Реферати

УДК 35.078:342.738

З ІСТОРІЇ ЗАХИСТУ ДЕРЖАВНОЇ ТАЄМНИЦІ В УКРАЇНІ (КІНЕЦЬ XIX - ПОЧАТОК XX СТ.)

Богдан Бернадський, Валерій Ворожко*

*Міжрегіональна академія управління персоналом, *Національний авіаційний університет*

Для висвітлення історії охорони державної таємниці на території України повчальним є вивчення відповідного досвіду того часу, коли Україна входила до складу Російської імперії. На думку авторів є підстави стверджувати, що ефективнодіючого режиму секретності у Російській імперії створено не було. Кожна із складових частин державного апарату на власний розсуд визначала, які саме відомості вважаються таємними та здійснювала діяльність з захисту такого роду інформації. Розвідка і особливо контррозвідка стали відгалуженням Департаменту поліції, несучи в собі як позитивні, так і негативні сторони політичної поліції. Правовою основою організації і діяльності органів політичного розшуку з забезпечення державної безпеки в цілому та недоторканості державної таємниці служили правові норми державного кримінально-правового, кримінально-процесуального і адміністративно-поліцейського законодавства. Російське законодавство тривалий час не вирізняло як окремі види злочинів державну зраду і шпигунство. Не приділялось належної уваги розголошенню відомостей, що становлять державну таємницю. Передусім, так і не було створено органу, що координував би роботу різних відомств у цій сфері. Досить аморфним було і уявлення про саму державну таємницю, що фактично зводилось до поняття військової таємниці. Поряд із цим сама робота спецслужб була ефективною. Як свідчить вивчення досвіду царських спецслужб, найкращі їх методичні розробки було творчо осмислені та використовувались в подальші роки.

ИЗ ИСТОРИИ ЗАЩИТЫ ГОСУДАРСТВЕННОЙ ТАЙНЫ В УКРАИНЕ (КОНЕЦ XIX - НАЧАЛО XX СТ.)

Богдан Бернадский, Валерий Ворожко*

*Межрегиональная академия управления персоналом *Національний авиационный университет*

Для освещения истории охраны государственной тайны на территории Украины поучительным является изучение соответствующего опыта того времени, когда Украина входила в состав Российской империи. По мнению авторов есть основания утверждать, что эффективно действующего режима секретности в Российской империи создано не было. Каждая из составных частей государственного аппарата на собственное усмотрение определяла, какие именно сведения считаются тайными и осуществляла деятельность из защиты такого рода информации. Разведка и особенно контрразведка стали ответвлением Департамента полиции, неся в себе как позитивные так и негативные стороны политической полиции. Правовой основой организации и деятельности органов политического розыска из обеспечения государственной безопасности в целом и неприкосновенности государственной тайны служили правовые нормы государственного криминально-правового, криминально-процессуального и административно полицейского законодательство. Российское законодательство длительное время не выделяло как отдельные виды преступлений государственную измену и шпионаж. Не уделялось надлежащего внимания разглашению сведений, которые составляют государственную тайну. Прежде всего, так и не было создано орган, который координировал бы работу разных ведомств в этой сфере. Достаточно аморфным было и представление о самой государственной тайне, что фактически сводилось к понятию военной тайны. Вместе с тем сама работа спецслужб была эффективной. Как свидетельствует изучения опыта царских спецслужб, наилучшие их методические разработки было творчески осмысленные и использовались в последующие годы.

FROM HISTORY OF DEFENCE OF STATE SECRET IN UKRAINE (END XIX – BEGINNING OF XX)

Bohdan Bernadskiy, Valery Vorozhko*

*The Mizhregional'na academy of management a personnel,*National aviation university*

For illumination of history of guard of state secret on territory of Ukraine instructive is a study of the proper experience that time, when Ukraine entered in the complement of the Russian empire. In opinion of authors there are grounds to assert that effectively operating mode of secrecy in the Russian empire created it was not. Each of component parts of state machine on own discretion determined, which one information was considered secret and carried out activity from defence such of information. Secret service and especially counter-intelligence became the branch of Department of police, carrying in itself as positive so negative sides of political police. By legal framework of organization and activity of organs of political search from providing of state security on the whole and legal norms served inviolability of state secret state kriminal'no-pravovogo, kriminal'no-procesual'nogo and administratively constabulary legislations. The Russian legislation long time did not select as separate types of crimes high treason and espionage. Not spared the proper attention the disclosure of information which make a state secret. Foremost, so it was not created an organ which would co-ordinate work of different departments in this sphere. Amorphous enough was and picture of state secret, that was actually taken to the concept of military secret. Next to it work of the special services was effective. As testifies the studies of experience of the tsar's special services, the best them methodical developments it was creatively intelligent and used in subsequent years.

УДК 621.391

ДЕЯКІ АСПЕКТИ ОРГАНІЗАЦІЙНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ В УКРАЇНІ

Іван Грабовенко

Комітет з питань національної безпеки і оборони Верховної Ради України

Розглянуті етапи реорганізації служб, що пов’язані з реалізацією спеціального зв'язку та захисту інформації в Україні. Спочатку Управління урядового зв’язку, яке забезпечувало лише експлуатацію регіональної частини союзної системи спеціального зв’язку, було реорганізовано в Головне управління урядового зв’язку СБ України. Основним завданням Управління стало створення власної системи урядового зв’язку суверенної держави. Як довела практика, об’єднання функцій криптографічного та технічного захисту інформації в одному підрозділі дало можливість комплексно вирішувати питання захисту інформації, знаходити більш ефективні рішення, заощаджувати державні кошти та суттєво скоротити терміни розробки і реалізації проектів.

У зв‘язку з необхідністю додержання прав людини під час проведення оперативно-технічних заходів виникла потреба створення в державі служби спеціального зв’язку та захисту інформації України (Держспецзв’язку), як центрального органу виконавчої влади із спеціальним статусом, визначивши її основними завданнями реалізацію державної політики у сфері захисту державних інформаційних ресурсів у мережах передачі даних, забезпечення функціонування Державної системи урядового зв’язку, Національної системи конфіденційного зв’язку, криптографічного та технічного захисту інформації. Подальша ефективна діяльність Держспецзв’язку повинна проходити шляхом нарощування потужностей структур, на які покладено реалізацію згаданих завдань, підвищення їхнього значення в системі органів державного управління, створення додаткових важелів впливу на процеси реалізації державної політики у сфері інформаційної безпеки, особливо з позиції її важливості для безпечного та стабільного розвитку суспільства в умовах глобалізації процесів інформаційного обміну.

НЕКОТОРЫЕ АСПЕКТЫ ОРГАНИЗАЦИОННО-ПРАВОВОГО ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ В УКРАИНЕ

Иван Грабовенко

Комитет по вопросам национальной безопасности и обороны Верховной Рады Украины

Рассмотренные этапы реорганизации служб, которые связаны с реализацией специальной связи и защиты информации в Украине. Сначала Управление правительственной связи, которое обеспечивало лишь

эксплуатацию региональной части союзной системы специальной связи, было реорганизовано в Главное управление правительственной связи СБ Украины. Основным заданием Управления стало создание собственной системы правительственной связи суверенного государства. Как довела практика, объединение функций криптографической и технической защиты информации в одном подразделении дало возможность комплексно решать вопросы защиты информации, находить более эффективные решения, экономить государственные средства и существенно сократить сроки разработки и реализации проектов.

В связи с необходимостью соблюдения прав человека во время проведения оперативно-технических мероприятий возникла потребность создания в государстве службы специальной связи и защиты информации Украины (Госспецсвязи), как центрального органа исполнительной власти со специальным статусом, определив ее основными заданиями реализацию государственной политики в сфере защиты государственных информационных ресурсов в сетях передачи данных, обеспечения функционирования Государственной системы правительственной связи, Национальной системы конфиденциальной связи, криптографической и технической защиты информации. Последующая эффективная деятельность Госспецсвязи должна проходить путем наращивания мощностей структур, на которые положена реализация упомянутых заданий, повышения их значения в системе органов государственного управления, создания дополнительных рычагов влияния на процессы реализации государственной политики в сфере информационной безопасности, особенно с позиций ее важности для безопасного и стабильного развития общества в условиях глобализации процессов информационного обмена.

SOME ASPECTS OF ORGANIZATIONALLY LEGAL PROVIDING OF PRIV ARE IN UKRAINE

Ivan Grabovenko
Committee on questions national safety and defensive of Verkhovna Rada of Ukraine

Considered stages of reorganization of services which are related to realization of special zv"yazku and to the priv in Ukraine. At first Management of governmental connection, which provided exploitation of regional part of the allied special communication network only, was reorganized in Main administration of governmental connection of SB of Ukraine. The basic task of Management was become by creation of own governmental communication of nation-state network. As practice, association of functions of cryptographic and technical priv, led to in one subsection enabled complex to decide the question of priv, find more effective decisions, save state facilities and substantially to reduce the terms of development and realization of projects.

In connection with the necessity of inhibition of human rights during the leadthrough of operativno-tekhnichnikh measures there was a necessity of creation in the state of special intercommunication and priv Ukraine service, as a central organ of executive power with the special status, defining it basic tasks realization of public policy in the field of defence of state informative resources in DTNS, providing of functioning of the State governmental communication, National confidential communication, cryptographic and technical priv network. Subsequent effective activity of Derzhspeczv'yazku must prokhoditi by the increase of powers of structures, on which realization of the mentioned tasks, increase of their value, is fixed in the system of organs of state administration, creation of additional levers of influence on the processes of realization of public policy, in the field of informative safety, especially from position of its importance for safe and stable development of society in the conditions of globalization of processes of informative exchange.

УДК 681.3:34

ПЕРСПЕКТИВИ ПРОТИДІЇ КРИМІНАЛЬНИМ ЗАГРОЗАМ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ В УМОВАХ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

Дарія Прокоф'єва-Янчиленко
Головне управління по боротьбі з корупцією та організованою злочинністю СБ України

Значну питому вагу в системі загроз національній безпеці України мають прояви злочинної діяльності, а також інші види правопорушень та девіантної поведінки, які опосередковують або зумовлюють злочинні прояви. Від кримінальних загроз потерпають всі складові національної безпеки України, що дозволяє вести мову як про загальний вимір національної безпеки, в якому має забезпечуватись безпека від кримінальних загроз, так і про самостійну кримінологічну складову національної безпеки.

В умовах бурхливого розвитку інформаційного суспільства забезпечення кримінологічної безпеки неможливе без врахування специфіки інформаційної сфери та можливостей інформаційного простору як щодо продуціювання кримінальних загроз, так і щодо підвищення результативності протидії вказаним загрозам, що вимагає врахування в діяльності з забезпечення кримінологічної безпеки факторів інформаційної причинності у злочинній діяльності та інформаційних характеристик кримінальних загроз.

ПЕРСПЕКТИВЫ ПРОТИВОДЕЙСТВИЯ КРИМИНАЛЬНИМ УГРОЗАМ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ УКРАИНЫ В УСЛОВИЯХ ІНФОРМАЦИОННОГО ОБЩЕСТВА

Дария Прокофьева-Янчиленко
Главное управление по борьбе с коррупцией и организованной преступностью СБ Украины

Высоким удельным весом в системе угроз национальной безопасности Украины характеризуются проявления преступной деятельности, а также иные виды правонарушений и девиантного поведения, которые опосредуют или обуславливают преступные проявления. Криминальные угрозы представляют опасность для всех составляющих национальной безопасности Украины, что позволяет вести речь как об общем уровне национальной безопасности, в котором должна обеспечиваться безопасность от криминальных угроз, так и о самостоятельной криминологической составляющей национальной безопасности.

В условиях бурного развития информационного общества обеспечение криминологической безопасности невозможно без учета специфики информационной сферы и возможностей информационного пространства как в отношении продуцирования криминальных угроз, так и в отношении повышения результативности противодействия таким угрозам, что требует учитывать в деятельности по обеспечению криминологической безопасности факторы информационной причинности в преступной деятельности и информационные характеристики криминальных угроз.

PROSPECTS FOR COUNTERING THE CRIMINAL THREATS BY NATIONAL SECURITY OF UKRAINE IN THE CONDITIONS OF INFORMATION SOCIETY.

Dariya Prokof'eva-Yanchilenko
The Main anti-corruption and organized crime department of the Security Service of Ukraine(SBU)

The criminal activity's manifestations has a high specific gravity in the system of threats of National Security in Ukraine, and also another types of offences and deviant behavior, which will mediate or stipulate criminal activity. Criminal threats present a danger for all constituents of national security, what allows to conduct as about the general measuring of national security, where security must be provided from criminal threats, so about the independent criminology constituent of national security.

In the conditions of rapid development of informative society providing of criminology security is impossible without the account of specific of informative sphere and possibilities of informative space as in regard to producting of criminal threats, so in regard to the increase of effectiveness of counteraction to such threats, that requires to take into account the factors of informative causality in criminal activity and informative descriptions of criminal threats while provide criminology security.

УДК 621.391

СТРУКТУРА ТА МОДЕЛЬ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В РАМКАХ ПРОЦЕСНОГО ПІДХОДУ

Олександр Потій, Анатолій Лєншин, Дмитро Пилипенко
Інститут інформаційних технологій

Пропонується концепція Демінга-Шухарата побудови системи управління інформаційною безпекою (СУІБ), яка описується як послідовність: планування (Plan); здійснення (Do); перевірка (контроль) (Check);

дія (Act). Модель системи управління, що запропонована в роботі, може виступати основою для впровадження у практику захисту інформації вимог стандарту ISO/IEC 27001. Відмінною рисою моделі є виділення двох контурів управління – контуру управління за результативністю та контуру управління за зрілістю. Така структура управління дозволяє контролювати як результати виконання заходів захисту, так і якість (ефективність) досягнення цих результатів. Система управління процесом захисту інформації може розглядатися як дворівнева багатоцільова система, формалізацію якої надано у роботі. Розроблення моделі дало змогу сформулювати задачі управління, які мають розв'язуватися під час прийняття управлінських рішень. Отримані моделі є розвитком теорії захисту інформації у напрямку моделювання управління інформаційною безпекою. Перспективними напрямками досліджень є вирішення задач розроблення узгодженої оцінки результативності захисту інформації у різних ланках управління, а також рівня зрілості процесів захисту інформації, що спираються на сукупність кількісних показників зрілості.

СТРУКТУРА И МОДЕЛЬ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В РАМКАХ ПРОЦЕССНОГО ПОДХОДА

Александр Потий, Анатолий Леншин, Дмитрий Пилипенко
Институт информационных технологий

Предлагается концепция Деминга-Шухарата построения системы управления информационной безопасностью (СУИБ), которая описывается как последовательность: планирование (Plan), осуществление (Do); проверка (контроль) (Check); действие (Act). Модель системы управления, предложенная в работе, может выступать основой для внедрения в практику защиты информации требований стандарта ISO/IEC 27001. Отличительной чертой модели является выделение двух контуров управления - контура управления по результативности и контура управления по зрелости. Такая структура управления позволяет контролировать как результаты выполнения мер защиты, так и качество (эффективность) достижение этих результатов. Система управления процессом защиты информации может рассматриваться как двухуровневая многоцелевая система, формализация которой предоставлена в работе. Разработка модели позволила сформулировать задачи управления, которые должны решаться при принятии управленческих решений. Полученные модели являются развитием теории защиты информации в направлении моделирования управления информационной безопасностью. Перспективными направлениями исследований является решение задач разработки согласованной оценки результативности защиты информации в различных звеньях управления, а также уровня зрелости процессов защиты информации, опирающихся на совокупность количественных показателей зрелости.

STRUCTURE AND MODEL OF INFORMATION SECURITY IN THE PROCESS APPROACH

Alexander Potiy, Anatoly Lenshin, Dmitriy Pilipenko
Institute of information technologies

The concept of the Deming-Shewhart about the construction of information security management system (ISMS), which is described as a sequence: plan (Plan) exercise (Do); checking (supervision) (Check); action (Act).The model management system which is proposed in this paper, may serve as a basis for introducing the practice of information security requirements of ISO/IEC 27001. A distinctive feature of the model is the separation of the two control loops - loop control performance and control loop to maturity. This management structure allows you to control how the results of the protection measures and the quality (efficiency) are achieved these results. The process control system of information security can be viewed as two-level multi-purpose system, the formalization of which is given in item. Development of a model allowed to formulate the control problem that must be addressed in management decisions. The models are an extension of the theory of information security in the direction of modeling for information security management. The potential areas of research are the solving problems of developing a coherent assessment of the effectiveness of information security at various levels of government, as well as the maturity level of information security processes, based on a set of quantitative indicators of maturity.

УДК 621.327.12

СІНЕРГЕТИЧНИЙ ПРОЦЕС ПЕРЕДАЧИ ЕНЕРГІЇ СИГНАЛІВ МОВИ

Володимир Журавльов
Запорізький національний технічний університет

На основі факту імпульсного методу управління центральною нервовою системою фізіологічними органами мовної та слухової системи уперше запропоновані дискретна фізична, психофізична і математична моделі мовного сигналу, які теоретично і експериментально доводять моделюючу функцію кінем – мовоутворюючих рухів органів артикуляції. Розвинена теорія моделювання та обробки мовних сигналів. В основі розроблених і досліджених моделей лежать сінергетичні процеси обміну енергією і інформацією, які базуються на ефекті імпульсної дисипації потенційної енергії повітря легенів в кінетичну енергію дискретних вихрів. Інтервалом стаціонарності сигналів є час нерівноважного стану повітря між двома, наступними один за одним, процесами дисипації енергії. Проведені теоретичні, розрахункові та експериментальні дослідження котрі непрямо (у зв'язку з відсутністю технічних засобів прямих вимірювань енергетичних параметрів сигналів турбулентних вихрів) доводять сінергетичні властивості сигналів мови. Адекватність розроблених моделей експериментально підтверджено порівнянням результатів експериментальних досліджень автора з результатами, опублікованими в наукових виданнях. Теоретично і експериментально доведено, що параметри гучності і висоти тону сигналів мови регулюються центральною нервовою системою за допомогою управління параметрами індексу амплітудної модуляції імпульсів енергії вихрів і їх шпаруватості.

СИНЕРГЕТИЧЕСКИЙ ПРОЦЕСС ПЕРЕДАЧИ ЭНЕРГИИ РЕЧЕВОГО СИГНАЛА

Владимир Журавлёв
Запорожский национальный технический университет

На основе факта импульсного метода управления центральной нервной системой физиологическими речеслуховыми органами впервые предложены дискретная физическая, психофизическая и математическая модель речевого процесса, которые теоретически и экспериментально доказывают модулирующую функцию кинем – речеобразующих движений артикуляционных органов. В основе разработанных и исследованных моделей лежат синергетические процессы обмена энергией и информацией, которые базируются на эффекте импульсной диссипации потенциальной энергии воздуха лёгких в кинетическую энергию дискретных вихрей. Проведены теоретические, расчетные и экспериментальные исследования, косвенно (в связи с отсутствием технических средств для прямых измерений энергетических параметров сигналов турбулентного вихревого потока) доказывающие синергетические свойства речевого сигнала. Интервалом не строгой стационарности моделей является время неравновесного состояния воздуха между двумя, следующими друг за другом, процессами диссипации энергии. Адекватность разработанных моделей экспериментально подтверждена сравнением результатов экспериментальных исследований автора с результатами, опубликованными в научных изданиях. Теоретически и экспериментально доказано, что параметры громкости и высоты тона речевого сигнала регулируются центральной нервной системой посредством управления параметрами индекса амплитудной модуляции импульсов энергии дискретных вихрей и их скважности.

THE SYNERGIC PROCESS OF SPEECH SIGNAL ENERGY TRANSFER

Vladimir Zhuravlev
Zaporozhia national technical university

On the basis of the fact of impulse method of central nervous system administration of physiological speech – hearing organs the discrete physical, psycho-physical and math models of speech process, which theoretically and experimentally proved the modulation function of kinems – speech production movements of articulation organs are suggest for the first time. The synergic process of energy and informational exchange are in base of worked up and

investigated models, which are based on the effect of impulse dissipation of the air in the lungs potential energy to the discrete vortex kinetic energy. Theoretical, calculating and experimental researches are conducted, which indirect (because of absence of technical means for direct measuring of energy parameters of the signal of whirl vortex flow) proves the synergetic characteristics of speech signal. Time of air non-equilibrium condition between two, following each other, energy dissipation processes is the interval of non-strict steady models. Adequacy of the worked out models is experimentally confirmed by comparison of experimental researches with results, published in scientific editions. Theoretically and experimentally proved, that parameters of speech signal volume and tone height are regulated by central nervous system by the means of managing of discrete vortex energy impulse amplitude modulation and their off-duty factor index parameters.

УДК 631.15:006.83

РОЗРОБКА СИСТЕМИ ПРИНЦИПІВ ПОБУДОВИ РАЦІОНАЛЬНОГО ПАКЕТУ НОРМАТИВНОЇ ДОКУМЕНТАЦІЇ СИСТЕМИ УПРАВЛІННЯ ЯКІСТЮ НАУКОВО-ДОСЛІДНИХ УСТАНОВ

Ніна Полякова, Ірина Лазько*

*СВ ІПДОіДН СНУ імені Володимира Даля, *ДП «ІАП»*

Результативність науково-дослідних робіт (НДР) та системи управління якістю (СУЯ) значною мірою залежить від якості перебігу процесу документування. Показано, що пакет нормативної документації СУЯ, побудований з різних її типів та видів, які відрізняються за структурою та складом, формується, як правило, на розсуд розробника. Авторами обґрунтовано доцільність застосування наступних принципів, за якими необхідно формувати раціональний пакет нормативної документації СУЯ НДР: додержання вимог національної системи стандартизації (відповідність призначенню, сумісність, обмеження різноманітності та взаємозамінність); формалізація принципів стандартів серії ДСТУ ISO 9000 та сприяння їх впровадженню; спадкоємність. Запропонована система принципів найбільш повна й адекватна практиці стандартизації науково-дослідних установ (НДУ), узагальнює цю практику та дозволяє поставити її на більш науково обґрунтовану основу. Результативне проведення робіт з побудови раціонального пакету нормативної документації СУЯ НДУ вимагає додержання всієї системи встановлених принципів в комплексі. Невиконання хоча б одного з них веде до розгалуження процесу побудови.

РАЗРАБОТКА СИСТЕМЫ ПРИНЦИПОВ ПОСТРОЕНИЯ РАЦИОНАЛЬНОГО ПАКЕТА НОРМАТИВНОЙ ДОКУМЕНТАЦИИ СИСТЕМЫ УПРАВЛЕНИЕ КАЧЕСТВОМ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИХ УЧРЕЖДЕНИЙ

Нина Полякова, Ирина Лазько*

*СО ИПДОиДО ВНУ имени Владимира Даля, *ГД «ИАП»*

Результативность научно-исследовательских работ (НИР) и системы управления качеством (СУК) в значительной мере зависит от качества хода процесса документирования. Показано, что пакет нормативной документации СУК, построенный из разных ее типов и видов, которые отличаются за структурой и составом, формируется, как правило, на усмотрение разработчика. Авторами обоснованно целесообразность применения следующих принципов, за которыми необходимо формировать рациональный пакет нормативной документации СУК НИР: соответствие требований национальной системы стандартизации (соответствие назначению, совместимость, ограничение разнообразия и взаимозаменяемость); формализация принципов стандартов серии ДСТУ ISO 9000 и содействие их внедрению; преемственность. Предложенная система принципов наиболее полна и адекватна практике стандартизации научно-исследовательских учреждений (НИУ), обобщает эту практику и позволяет поставить ее на более научно обоснованную основу. Результативное проведение работ из построения рационального пакета нормативной документации СУК НИУ требует соблюдения всей системы установленных принципов в комплексе. Невыполнение хотя бы одного из них ведет к разветвлению процесса построения.

DEVELOPMENT OF SYSTEM OF PRINCIPLES OF CONSTRUCTION OF RATIONAL PACKAGE OF NORMATIVE DOCUMENT OF SYSTEM MANAGEMENT BY QUALITY OF RESEARCH ESTABLISHMENTS

Nina Polyakova, Iryna Laz'ko*
*NS IADE DT ENU of the name of Volodymyr Dalya, *SE of «INP»*

Effectiveness of research works (RW) and control system by quality (CSQ) to a great extent depends on quality of motion of process of documenting. It is rotined that the package of normative document of CSQ, built from its different types and kinds which differ after a structure and composition, is formed, as a rule, at discretion of developer. By authors grounded expedience applications of next principles, after which it is necessary to form the rational package of normative document of CSQ of RW: inhibition of requirements of the national system of standardization (accordance setting, compatibility, limitation of variety and interchangeability); formalization of principles of standards of series ДСТУ ISO 9000 but assistance their introduction; succession. The offered system of principles is most full and adequate practice of standardization of RW, summarizes this practice and allows to put it on the more scientifically grounded basis. The effective leadthrough of works from the construction of rational package of normative document of CSQ RW requires inhibition of all system of the set principles in a complex. Non-fulfillment even conduces one of them to the fork of process constructions.

УДК 343.159.5

ВІДМОВА У ВІДШКОДУВАННІ ШКОДИ, ЗАВДАНОЇ ОСОБІ ОРГАНАМИ ДОСУДОВОГО РОЗСЛІДУВАННЯ, ПРОКУРАТУРИ І СУДУ

Вероніка Горєлова
Університет економіки та права «КРОК»

Мають місце в Україні непоодинокі випадки порушень прав громадян органами досудового слідства, прокуратури та суду, що завдали значної шкоди здоров'ю, честі, діловій репутації особи, але вдало вклались в межі норм, що позбавляють особу права на компенсацію. Метою роботи є дослідження природи самообмови як підстави, що позбавляє особу права на відшкодування шкоди в кримінальному судочинстві, а також запропонувати зміни до діючого законодавства з урахуванням норм міжнародного права. Відмова у відшкодуванні шкоди внаслідок самообмови виявляється вимогою невідповідною щодо справедливості, компенсації шкоди і в залежності від справи та характеру дій особи, що відносяться до самообмови, можливі на розсуд суду такі дії: компенсація, реституція або соціальна допомога.

Встановлюючи самообмову підставою, що позбавляє особу права на відшкодування шкоди, держава не створила надійного та діючого механізму захисту людини від існуючого беззаконня. Тому доцільно виключити ч.4 ст.1176 Цивільного кодексу України, що визначає самообмову підставою, яка позбавляє права особи на відшкодування завданої їй шкоди в кримінальному судочинстві.

ОТКАЗ В ВОЗМЕЩЕНИИ УЩЕРБА, НАНЕСЕННОГО ЛИЦУ ОРГАНАМИ ДОСУДЕБНОГО РАССЛЕДОВАНИЯ, ПРОКУРАТУРЫ И СУДА

Вероника Горелова
Университет экономики и права «ШАГ»

Имеют место в Украине неодиночные случаи нарушений прав граждан органами досудебного следствия, прокуратуры и суда, что нанесли значительный вред здоровью, чести, деловой репутации лица, но удачно уложились в пределы норм, которые лишают лицо права на компенсацию. Целью работы является исследование природы самооговора как основания, которое лишает лицо права на возмещение вреда в криминальном судопроизводстве, а также предложить изменения к действующему законодательству с учетом норм международного права. Отказ в возмещении вреда в результате самооговора оказывается

требованием несоответствующим относительно справедливости, компенсации вреда и в зависимости от дела и характера действий лица, которые относятся к самооговору, возможные на усмотрение суда такие действия: компенсация, реституция или социальная помощь.

Устанавливая самооговор основанием, которое лишает лицо права на возмещение вреда, государство не создало надежный и действующий механизм защиты человека от существующего беззакония. Поэтому целесообразно исключить ч.4 ст.1176 Гражданского кодекса Украины, которая определяет самооговор основанием, которое лишает права личности на возмещение нанесенного ей вреда в криминальном судопроизводстве.

A REFUSE IS IN COMPENSATION OF SHKODI, INFLICTED PERSON BY ORGANS OF PRE-TRIAL INVESTIGATION, OFFICE OF PUBLIC PROSECUTOR AND COURT

Veronica Gorelova is
University of economy and right «STEP»

Take place in Ukraine unsingle cases of violations of rights for citizens by the organs of pre-trial investigation, office of public prosecutor and court, that inflicted considerable harm a health, honour, business reputation of person, but successfully laid in limits norms which deprive the face of right on indemnification. The purpose of work is research of nature of self-incrimination, as foundation which deprives the face of right on the compensation of harm in the criminal legal proceeding, and also to offer changes to the current legislation taking into account the norms of international law. A refuse in the compensation of harm as a result of self-incrimination appears a requirement incongruous in relation to justice, indemnifications of harm and depending on business and character of actions of person, which behave to self-incrimination, possible at discretion of court such actions: indemnification, restituciya or social help.

Setting self-incrimination foundation which deprives the face of right on the compensation of harm, the state did not create the reliable and operating mechanism of defence of man from existent lawlessness. It is Therefore expedient to eliminate ch.4 st.1176 of the Civil code of Ukraine, which determines self-incrimination foundation which disentitles personality on the compensation of the harm inflicted it in the criminal legal proceeding.

УДК 004.056

РОЗСЛІДУВАННЯ ІНЦИДЕНТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Юрій Копитін
КП «Обласний інформаційно-аналітичний центр»

Найбільш складним питанням в процесі управління інцидентами інформаційної безпеки (ІБ) є розслідування інцидентів безпеки. Процес розслідування випадків порушення політики безпеки, небезпечних та непередбачених подій, здійснення аналізу причин, що призвели до них, супроводження банку даних таких подій є невід'ємною функцією служби захисту інформації під час експлуатації комплексної системи захисту, регламентується великою кількістю нормативних документів та рекомендацій (ISO/IEC 27001, ISO/IEC 27002, ISO/IEC TR 18044, CMU/SEI-2004-TR-015, NIST SP 800-61, NIST SP 800-12, ITU-T E.409, RFC 2350), передбачає чотири етапи: збір; дослідження; аналіз; відображення, а на думку автора до них ще слід додати етап оцінювання області розслідування інцидентів ІБ.

Запропонований в роботі підхід дозволить відтворити образ потенційного порушника, зрозуміти про причини та процес настання інциденту, сформувати загальні представлення про процес розслідування інцидентів, а запровадження організаціями процесу розслідування інцидентів ІБ дозволить підвищити рівень ІБ, підсилити увагу до попередження інцидентів шляхом віднаходження винних у його виникненні та його причин, знизити негативні наслідки на бізнес-процеси організації, скорегувати політику інформаційної безпеки організації.

РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Юрий Копытин
КП «Областной информационно-аналитический центр»

Наиболее сложным вопросом в процессе управления инцидентами информационной безопасности (ИБ) является расследование инцидентов безопасности. Процесс расследования случаев нарушения политики безопасности, опасных и непредвиденных событий, осуществления анализа причин, которые привели к ним, сопровождение банка данных таких событий является неотъемлемой функцией службы защиты информации во время эксплуатации комплексной системы защиты, регламентируется большим количеством нормативных документов и рекомендаций (ISO/IEC 27001, ISO/IEC 27002, ISO/IEC TR 18044, CMU/SEI-2004-TR-015, NIST SP 800-61, NIST SP 800-12, ITU-T E.409, RFC 2350), предусматривает четыре этапа: сбор; исследование; анализ; отображение, а по мнению автора к ним еще следует прибавить этап оценивания области расследования инцидентов ИБ.

Предложенный в работе подход позволит воспроизвести образ потенциального нарушителя, понять о причинах и процессе наступления инцидента, сформировать общие представления о процессе расследования инцидентов, а внедрение организациями процесса расследования инцидентов ИБ позволит повысить уровень ИБ, усилить внимание к предупреждению инцидентов путем отыскания виновных в его возникновении и его причин, снизить негативные последствия на бизнес-процессы организации, скорректировать политику информационной безопасности организации.

INVESTIGATION OF INCIDENTS OF INFORMATIVE SAFETY

Yuriy Kopytin
KE «Regional informaciyno-analitichniy center»

A most stumper in the process of management of informative safety (IB) incidents investigation of incidents of safety is. The process of investigation of cases of violation of policy of safety, hazardous and unforeseen occurrences, realization of analysis of reasons which resulted in them, accompaniment of bank of data of such events is the inalienable function of service of priv during exploitation of the complex system of defence, is regulated plenty of normative documents and recommendations (ISO/IEC 27001, ISO/IEC 27002, ISO/IEC TR 18044, CMU/SEI-2004-TR-015, NIST SP 800-61, NIST SP 800-12, ITU-T E.409, RFC 2350), foresees four stages: collection; research; analysis; reflection, and in opinion of author to them yet it follows to add the stage of evaluation of area of investigation of incidents of IB.

Offered approach in-process will allow to reproduce appearance of potential violator, understand about reasons and process of offensive of incident to form the general pictures of process of investigation of incidents, and introduction organizations of process of investigation of incidents of IB will allow to promote the level of IB, strengthen attention to warning of incidents by searching for of guilty in his origin and his reasons, reduce negative consequences on biznes-procesi of organization, to correct the policy of informative safety of organization.

УДК 691.321

МЕТОДИКА ПЕРЕВІРКИ НЕЗАЛЕЖНОСТІ СТАТИСТИЧНИХ ТЕСТІВ ПРИ НЕВІДОМИХ СТАТИСТИЧНИХ ВЛАСТИВОСТЯХ ГЕНЕРАТОРА ПОСЛІДОВНОСТЕЙ

Леонід Скрипник, Людмила Ковальчук, Віктор Бездітний*
*Інститут спеціального зв'язку та захисту інформації НТУУ «КПІ»,*ТОВ «НВФ «УНІС»*

В роботі запропоновано методику перевірки незалежності статистичних тестів з використанням генераторів послідовностей випадкових величин з невідомими статистичними характеристиками.

При виборі шаблону, який складається з усіх одиниць, ця методика повністю співпадає з методикою Л. Ковальчук щодо перевірки незалежності статистичних тестів (МПНСТ), призначених для оцінки криптографічних якостей генераторів випадкових послідовностей. При застосуванні запропонованої методики до тестів, рівень значимості яких співпадає з ймовірністю їх проходження випадковою рівноімовірною послідовністю, результати тестування співпадатимуть з результатами застосування методики МПНСТ. Узагальнення дозволяє уникнути отримання тривіальних результатів тестування.

МЕТОДИКА ПРОВЕРКИ НЕЗАВИСИМОСТИ СТАТИСТИЧЕСКИХ ТЕСТОВ ПРИ НЕИЗВЕСТНЫХ СТАТИСТИЧЕСКИХ СВОЙСТВАХ ГЕНЕРАТОРА ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Леонид Скрипник, Людмила Ковальчук, Виктор Бездетный*
*Институт специальной связи и защиты информации НТУУ «КПИ»,*ООО «НПФ «УНИС»*

В роботе предложена методика проверки независимости статистических тестов с использованием генераторов последовательностей случайных величин с неизвестными статистическими характеристиками.

При виборе шаблона, котрый содержит все единицы, эта методика полностью совпадает с методикою Л. Ковальчук относительно проверки независимости статистических тестов (МПНСТ), предназначенных для оценки криптографических свойств генераторов случайных последовательностей. При применении предложенной методики к тестам, уровень значимости которых совпадает с вероятностью их прохождения случайной равновероятной последовательностью, результаты тестирования будут совпадать с результатами использования методики МПНСТ. Обобщение позволяет исключить получение тривиальных результатов тестирования.

METHOD OF VERIFICATION OF INDEPENDENCE STATISTICAL TESTS WITH UNKNOWN STATISTICAL PROPERTIES OF SEQUENCE GENERATOR

Leonid Skripnik,Ludmila Kovalchuk,Viktor Bezdetnuy
*Institute of Special Communications and Information Security of NTU "KPI", * SPC "UNIS"*

The technique of checking the independence of statistical tests using the generators of sequences of random variables with unknown statistical characteristics are shown in the work.

When you select a pattern,which includes all units,this technique is identical to the L.Kovalchuk's procedure regarding checking the independence of statistical tests (MPNST),designed to evaluate the cryptographic properties of random sequence generators.In applying the proposed technique to the tests, the significance level which coincides with the probability of a random equiprobable sequence,the results of tests will coincide with the results of the use of techniques MPNST. Generalization avoids the trivial getting test results.

УДК: 004.056.5

ВИРІШЕННЯ ПРОБЛЕМИ ПОГІРШЕННЯ ЯКОСТІ ВЕКТОРНИХ ЗОБРАЖЕНЬ ПРИ ВБУДОВУВАННІ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ

Василь Карпінець, Юрій Яремчук
Вінницький національний технічний університет

У роботі запропоновано стеганографічний метод вбудовування цифрових водяних знаків (ЦВЗ) у векторні зображення, який для виявлення ЦВЗ, окрім секретного ключа, не вимагає ні знання оригінального зображення, ні вбудованого ЦВЗ. Особливістю методу є використання двовимірного дискретного косинус перетворення (ДКП) для матриць розміром 8x8 та зміна в них високочастотних (ВЧ) коефіцієнтів. Суть зміни полягає у заміні значень ВЧ-коефіцієнтів на середньоарифметичне значення цих коефіцієнтів, збільшене або зменшене на невелику величину залежно від біту ЦВЗ.

Проведено аналіз методу з точки зору впливу ЦВЗ на якість зображення, який показав, що запропонований метод дозволяє вирішити проблему погіршення якості зображення внаслідок вбудовування ЦВЗ.

Проведено порівняльний аналіз використання двовимірного та одновимірного ДКП для захисту векторних зображень на прикладі частини векторної карти. Аналіз показав, що використання двовимірного ДКП порівняно з одновимірним дозволяє зменшити негативний вплив ЦВЗ на якість зображення приблизно у 8 разів.

Проведено аналіз стійкості запропонованого методу з точки зору стійкості векторного зображення до активних атак, які спрямовані на знищення чи підміну ЦВЗ. Запропонований метод, як і існуючі методи, має достатній рівень стійкості до найпоширеніших видів стеганографічних атак.

РЕШЕНИЕ ПРОБЛЕМЫ УХУДШЕНИЯ КАЧЕСТВА ВЕКТОРНЫХ ИЗОБРАЖЕНИЙ ПРИ ВСТРАИВАНИИ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ

Василий Карпинец, Юрий Яремчук
Винницкий национальный технический университет

В работе предложен стеганографический метод встраивания цифровых водяных знаков (ЦВЗ) в векторные изображения, который для выявления ЦВЗ, кроме секретного ключа, не требует ни знания оригинального изображения, ни встроенного ЦВЗ. Особенностью метода является использование двумерного дискретного косинус преобразования (ДКП) для матриц размером 8x8 и изменение в них высокочастотных (ВЧ) коэффициентов. Суть изменения состоит в замене значений ВЧ-коэффициентов на среднеарифметическое значение этих коэффициентов, увеличенное или уменьшенное на небольшую величину в зависимости от бита ЦВЗ.

Проведен анализ метода с точки зрения влияния ЦВЗ на качество изображения, который показал, что предложенный метод позволяет решить проблему ухудшения качества изображения вследствие встраивания ЦВЗ.

Проведен сравнительный анализ использования двумерного и одномерного ДКП для защиты векторных изображений на примере части векторной карты. Анализ показал, что использование двумерного ДКП по сравнению с одномерным позволяет уменьшить негативное влияние ЦВЗ на изображение примерно в 8 раз.

Проведен анализ устойчивости предложенного метода с точки зрения устойчивости векторного изображения к активным атакам, которые направлены на уничтожение или подмену ЦВЗ. Предложенный метод, как и существующие методы, имеет достаточный уровень устойчивости к распространенным видам стеганографических атак.

SOLVING PROBLEMS WORSENING QUALITY VECTOR IMAGES WHEN EMBEDDING DIGITAL WATERMARKS

Vasyl Karpinets, Yuriy Yaremchuk
Vinnytsia National Technical University

The paper proposed steganographic method of embedding digital watermarks into vector images, which for the watermark detection, except the secret key requires no knowledge of the original image, or embedded watermark. The feature of the method is to use two-dimensional discrete cosine transform (DCT) for the 8x8 matrix and a change in their high-frequency (HF) coefficients. The essence of the changes is to replace the values of the HF-coefficients at an average mean of these coefficients increased or decreased by a small amount depending on the watermark bit.

The analysis method in terms of impact on the quality of watermark image, which showed that the proposed method resolves the problem of image quality deterioration due to watermark embedding.

A comparative analysis of two-dimensional and one-dimensional DCT to protect the vector images on the example of vector map. Analysis showed that the use of two-dimensional DCT compared with one-dimensional reduce the negative impact of watermark image quality at about 8 times.

The analysis of stability of the proposed method in terms of vector images to active attacks aimed at destroying or substitution watermark. The proposed method, as existing methods has a sufficient level of resistance to most common types of steganographic attacks.

УДК 681.3

КРИТЕРІЇ І МЕТОДОЛОГІЯ ОЦІНКИ ЕФЕКТИВНОСТІ ОРГАНИЗАЦІЇ І ПОБУДОВИ АРХИТЕКТУРИ ЗАХИЩЕНИХ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

В'ячеслав Шорошев
ДНДІ МВС України

Одним із основних методологічних шляхів пошуку рішення проблеми організації та побудови архітектури захищених комп'ютерних систем (ЗКС) визначається використання методів концептуальної евристики. При організації і побудові архітектури ЗКС має бути, насамперед, пріоритетність вимог чинних вітчизняних нормативно-правових документів з урахуванням міжнародного досвіду. Запропонована концептуальна модель політики побудови архітектури ЗКС з нормуванням її інформаційної безпеки стандартизованими рівнями, а також за критерієм рейтинг профілю - ризик безпеки - рівень обмежень видів інформаційної діяльності - вартість. Зміни цих факторів формалізуються їх стандартизованими ДСТУ рівнями (Layer), а саме – захищеність інформації регламентується двома рівнями – необхідний та максимальний, види інформаційної діяльності - допустимим, заданим та мінімальним рівнями обмежень, рівень захисту інформації - необхідним і максимальним рівнями, витрати на захищеність інформації - мінімальним, допустимим та необхідним рівнями. За результатами досліджень визначаються такі концептуальні, найбільш ефективні і результативні шляхи *(концепт-правила)* рішення проблеми підвищення ефективності за рахунок формування відповідної (адаптивної) політики побудови та організації архітектури ЗКС. Пропонується визначати та реалізовувати в *політиці безпеки архітектури* десять найбільш результативних концептуальних чинників (*концепт-правил*) аналогічно методології міжнародного стандарту ISO 17799 щодо десяти принципів управління інформаційною безпекою та десяти ключових засобів її аудиту. Ефективність обраної політики побудови архітектури ЗКС слід оцінювати в залежності від пріоритетності обраного кінцевого результату - або ефективне нормування рівнів, або ефективний адаптивний загрозам функціональний профіль за підкласами конфіденційності К, цілісності Ц, доступності Д та їх сполучень КЦ, КД, ЦД, КЦД, або вартість. Пропонується обрати найбільш пріоритетним показник стійкості захищеності всієї ЗКС від несанкціонованого доступу. Для практичної реалізації запропонованих методичних рекомендацій доцільно створення Національного електронного каталогу профілів захищеності інформації АФП-Т в АС усіх класів і підкласів, адаптивних загрозам, замість визначеної і неповної низки регламентованих базових профілів захищеності в чинних НД ТЗІ 2.5-005-99 (всього 90 профілів з їх повної низки 740360298600).

КРИТЕРИИ И МЕТОДОЛОГИЯ ОЦЕНКИ ЭФФЕКТИВНОСТИ ОРГАНИЗАЦИИ И ПОСТРОЕНИЯ АРХИТЕКТУРЫ ЗАЩИЩЕННЫХ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Вячеслав Шорошев
ГНИИ МВД Украины

Одним из основных методологических путей поиска решения проблемы организации и построения архитектуры защищенных компьютерных систем (ЗКС) определяется использование методов концептуальной эвристики. При организации и построении архитектуры ЗКС должна быть, прежде всего, приоритетность требований действующих отечественных нормативно-правовых документов с учетом международного опыта. Предложена концептуальная модель политики построения архитектуры ЗКС с нормированием ее информационной безопасности стандартизированными уровнями, а также по критерию рейтинг профиля - риск безопасности - уровень ограничений видов информационной деятельности - стоимость. Изменения этих факторов формализуются их стандартизированными ДСТУ уровнями (Layer), а именно – защищенность информации регламентируется двумя уровнями - необходимый и максимальный, виды информационной деятельности - допустимым, заданным и минимальным уровнями ограничений, уровень защиты информации - необходимым и максимальным уровнями, расходы на защищенность информации - минимальным, допустимым и необходимым уровнями. По результатам исследований определяются такие концептуальные, наиболее эффективные и результативные пути (концепт-правила)

решения проблемы повышения эффективности за счет формирования соответствующей (адаптивной) политики построения и организации архитектуры ЗКС. Предлагается определять и реализовывать в политике безопасности архитектуры десять наиболее результативных концептуальных факторов (концепт-правил) аналогично методологии международного стандарта ISO 17799 по десяти принципах управления информационной безопасностью и десяти ключевых средств ее аудита. Эффективность избранной политики построения архитектуры ЗКС следует оценивать в зависимости от приоритетности выбранного конечного результата - либо эффективное нормирование уровней, или эффективный адаптивный угрозам функциональный профиль по подклассам конфиденциальности К, целостности Ц, доступности Д и их сочетаний КЦ, КД, СД, КЦД, или стоимость. Предлагается выбрать наиболее приоритетным показатель устойчивости защищенности всей ЗКС от несанкционированного доступа. Для практической реализации предложеных методических рекомендаций целесообразно создание Национального електронного каталога профилей защищенности информации АФП-Т в АС всех классов и подклассов адаптивных угроз, вместо определенного и неполного ряда регламентированных базовых профилей защищенности в действующих НД ТЗИ 2.5-005-99 (всего 90 профилей с их полного ряда 740360298600).

THE CRITERIA AND METHODOLOGY TO ASSESS THE EFFECTIVENESS OF THE ORGANIZATION AND CONSTRUCTION OF ARCHITECTURE-OF THE PROTECTED INFORMATION AND TELECOMMUNICATIONS SYSTEMS

V'yacheslav Shoroshim
SSRI MIAof Ukraine

One of the major methodological ways to find a solution to the problem of organizing and building architecture of a secure Computing Systems (SCA) is determined using the methods of conceptual heuristics. When organizing and constructing the architecture of SCA should be, above all, the priority requirements of existing domestic legal and regulatory documents in the light of international experience. We propose a conceptual model of policy construction SCA architecture with a valuation of its information security standardized levels, as well as by the criterion of rate profile - security risk - the level of restrictions on information activities - the cost. Changes in these factors are formalized their standardized DSTU levels (Layer), namely the security of information is regulated by two levels - the necessary and the maximum, the types of information activity - a valid, given the restrictions and minimum levels, the level of information security - a necessary and maximum levels, spending on information security -minimum, a valid and necessary levels. According to the results of the study is such conceptual, the most effective and efficient way (a concept-rule) address the efficiency through the formation of appropriate (adaptive) policy of building and organizing architecture PCL. It is proposed to define and implement a security policy architecture of the ten most successful conceptual factors (the concept of rules) is similar to the methodology of the international standard ISO 17799 on the ten principles of information security management and the ten key tools of audit.The effectiveness of the chosen policy of building architecture PCL should be evaluated according to the priority of the selected outcome - either an effective valuation levels, or an effective adaptive threats functional profile of subclasses to privacy, integrity, C, D accessibility and their combinations CC, CD, CD, RACs, or the cost. Asked to select the highest priority indicator of stability security throughout ZKS from unauthorized access. For the practical implementation of the proposals methodical reccomandations appropriate for a National directory of profiles electronically protected information AFT-T in AS all classes and subclasses of adaptive threats,instead of a specific variety of regulated and incomplete baseline profile of protection in the exisiting ND TZI 2.5-005-99 (of 90 profiles from the total number 740360298600).

УДК 681.3

НОВА КОНЦЕПЦІЯ ПОЛІТИКИ ПОБУДОВИ ТА ОРГАНІЗАЦІЇ АРХІТЕКТУРИ ЗАХИЩЕНОЇ КОМП'ЮТЕРНОЇ СИСТЕМИ З НОРМУВАННЯМ РІВНІВ ЇЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Олександр Дмитренко
УТЗІ ДДЗР МВС УКРАЇНИ

Пропонується нова Концепція політики побудови архітектури захищеної комп'ютерної системи (ЗКС) з

нормуванням рівнів її інформаційної безпеки за критерієм рейтинг профілю - ризик безпеки - рівень обмежень видів інформаційної діяльності - вартість. Як основний механізм пошуку рішення щодо організації і побудови архітектури ЗКС пропонується використовувати методи концептуальної евристики. Вони передбачають визначення множини таких шляхів рішення проблемної задачі, серед яких з достатньою імовірністю є і найбільш результативний шлях з використанням функціональних профілів, адаптивних загрозам (АФП).

Новизна Концепції політики побудови та організації архітектури захищених комп'ютерних систем полягає в наступних концептуальних чинниках: пропонується визначати найбільш пріоритетною і *комплексною* послугою безпеки адаптивний загрозам НСД функціональний профіль захищеності інформації за моделлю політики побудови архітектури ЗКС з нормуванням рівнів рейтингу профілю, гарантій безпеки, обмежень видів інформаційної діяльності, вартості. Завдяки цьому в роботі дістала подальшого розвитку теорія технічного захисту інформації щодо необхідності обов'язкового використання державними експертами при оцінюванні не тільки функціональних послуг безпеки, але і їх рівня гарантій не тільки за запропонованими автором методичними вказівками, але і за методичними вказівками щодо оцінювання функціональних послуг безпеки, адаптивних загрозам. Запропонована Концепція може бути використана для формування та обґрунтування положень політики безпеки архітектури захищених комп'ютерних систем за критерієм ризик безпеки-гарантія безпеки-вид інформаційної діяльності-вартість.

НОВАЯ КОНЦЕПЦИЯ ПОЛИТИКИ ПОСТРОЕНИЯ И ОРГАНИЗАЦИИ АРХИТЕКТУРЫ ЗАЩИЩЕННОЙ КОМПЬЮТЕРНОЙ СИСТЕМЫ С НОРМИРОВАНИЕМ УРОВНЕЙ ЕЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Александр Дмитренко
УТЗИ ДДЗР МВД УКРАИНЫ

Предлагается новая Концепция политики построения архитектуры защищенной компьютерной системы (ЗКС) с нормированием уровней ее информационной безопасности по критерию рейтинг профиля - риск безопасности - уровень ограничений видов информационной деятельности - стоимость. Как основной механизм поиска решения по организации и построении архитектуры ЗКС предлагается использовать методы концептуальной эвристики. Они предусматривают определение множества таких путей решения проблемной задачи, среди которых с достаточной вероятностью является и наиболее результативный путь с использованием функциональных профилей, адаптивных угрозам (АФП).

Новизна Концепции политики построения и организации архитектуры защищенных компьютерных систем заключается в следующих концептуальных факторах: предлагается определять наиболее приоритетную и комплексную услугу безопасности адаптивный угрозам НСД функциональный профиль защищенности информации по модели политики построения архитектуры ЗКС с нормированием уровней рейтинга профиля, гарантий безопасности, ограничений видов информационной деятельности, стоимости. Благодаря этому в работе получила дальнейшее развитие теория технической защиты информации относительно необходимости обязательного использования государственными экспертами при оценке не только функциональных услуг безопасности, но и их уровня гарантий не только по предложенным автором методическим указаниям, но и по методическим указаниям по оценке функциональных услуг безопасности, адаптивных угрозам. Предложенная Концепция может быть использована для формирования и обоснования положений политики безопасности архитектуры защищенных компьютерных систем по критерию риск безопасности-гарантия безопасности - вид информационной деятельности - стоимость.

THE NEW CONCEPT OF POLICY OF CONSTRUCTION AND ORGANIZATION OF ARCHITECTURE OF PROTECTED COMPUTER SYSTEM WITH A VALUATION LEVEL OF INFORMATION SECURITY

Alexander Dmitrenko
UTZI DDZR The Ministry of Internal Affairs of Ukraine

A new concept of policy building of a secure computer architecture (SCA) with a valuation levels of information security according to the criterion rating profile - security risk - the level of restrictions on information activities - the cost. As the main mechanism for finding solutions to the organization and construction of architecture SCA are encouraged to use methods of conceptual heuristics. They provide a definition of the set of solutions to problem tasks, among them with sufficient probability is the most effective way of using functional profiles, adaptive threats (AFP).

The novelty of the Concept of policy construction and organization of protected computer systems architecture consists of the following conceptual factors: it is proposed to determine the highest priority and integrated services to the adaptive security threats to tamper functional profile of information security policy model building architecture with a valuation levels SCA rating profile, security assurances, limitations of types of information activity, value. Through this work was further developed the theory of technical protection of information regarding the need to mandate the use of government experts in assessing not only the functional security services, but also their level of guarantees not only the author of the proposed guidelines, but also for guidance in assessing the functional security services, adaptive threats. The proposed concept can be used for the formation and justification of the provisiond of security policy architecture protected computer systems by the criterion of the security risk ia s guarantee of security –the kind of information activity – the cost.

УДК 004.056: 004.942

СИСТЕМНИЙ ПІДХІД У ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Віталій Носов
Харківський національний університет внутрішніх справ

Запропоновано використання системного підходу у забезпеченні інформаційної безпеки корпоративних інформаційно-телекомунікаційних систем. Представлена формальна модель і ключові характеристики мережі взаємин комплексної системи захисту інформації у складі узагальненої інформаційно-телекомунікаційної системи.

СИСТЕМНЫЙ ПОДХОД ПРИ ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Виталий Носов
Харьковский национальный университет внутренних дел

Предложено использование системного подхода в обеспечении информационной безопасности корпоративных информационно-телекоммуникационных систем. Представлена формальная модель и ключевые характеристики сети взаимоотношений комплексной системы защиты информации в составе обобщенной информационно-телекоммуникационной системы.

APPROACH SYSTEMS TO INFORMATION SECURITY

Vitaliy Nosov
Kharkov national university of internal affairs

Approach Systems to information security of corporate information and telecommunication systems is proposed. The formal model and key characteristics of network relationships Information Security Complex System consisting in a Common Information and Telecommunication System is represented.

УДК 621.395

МОДЕЛЬ ОБСЛУГОВУВАННЯ ЗАЯВОК НА ЕТАПІ ДОСТУПУ ДО ЦЕНТРУ ІНТЕЛЕКТУАЛЬНИХ ПОСЛУГ

Дмитро Могилевич, Валерій Правило, Олексій Бреус
ВІТІ НТУУ "КПІ"

Автори розглядають центр інтелектуальних послуг (ЦІП), як архітектурну концепцію, що передбачає виділення служб вторинних мереж, які відповідають за надання послуг користувачам, як окремий елемент автоматизованої комутованої мережі зв'язку (МЗ). Функціонування ЦІП розглядається без урахування процесів, що протікають в мережі, складовою частиною якої і є ЦІП.

Питанням обслуговування заявок на надання доступу користувачів до ЦІП приділяється недостатня увага. Тому в статті розглядаються моделі обслуговування заявок на етапі доступу користувачів до ЦІП та аналізуються математичні вирази для розрахунку інтенсивності потоку навантажень, що надходить та обслуговуються. Розглянуті особливості основних груп моделей мереж: морфологічні моделі і моделі функціонування. Морфологічні моделі описують мережу зв'язку або її окремі складові з точки зору її складу і взаємозв'язку між елементами.

За результатами аналізу автоматизованої комутованої мережі зв'язку розроблена морфологічна модель транспортної мережі, що забезпечує доступ користувачів інтелектуальних послуг до ЦІП. Проведений аналіз інформаційних потоків в напрямку зв'язку від кінцевих комутаційних станцій МЗ до центрів інтелектуальних послуг. Розроблені п'ять моделей доступу користувачів до центрів інтелектуальних послуг. Визначені: передумови подальшого вивчення даної задачі; тракт проходження заявки при попаданні в ЦІП; процедури обслуговування заявок в ЦІП; процес взаємодії між складовими інтелектуальної мережі зв'язку.

МОДЕЛЬ ОБСЛУЖИВАНИЯ ЗАЯВОК НА ЭТАПЕ ДОСТУПА К ЦЕНТРУ ИНТЕЛЛЛЕКТУАЛЬНЫХ УСЛУГ

Дмитрий Могилевич, Валерий Правило, Алексей Бреус
ВИТИ НТУУ "КПИ"

Авторы рассматривают центр интеллектуальных услуг (ЦИУ), как архитектурную концепцию, которая предусматривает выделение служб вторичных сетей, которые отвечают за предоставление услуг пользователям, как отдельный элемент автоматизированной коммутированной сети связи (СС). Функционирование ЦИУ рассматривается без учета процессов, которые протекают в сети, составной частью которой и является ЦИУ.

Вопросам обслуживания заявок на предоставление доступа пользователей к ЦИУ уделяется недостаточное внимание. Поэтому в статье рассматриваются модели обслуживания заявок на этапе доступа пользователей к ЦИУ и анализируются математические выражения для расчета интенсивности потока нагрузок, который поступает и обслуживается. Рассмотренные особенности основных групп моделей сетей: морфологические модели и модели функционирования. Морфологические модели описывают сеть связи или ее отдельные составляющие с точки зрения ее состава и взаимосвязи между элементами.

За результатами анализа автоматизированной коммутированной сети связи разработана морфологическая модель транспортной сети, которая обеспечивает доступ пользователей интеллектуальных услуг к ЦИУ. Проведен анализ информационных потоков в направлении связи от конечных коммутационных станций СС к центрам интеллектуальных услуг. Разработаны пять моделей доступа пользователей к центрам интеллектуальных услуг. Определены: предпосылки последующего изучения данной задачи; тракт прохождения заявки при попадании в ЦИУ; процедуры обслуживания заявок в ЦИУ; процесс взаимодействия между составляющими интеллектуальной сети связи.

MODEL SERVICE APPLICATIONS FOR ACCESS TO THE CENTER STAGE OF THE INTELLIGENT SERVICE

Dmitriy Mogilevich, Valery Rule, Alexei Breus
Viti KPI

The authors consider the center of intellectual services (CIS), as an architectural concept, which will provide the services of secondary networks, which are responsible for providing services to users as a separate element of the automated commutated networks (ACN). Functioning CIS considered without regard to the processes that occur in the network, part of which is CIS.

Issue service requests for users to access CIS inadequate attention. Therefore, the article examines the models of service requests at the stage of user access to CIS and analyzed by mathematical expressions to calculate the intensity of the flow stress, which is received and serviced. Considered features of major groups of models of networks:

morphological model and operating model. Morphological models describe the communication network or its individual components in terms of its composition and the relationship between the elements.

The results of automated analysis of commutated networks developed morphological model of the transport network that provides access to intelligent services CIS. The analysis of information flows in the direction of communication from the end switching stations ACN to the centers of intellectual services. Developed five models of users' access to the centers of intellectual services. Identified: background further study of this problem; tract passing the application if it enters the CIS; maintenance procedures CIS applications, the process of interaction between the components of intelligent network

УДК 638.235.231

ЗНАЧИМІСТЬ РІВНЯ ПОТУЖНОСТІ ЗОНДУЮЧОГО СИГНАЛУ У НЕЛІНІЙНІЙ РАДІОЛОКАЦІЇ

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

Об'єктом дослідження в роботі є технічні пристрої несанкціонованого доступу до інформації, імітатори закладних пристроїв для нелінійних радіолокаторів, нелінійні радіолокатори. Мета роботи, це експериментальне встановлення основних чинників, що впливають на ефективність демаскуючої дії зондуючого випромінювання нелінійних радіолокаторів на напівпровідникові елементи з нелінійними вольт-амперними характеристиками; розробка гіпотези щодо фізики процесів у напівпровідникових структурах при дії відносно потужного НВЧ випромінювання від нелінійного радіолокатора. Одержані результати та їх новизна: експериментально встановлені вагомості основних чинників, що впливають на ефективність демаскуючої дії зондуючого випромінювання нелінійних радіолокаторів на напівпровідникові елементи з нелінійними вольт-амперними характеристиками; розроблено гіпотези щодо фізики процесів у напівпровідникових структурах при дії відносно потужного НВЧ випромінювання від нелінійного радіолокатора.

ЗНАЧИМОСТЬ УРОВНЯ МОЩНОСТИ ЗОНДИРУЮЩЕГО СИГНАЛА В НЕЛИНЕЙНОЙ РАДИОЛОКАЦИИ

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

Объектом исследования в работе является технические устройства несанкционированного доступа к информации, имитаторы закладных устройств для нелинейных радиолокаторов, нелинейные радиолокаторы. Цель работы, это экспериментальное определение основных факторов, которые влияют на эффективность демаскирующего действия зондирующего излучения на полупроводниковые элементы с нелинейными вольт-амперными характеристиками в нелинейной радиолокации; разработка гипотезы относительно физики процессов в полупроводниковых структурах при действии достаточно мощного СВЧ излучения нелинейного радиолокатора. Полученные результаты и их новизна: экспериментально определены основные факторы, которые влияют на эффективность демаскирующего действия зондирующего излучения нелинейных радиолокаторов на полупроводниковые элементы с нелинейными вольт-амперными характеристиками; разработана гипотеза относительно физики процессов в полупроводниковых структурах при действии достаточно мощного СВЧ излучения нелинейного радиолокатора.

MEANINGFULNESS OF POWER-LEVEL SOUNDING SIGNAL IS IN NONLINEAR RADIO-LOCATION

Max Zinchenko, George Zin'kovskiy, Michael Prokof'ev
Research center of technical protection of information "TESIS" National Technical University of Ukraine "Kyiv Polytechnic Institute"

The object of the research is technical devices of unauthorized division to information, imitators of devices of establishment for nonlinear radio-locators, and nonlinear radio-locators. The purpose of the work is experimental establishment of basic factors which influence on efficiency of unmasking action of nonlinear radio-locators

sounding radiation concerning the semiconductor elements with nonlinear volt-ampere descriptions; It is presented a hypothesis concerning physics of processes in semi-conductor structures at influence concerning the powerful microwave oven of radiation from a nonlinear radar.

The obtained results and their novelty: basic factors which influence on efficiency of unmasking action of nonlinear radio-locators sounding radiation on semiconductor elements with nonlinear volt-ampere descriptions are experimentally set; It is presented a hypothesis concerning physics of processes in semi-conductor structures at influence concerning the powerful microwave oven of radiation from a nonlinear radar.

УДК 62-768:537.531

АНАЛІЗ ЕФЕКТИВНОСТІ ЗАСТОСУВАННЯ МЕТАЛЕВОЇ СІТКИ ДЛЯ ЕКРАНУВАННЯ

Юрій Яремчук, Максим Притула, Євгеній Ніколаєв, Вікторія Козел
Вінницький національний технічний університет

У роботі проведено аналіз доцільності застосування металевої сітки для екранування. Відзначено переваги та недоліки використання металевих сіток в екрануючих конструкціях, проведено математичне дослідження ефективності екранів з металевої сітки. В результаті дослідження запропоновано математичну модель залежності ефективності екранування металевою сіткою від таких основних параметрів: довжина хвилі електромагнітного поля, діаметр дроту, відстань між волокнами, а також інші характеристики металу, з якого виконаний дріт.

При проведенні експериментальних досліджень залежності ефективності екранування від частоти для трьох мідних і трьох сталевих сіток з різними діаметрами дроту та відстанями між волокнами було встановлено:

1) якщо відношення відстані між волокнами до діаметру дроту є постійною величиною, то сітки, як із сталі так і із міді, з більшими відстанями між волокнами на низьких частотах більш ефективні, а на високих частотах менш ефективні, ніж сітки з меншими відстанями між волокнами;

2) при однакових значеннях відстані між волокнами та діаметру дроту, мідні сітки на низьких частотах мають кращу ефективність екранування, ніж стальні у стільки разів, у скільки питома провідність міді більша, ніж у сталі;

3) при однаковому значенні відстані між волокнами в одному і тому ж матеріалі, сітки з товстого провідника ефективніші сіток з тонких провідників.

Проведений аналіз показав, що металеві сітки можуть використовуватись для екранування для захисту інформації від витоку каналами побічних електромагнітних випромінювань та наведень. Але при цьому на кожному об’єкті, де вони використовуються, слід враховувати такі параметри інформативного випромінювання як частота, потужність, смуга випромінювання.

АНАЛИЗ ЭФФЕКТИВНОСТИ ИСПОЛЬЗОВАНИЯ МЕТАЛИЧЕСКОЙ СЕТКИ ДЛЯ ЭКРАНИРОВАНИЯ

Юрий Яремчук, Максим Притула, Евгений Николаев, Виктория Козел
Винницький национальный технический университет

В работе проведен анализ целесообразности применения металлической сетки для экранирования. Отмечено преимущества и недостатки использования металлических сеток в экранирующих конструкциях, проведено математическое исследование эффективности экранов из металлической сетки. В результате исследования предложена математическая модель зависимости эффективности экранирования металлической сеткой от таких основных параметров: длина волны электромагнитного поля, диаметр проволоки, расстояние между волокнами, а также другие характеристики металла, из которого выполнена проволока.

При проведении экспериментальных исследований зависимости эффективности экранирования от частоты для трех медных и трех стальных сеток с различными диаметрами проволоки и расстояниями между волокнами было установлено:

1) если отношение расстояния между волокнами к диаметру проволоки является постоянной величиной, то сетки, как из стали так и из меди, с большими расстояниями между волокнами на низких частотах более

эффективны, а на высоких частотах менее эффективны, чем сетки с меньшими расстояниями между волокнами;

2) при одинаковых значениях расстояния между волокнами и диаметра проволоки, медные сетки на низких частотах имеют лучшую эффективность экранирования, чем стальные во столько раз, во сколько удельная проводимость меди больше чем у стали;

3) при одинаковом значении расстояния между волокнами в одном и том же материале, сетки из толстого проводника эффективнее сеток из тонких проводников.

Проведенный анализ показал, что металлические сетки могут использоваться для экранирования при защите информации от утечки по каналам побочных электромагнитных излучений и наводок. Но при этом на каждом объекте, где они используются, следует учитывать такие параметры информативного излучения как частота, мощность, полоса излучения.

THE ANALYSIS OF METAL MESH EFFECTIVENESS FOR SHIELDING

Yuriy Yaremchuk, Maxym Prytula, Eugene Nikolaev, Victoria Kozel
Vinnitsa National Technical University

In this paper, the feasibility of applying metal mesh for shielding is analyzed. The advantages and disadvantages of using metal mesh screening in structures are noted.

In this paper, a mathematical research of the efficiency of metal mesh screens is studied. The research proposed a mathematical model of depends metal mesh shielding effectiveness of these parameters: wavelength of the electromagnetic field, wire diameter, the distance between the fibers, and other characteristics of the metal, which is made of wire.

When conducting experimental studies of shielding effectiveness depends on the frequency for the three copper and three metal mesh wire with different diameters and distances between fibers was found:

1) if the ratio of the distance between the fibers to the wire diameter is constant, the grids for both steel and brass, with large distances between the fibers at low frequencies are more effective at high frequencies and are less effective than nets with smaller distances between the fibers;

2) at identical values of the distance between the fibers and the diameter of wire, copper meshes at low frequencies have a better shielding than steel in many times, how much copper conductivity greater than steel;

3) in the same sense of distance between the fibers in the same material, with thick wire mesh nets are more effective with thin conductors.

The analysis showed, that the metal mesh can be used for screening in protecting information leakage channels from side electromagnetic radiations and pickups. But at the same time at each facility where they are used to consider the following parameters of informative radiation as frequency, power, strip light.