functional dependence of level (amplitude) of the second harmonic in the scattered by the NS the response signal from the power-level of SS of NR is the result of the time lag process of generating of aliquant harmonics. The considered property is characteristic only for semiconductor NS, and that is why it can be used for a discovery, identification and localization of NS in a nonlinear radar. The increase of efficiency of the NR usage is achived due to taking to a minimum of meaning of influence of such factors as: being in the investigated medium of obstacle MOM-structures; subjectivity of operator; presence of parasitic petals of polar pattern radiative antenna (due to limitation of power-level of SS of NR).

УДК 623.486

ОЦЕНКА ПОКАЗАТЕЛЕЙ КАЧЕСТВА ТЕХНИЧЕСКОГО ОБСЛУЖИВАНИЯ СИСТЕМ НЕПРЕРЫВНОГО ИСПОЛЬЗОВАНИЯ С ВРЕМЕННЫМ РЕЗЕРВОМ ПРИ ИЗВЕСТНЫХ НАЧАЛЬНЫХ МОМЕНТАХ РАСПРЕДЕЛЕНИЯ НАРАБОТКИ ДО ОТКАЗА

Дмитрий Могилевич, Борис Креденцер, Виктор Вишневский
ВИТИ НТУУ ,,КПИ'', ВИКНУ

Стаття: ***9 стор, 2 джерела.***

Учёт априорной неопределённости при исследовании надёжности и технического обслуживания систем различного целевого назначения представляет собой актуальную и достаточно сложную проблему.

Объектом исследования являются системы непрерывного использования с временным резервом, в условиях ограниченной информации о функции распределения наработки объекта до отказа, включающие в себя объект и пополняемый резерв времени, для которых получены новые расчётные соотношения для оценки граничных значений коэффициента простоя, коэффициента технического использования и средних удельных затрат, характеризирующих качество технического обслуживания.

Направлением дальнейших исследований в данной предметной области является получение аналогичных расчётных формул для систем эпизодического использования.

УДК 623.486

ОЦІНКА ПОКАЗНИКІВ ЯКОСТІ ТЕХНІЧНОГО ОБСЛУГОВУВАННЯ СИСТЕМ БЕЗПЕРЕРВНОГО ВИКОРИСТАННЯ З ЧАСОВИМ РЕЗЕРВОМ ПРИ ВІДОМИХ ПОЧАТКОВИХ МОМЕНТАХ РОЗПОДІЛУ НАПРАЦЮВАННЯ ДО ВІДМОВИ

Дмитро Могилевич, Борис Креденцер, Віктор Вишнівський
ВІТІ НТУУ ,,КПІ", ВІКНУ

Облік апріорної невизначеності при дослідженні надійності та технічного обслуговування систем різного цільового призначення являє собою актуальну і досить складну проблему. Об'єктом дослідження є системи безперервного використання з тимчасовим резервом, в умовах обмеженої інформації про функції розподілу напрацювання об'єкта до відмови, що включає в себе об'єкт і резерв часу, що поповнюється, для яких отримано нові розрахункові співвідношення для оцінки граничних значень коефіцієнта простою, коефіцієнта технічного використання і середніх питомих витрат, які характеризують якість технічного обслуговування. Напрямком подальших досліджень у даній предметній області є одержання аналогічних розрахункових формул для систем епізодичного використання.

УДК 623.486

EVALUATION OF QUALITY PERFORMANCES OF TECHNICAL MAINTENANCE SYSTEMS OF CONTINUOUS USE WITH RESERVE TIME AT A KNOWN INITIAL MOMENTS OF TIME TO FAILURE DISTRIBUTION

Dmytro Mogylevych, Borys Kredentser, Vyctor Vyshnivsky
VITI NTUU "KPI", VIKNU

Accounting of prior uncertainty in the study of reliability and maintenance of systems for various applications is relevant and sufficient challenge.The object of investigation of the continuous use of the temporary reserve includes facilities and replenish reserve time, for which the new settlement ratio for the boundary values of the coefficient estimates downtime, technical utilization ratio and average unit costs, characterize the quality of service in conditions of limited information on distribution function of the operating time of the object in advance.Direction for further research in this subject area is to provide similar systems design formulas for occasional use.