4 Реферати

УДК 35.078:342.738

ПРАВОВІ АСПЕКТИ ОРГАНІЗАЦІЇ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У СФЕРІ ПРАВООХОРОННОЇ ДІЯЛЬНОСТІ ВІДПОВІДНО ДО МІЖНАРОДНИХ СТАНДАРТІВ

Олексій Мервінський, Костянтин Мельник

Державна служба України з питань захисту персональних даних

Стаття: ***4 стор, 3 джерела.***

На сьогоднішній день питання організації захисту персональних даних правоохоронними органами є надзвичайно важливим. З моменту ратифікації Україною базових міжнародних стандартів у сфері захисту персональних даних дане питання потребує постійного дослідження та аналізу, адже ефективне виконання владних повноважень правоохоронними органами в Україні нерозривно пов'язане із забезпеченням права на приватне життя особи та захисту її персональних даних. Міжнародні стандарти в сфері захисту персональних даних відносять більшість персональних даних, що обробляються правоохоронними органами з огляду на певну специфіку їх діяльності, до категорії так званих «чутливих» персональних даних, зокрема про расове або етнічне походження людини, політичні, релігійні та світоглядні переконання, членство в політичних партіях або професійних спілках тощо. Цим, зокрема, і пояснюється важливість застосування особливих та додаткових правових гарантій захисту персональних даних під час їх обробки правоохоронними органами, адже чим більша чутливість та особливість персональних даних, тим більшим стає ризик порушення прав осіб на їх приватне життя. Варто зауважити, що міжнародні стандарти щодо захисту персональних даних у сфері правоохоронної діяльності в цілому належним чином імплементовані в національне законодавство України. Проте, деякі питання потребують подальшого опрацювання з огляду на стрімкий розвиток законодавчих процесів в нашій державі.

ПРАВОВЫЕ АСПЕКТЫ ОРГАНИЗАЦИИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В СФЕРЕ ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ СОГЛАСНО МЕЖДУНАРОДНЫМ СТАНДАРТАМ

Алексей Мервинский, Константин Мельник

Государственная служба Украины по вопросам защиты персональных данных

На сегодняшний день вопросы организации защиты персональных данных правоохранительными органами является чрезвычайно важными. С момента ратификации Украиной базовых международных стандартов в области защиты персональных данных данный вопрос требует постоянного исследования и анализа, ведь эффективное выполнение властных полномочий правоохранительными органами в Украине неразрывно связано с обеспечением права лица на частную жизнь и защиты его персональных данных. Международные стандарты в области защиты персональных данных относят большинство персональных данных, обрабатываемых правоохранительными органами, учитывая определенную специфику их деятельности, к категории так называемых «чувствительных» персональных данных, в частности о расовом или этническом происхождении человека, политические, религиозные и мировоззренческие убеждения, членство в политических партиях или профессиональных союзах и т.п.. Этим, в частности, и объясняется важность применения особых и дополнительных правовых гарантий защиты персональных данных при их обработке правоохранительными органами, ведь чем больше чувствительность персональных данных, тем больше становится риск нарушения прав лиц на их частную жизнь. Стоит отметить, что международные стандарты по защите персональных данных в сфере правоохранительной деятельности в целом должным образом имплементированы в национальное законодательство Украины. Однако, некоторые вопросы требуют дальнейшей проработки с учетом стремительного развития законодательных процессов в нашем государстве.

LEGAL ASPECTS OF THE PERSONAL DATA PROTECTION IN THE AREA OF THE LAW ENFORCEMENT ACTIVITY ACCORDING TO INTERNATIONAL STANDARDS

Oleksiy Mervinskiy, Kostyantyn Melnyk
The State Service of Ukraine on Personal Data Protection

Today, the issue of personal data protection by the law enforcement agencies is essential. Since the ratification by Ukraine of the basic international standards in the field of the personal data protection this issue requires the constant research and analysis, as the effective power of law enforcement in Ukraine is inseparably linked with the rights of individual on privacy and the protection of its personal data. International standards for the protection of personal data include the majority of personal data processed by law enforcement agencies, taking into account the specifics of their particular activity, to the category of so-called "sensitive" personal data, particularly on racial or ethnic origin of the human, political, religious or philosophical beliefs, membership in political parties or trade unions etc. This, in particular, explains the importance of special and additional legal safeguards to protect personal data as they are processed by law enforcement agencies, because the more sensitive personal data, the greater the risk of violating the rights of individuals to their privacy. It should be noted that international standards for the protection of personal data in the field of law enforcement, in general, properly implemented in the national legislation of Ukraine. However, some issues require further study, taking into account the rapid development of the legislative process in our state.

УДК 351.745.7:343.9:007

ІНФОРМАЦІЙНИЙ ДЕТЕРМІНІЗМ В НАУКАХ КРИМІНАЛЬНОГО ЦИКЛУ У СВІТЛІ БУТСТРАП-КОНЦЕПЦІЇ

Дарія Прокоф'єва-Янчиленко
Служба безпеки України

Стаття: ***10 стор., 86 джерел.***

В умовах ноосферного розвитку та поступового відходу від картезіанської наукової парадигми об'єктивною необхідністю стає й відповідне реформування поглядів на злочин та злочинність, яка сьогодні визнається однією з найбільш істотних загроз національній безпеці на загальнодержавному та міжнародному рівні, а також розробка нових стратегій протидії зазначеним негативним явищам.

Науки кримінального циклу за тривалий період свого розвитку накопичили в своєму арсеналі безліч концептуальних ідей щодо поняття злочинності, її причин та умов, особистості злочинця, механізму злочину та особливостей його відображення тощо, аналізуючи відповідні явища в контексті детермінаційних процесів відповідно до своїх завдань та предмету. Водночас, ці результати лишаються взаємно ізольованими та недостатніми для досягнення спільної мети наук кримінального циклу та правоохоронної практики.

Тому видається за доцільне з використанням нетрадиційного філософського підґрунтя окреслити новий системний підхід до пізнання природи злочинності, а також закономірностей реалізації і відображення механізму злочину. Перспективним в цьому контексті видається застосування бутстрап-концепції та розгляд злочинності як бутстрап-системи, якій властиві відповідні загальні риси бутстрап-систем. На перший план, таким чином, виходить проблема інформаційного детермінізму та інформаційної безпеки, 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 особи, держави, суспільства та навколишнього природного середовища.

ИНФОРМАЦИОННЫЙ ДЕТЕРМИНИЗМ В НАУКАХ УГОЛОВНОГО ЦИКЛА В СВЕТЕ БУТСТРАП-КОНЦЕПЦИИ

Дария Прокофьева-Янчиленко
Служба безопасности Украины

В условиях ноосферного развития и постепенного отхода от картезианской научной парадигмы объективной необходимостью становится и соответствующее реформирование взглядов на преступление и

преступность, которая сегодня признается одной из наиболее существенных угроз национальной безопасности на общегосударственном и международном уровне, а также разработка новых стратегий противодействия указанным негативным явлениям.

Науки криминального цикла за продолжительный период развития накопили в своем арсенале множество концептуальных идей относительно понятия преступности, ее причин и условий, личности преступника, механизма преступления и особенностей его отображения и т.п., анализируя соответствующие явления в контексте детерминационных процессов в соответствии со своими задачами и предметом. Вместе с тем, эти результаты остаются взаимно изолированными и недостаточными для достижения общей цели наук криминального цикла и правоохранительной практики.

Поэтому представляется целесообразным с использованием нетрадиционного философского базиса очертить новый системный подход к познанию природы преступности, а также закономерностей реализации и отображения механизма преступления. Перспективным в этом контексте является применения бутстрап-концепции и рассмотрение преступности как бутстрап-системы, которой присущи соответствующие общие черты бутстрап-систем. На первый план, таким образом, выходит проблема информационного детерминизма и информационной безопасности, 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 личности, государства, общества и окружающей природной среды.

INFORMATIVE DETERMINISM IN SCIENCES OF CRIMINAL CYCLE IN THE LIGHT OF BUTSTRAP-CONCEPTION

Darius Prokof'eva-Yanchilenko
Service safety of Ukraine

The corresponding reforming of sights at a crime and criminality which admits today as one of the most essential threats of national safety at nation-wide and international level, and also working out of new strategy of counteraction to this specified negative phenomena has become an objective necessity in the conditions of noosphere development and a gradual withdrawal from a Cartesian scientific paradigm.

Sciences of a criminal cycle for the long period of their development have saved up in the arsenal set of conceptual ideas concerning concept of criminality, its reasons and conditions, persons of the criminal, the mechanism of a crime and features of its display etc., while analyzing the corresponding phenomena in a context of determinating processes according to the problems and a subject. At the same time, these results remain mutually isolated and insufficient for achievement of an overall aim of sciences of a criminal cycle and law-enforcement practice.

Therefore it is expedient to use the nonconventional philosophical basis to outline the new system approach to knowledge of the nature of criminality, and also laws of realization and display of the mechanism of a crime. Perspective in this context is applications of the bootstrap-concept and criminality consideration as bootstrap-systems in which corresponding common features of bootstrap-systems are inherent. On the foreground, thus, there is a problem of an information determinism and information security, because using of knowledge about information interrelations in the sciences of a criminal cycle and law-enforcement practice opens new prospects in achievement of their basic overall aim – safeguarding of criminological security of the person, the state, a society and surrounding environment.

УДК 354:007

ВПЛИВ ВІРТУАЛЬНИХ СПІЛЬНОТ НА ІНФОРМАЦІЙНУ БЕЗПЕКУ: СУЧАСНИЙ СТАН ТА ТЕНДЕНЦІЇ РОЗВИТКУ

Гриненко Ігор, Прокоф'єва-Янчиленко Дарія*
*Національна Академія Служби безпеки України, **Служба безпеки України*

Стаття***: 5 стор., 11 джерел***

Інформаційна революція зумовлює появу нових викликів у сфері політики, культури, економіки і національної безпеки. Ключове значення для національної безпеки на сучасному етапі набуває питання створення ефективних і прозорих систем управління, які, в той же час, були б здатними захистити громадян і

життєво-важливі національні інтереси. Істотним чинником, який впливає на національну і міжнародну безпеку, при цьому стає існування віртуальних співтовариств, побудованих шляхом використання сучасних телекомунікаційних технологій. Формування таких співтовариств обумовлене як розширення інформаційної сфери із залученням до неї традиційних акторів, так і диверсифікацією активності у рамках кіберпростору. Діяльність вказаних віртуальних співтовариств носить явний транснаціональний характер і, з одного боку, виражає певні законні інтереси громадськості, а з іншої - несе в собі певні загрози і виклики, які повинні враховуватися при напрацюванні систем і заходів забезпечення інформаційної безпеки, зокрема, віртуальні співтовариства, які діють в он-лайн режимі, мають значний потенціал в здійсненні асиметричних атак. Надалі прогнозується розширення сфери впливу таких структур, які гратимуть все більшу роль у формуванні не лише інформаційного середовища, але і в широкому спектрі процесів громадського життя внаслідок глобалізації. Тому дослідження впливу таких віртуальних співтовариств на інформаційний простір є важливою передумовою напрацювання заходів забезпечення національної і міжнародної безпеки як в інформаційній, так і в інших сферах життєдіяльності суспільства.

ВЛИЯНИЕ ВИРТУАЛЬНЫХ СООБЩЕСТВ НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ: СОВРЕМЕННОЕ СОСТОЯНИЕ И ТЕНДЕНЦИИ РАЗВИТИЯ

Гриненко Игорь, Прокофьева-Янчиленко Дария*

*Национальная Академия Службы безопасности Украины, *Служба безопасности Украины*

Информационная революция предопределяет появление новых вызовов в сфере политики, культуры, экономики и национальной безопасности. Ключевое значение для национальной безопасности на современном этапе приобретает вопрос создания эффективных и прозрачных систем управления, которые, в то же время, были бы способными защитить граждан и жизненно-важные национальные интересы. Существенным фактором, который влияет на национальную и международную безопасность, при этом становится существование виртуальных сообществ, построенных путем использования современных телекоммуникационных технологий. Формирование таких сообществ обусловлено как расширением информационной сферы с вовлечением в нее традиционных актеров, так и диверсификацией активности в рамках киберпространства. Деятельность указанных виртуальных сообществ носит явный транснациональный характер и, с одной стороны, выражает определенные законные интересы общественности, а с другой – несет в себе определенные угрозы и вызовы, которые должны учитываться при наработке систем и мер обеспечения информационной безопасности, в частности, виртуальные сообщества, которые действуют в он-лайн режиме, имеют значительный потенциал в совершении асимметрических атак. В дальнейшем прогнозируется расширение сферы влияния таких структур, которые будут играть все большую роль в формировании не только информационного среды, но и в широком спектре процессов общественной жизни вследствие глобализации. Поэтому исследование влияния таких виртуальных сообществ на информационное пространство является важной предпосылкой наработки мер обеспечения национальной и международной безопасности как в информационной, так и в других сферах жизнедеятельности общества.

THE INFLUENCE OF VIRTUAL COMMUNITIES ON INFORMATION SECURITY: A CURRENT STATE AND DEVELOPMENT TENDENCIES

Grynenko Igor, Prokofieva-Yanchylenko Daria*

*National Academy of the State security service of Ukraine, *State security service of Ukraine*

Information revolution predetermines occurrence of new calls in sphere of a policy, culture, economy and national security. At the present stage key value for national security gets a question of creation of effective and transparent control systems which, at the same time, would be capable to protect citizens and the vital national interests. Existence of the virtual communities constructed by using of modern telecommunication technologies becomes the essential factor which influences national and international security. Formation of such communities is caused as expansion of information sphere with involving traditional actors in it, and a diversification of activity

within the limits of a cyberspace. Activity of the specified virtual communities has obvious transnational character and, on the one hand, expresses certain legitimate interests of the public, and with another – bears the certain threats and calls which should be considered at an operating time of systems and measures of maintenance of information security, in particular, virtual communities which operate in online a mode, have considerable potential in fulfillment asymmetric attacks. Further expansion of such structures influence and they will play the increasing role in formation not only information environments, but also in a wide spectrum of processes of public life owing to globalization is predicted. Therefore research of such virtual communities influence on information field is the important precondition of an operating time of measures of maintenance of national and international security both in information and in other spheres of ability of a society life.

УДК 004.056.5(52)

МОДЕЛЬ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ БАЗ ДАНИХ В ОРГАНІЗАЦІЯХ, ЯКІ ВИКОРИСТОВУЮТЬ ВІДОМОСТІ, ЩО МІСТЯТЬ ДЕРЖАВНУ ТАЄМНИЦЮ

Давуд Рустамов, Мірза Рзаєв
Міністерство Національної Безпеки Азербайджанської Республіки

Стаття: ***3 стор., 3 джерела.***

Запропонована модель забезпечення безпеки реляційних баз даних (РБД) відомостей, що становлять державну таємницю, (ВСДТ) складається з двох частин:

1. Управління доступом до РБД з архітектури багаторівневої системи (БРС);
2. Контроль діяльності користувачів, які отримали доступ до РБД.

Основна мета пропонованої моделі безпеки - поліпшена форма управління доступом до баз даних з інформацією, що містить державну таємницю, і контроль всіх дій, що виконуються над інформацією. Модель дозволяє перекрити більшість уразливих, з точки зору несанкціонованого доступу, точок баз даних. У запропонованій системі перевірки доступу до БД ВСДТ використовується трьох етапний процес визначення допустимого рівня роботи користувачів з документами.

На будь-якій стадії перевірок користувачеві може бути відмовлено в доступі до конкретного документа. Пропонована схема найбільш зручна для використання в організаціях зі складною структурою прав доступу до ВСДТ бо вона легко може врахувати такі параметри, як гриф секретності, структурну організацію підрозділів, посадову структуру і т.д. і є доповненням до наведеного раніше методу контролю доступу в плані виявлення позаштатного поводження з даними тих, хто пройшов законну аутентифікацію і отримав той чи інший рівень доступу до документів.

Відзначаються такі твердження:

1. Якщо процес перевірки рівня доступу завершено успіхом, то діяльність користувачів, які пройшли ідентифікацію, можна відстежити за допомогою деякого відображення $G_1 : U \times OP \to D$ (де U - кінцева множина користувачів СУБД; D – кінцева множина зберігаємих в РБД документів; ОР – кінцева множина операцій, виконаних користувачами над документами) і таким чином визначити множину документів, над якими конкретні користувачі виконували ті чи інші операції.

2. Якщо процес перевірки рівня доступу згідно поданої вище схеми завершено успіхом, то множина користувачів, які зробили певні дії над документами визначається за допомогою деякого відображення $G_2 : D \times OP \to U$ і таким чином можна виявити всіх користувачів, які використовують у своїй роботі конкретні документи.

На практиці ці відображення можна побудувати з використанням допоміжних системних таблиць, заповнення яких здійснюється виключно на рівні самої СУБД з допомогою набору тригерів. В цих таблицях відзначаються ідентифікатори користувачів і документів, з якими вони працювали, тип операцій, дата проведення операції, старі і нові значення змінених даних. Аналіз даних таблиць дозволяє визначити всі маніпуляції користувачів над документами, виявити активність користувачів, сферу їх інтересів і тенденції їх діяльності.

МОДЕЛЬ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ БАЗ ДАННЫХ В ОРГАНИЗАЦИЯХ, ИСПОЛЬЗУЮЩИХ СВЕДЕНИЯ, СОДЕРЖАЩИЕ ГОСУДАРСТВЕННУЮ ТАЙНУ

Давуд Рустамов, Мирза Рзаев
Министерство Национальной Безопасности Азербайджанской Республики

Предложена модель обеспечения безопасности реляционных баз данных (РБД) сведений, содержащих государственную тайну, (ССГТ) состоит из двух частей:

1. Управление доступом к РБД по архитектуре многоуровневой системы (МУС);
2. Контроль деятельности пользователей, получивших доступ к РБД.

Основная цель предлагаемой модели безопасности – улучшенная форма управления доступом к базам данных с информацией, содержащей государственную тайну, и контроль всех действий, производимых над информацией. Модель позволяет перекрыть большинство уязвимых, с точки зрения несанкционированного доступа, точек баз данных. В предлагаемой системе проверки доступа к БД ССГТ используется трехэтапный процесс определения допустимого уровня работы пользователей с документами.

На любой стадии проверок пользователю может быть дан отказ в доступе к конкретному документу. Предлагаемая схема наиболее удобна для использования в организациях, со сложной структурой прав доступа к ССГТ, т.к. легко может учесть такие параметры, как гриф секретности, структурную организацию подразделений, должностную структуру и т.д. и является дополнением к приведенному ранее методу контроля доступа, в плане выявления нештатного обращения с данными тех, кто прошел законную аутентификацию и получил тот или иной уровень доступа к документам.

Отмечаются следующие утверждения:

1. Если процесс проверки уровня доступа завершен успехом, то деятельность пользователей, прошедших аутентификацию, можно отследить при помощи некоторого отображения $G_1 : U \times OP \to D$ (где U – конечное множество пользователей СУБД; D – конечное множество хранимых в РБД документов; OP – конечное множество операций, производимых пользователями над документами) и таким образом определить множество документов, над которыми конкретные пользователи выполняли те, или иные операции.

2. Если процесс проверки уровня доступа согласно представленной выше схеме завершен успехом, то множество пользователей, совершивших определенные действия над документами определяется при помощи некоторого отображения $G_2 : D \times OP \to U$ и таким образом можно выявить всех пользователей, использовавших в своей работе конкретные документы.

На практике эти отображения можно построить с использованием вспомогательных системных таблиц, заполнение которых осуществляется исключительно на уровне самой СУБД с помощью набора триггеров. В этих таблицах отмечаются идентификаторы пользователей и документов, с которыми они работали, тип операций, дата проведения операции, старые и новые значения измененных данных. Анализ данных таблиц позволяет определить все манипуляции пользователей над документами, выявить активность пользователей, сферу их интересов и тенденции их деятельности.

THE SECURITY MODEL OF THE DATABASES IN THE ORGANIZATIONS USING INFORMATION CONTAINING STATE SECRETS

Davud Rustamov, Mirza Rzaev
The Ministry Of National Security Of The Republic Of Azerbaijan

A model of the security relational database (RDB) of the information containing a state secret (ICSS) consists of two parts:

1. Access control RDB on the architecture of the multi-level system (MLS);
2. Control of the activity of users that have access to the RDB.

The main objective of the proposed model of security - enhanced form of access control to a database with the information containing the state secret, and the control of all the action, produced on the information. The model

allows to block most vulnerable, from the point of view of unauthorized access points database. In the proposed system test access to the database ICSS uses a three-step process of determining the acceptable level of user work with the documents.

At any stage of the audit, the user can be given the denial of access to a particular document. The proposed scheme is the most convenient to use in organizations, with a complex structure of rights of access to ICSS, as can easily take into account parameters such as the stamp of secrecy, the structural organization of subdivisions, job structure, etc. and is an addition to the earlier method of access control, in terms of identification of the non-established treatment with the data of those who had passed the lawful authentication and received a certain level of access to documents.

Are the following statements:

1. If the process of checking the level of access is completed successfully, the activity of the users, authenticated, can be traced with the help of some display (where U is the final number of users of the database; $G_1 : U \times OP \to D$ (D - finite set of stored in a distributed database system documents; OP - finite set of operations performed by users on documents) and thus define the set of documents, on which specific users perform those, or other operations.

2. If the process of checking the access level according to the above scheme is completed successfully, then the set of users who have committed certain actions on documents determined by means of a display $G_2 : D \times OP \to U$ and thus you can identify all the users, who use in their work of specific documents.

In practice, these mappings can be built with the use of the system tables, the filling of which is carried out exclusively at the level of the database using a set of triggers. In these tables are user IDs and documents, with whom they worked, type of operations, the date of the operation, the old and new values of changed data. Analysis of the data tables allows you to identify all of the manipulation of users over the documents, to identify the users activity, sphere of their interests and the trends of their activity.

УДК 004.77:340:

ЗАКОНОДАВЧЕ ЗАБЕЗПЕЧЕННЯ ОХОРОНИ Й ЗАХИСТУ ПЕРСОНАЛЬНОЇ ІНФОРМАЦІЇ В МЕРЕЖІ ІНТЕРНЕТІ

Олександр Радкевич

Національна академія внутрішніх справ

Стаття: ***4 стор, 6 джерел.***

Запровадження інформаціно – телекомунікаційних технологій у суспільне життя спричинило поширення практики порушення немайнових прав особи, що проявляється в незаконному зборі, використанні й поширенні інформації персонального характеру. Виникненню даної проблеми неабияк сприяє правовий нігілізм населення нашої держави. Відсутність належного законодавчого забезпечення охорони й захисту персональної інформації в мережі Інтернет призводить до збільшення кількості правопорушень у цій сфері. Розглядаючи дефініції охорони й захисту можна виявити що вони є передбаченою нормами права діяльністю як державних, так і громадських органів, спрямованою на примусове відновлення порушених прав. З огляду на це охорону й захист персональної інформації можна розглядати як сукупність методів, засобів і заходів для забезпечення інформаційної безпеки людини, суспільства і держави в усіх сферах життєдіяльності.

Окрім цього, персональну інформацію можна розуміти як: перелік конкретної інформації про особу, за допомогою якої можна конкретно ідентифікувати особу. З розвитком високих технологій постала проблема забезпечення належного захисту персональної інформації громадян держави. Так, інформаціно – телекомунікаційні технології за своєю властивістю можуть збирати, накопичувати та передавати величезні масиви інформації на значну відстань. З огляду на це мережа Інтернет слугує інформаційною базою як про навколишню природу, так і про людей. Таким чином, мережа Інтернет – це лише знаряддя для доступу до персональної інформації. Відтак під мережею Інтернет можна розуміти засіб за для реалізації прав на вільне збирання, зберігання, використання й поширення інформації.

Основоположним документом, який забезпечує нормативно-правове регулювання відносин у мережі Інтернет, є Конституція України. Зокрема, права на недоторканість приватного життя регулюються ч. 1 ст. 32, ст. 30 (недоторканність житла), ст. 31 (таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції), ч. 2 ст. 34 (право на свободу інформації) Конституції України тощо. Перераховане свідчить про наявність положень, які можна трактувати як такі, що забезпечують охорону й захист осіб у мережі

Інтернет, але в ній відсутні положення, що чітко регулювали б відносини в мережі Інтернет та відображали б законодавство про захист персональної інформації.

Окрім Конституції, важливу роль відіграють закони, покликані ліквідувати прогалини у законодавстві у сфері охорони й захисту персональної інформації. Значну роль у цьому питанні відіграє міжнародний досвід охорони й захисту персональної інформації. Так, відносини, пов'язані з інформацією у мережі Інтернет, регулюються «Хартією глобального інформаційного суспільства», Конвенцією ООН «Про використання електронних повідомлень у міжнародних договорах», Декларацією «Про свободу обміну інформацією в Інтернеті» тощо. У контексті регулювання персональної інформації науковий інтерес становить досвід Японії, згідно з яким до персональної інформації, яка охороняється і захищається відповідно до закону, зараховано: електронний «нік», Ір-адреса, електронна адреса, індифікаційний номер на сайті та інші відомості, що перебувають в електронному вигляді, тобто таку інформацію, завдяки якій можна ідентифікувати особу.

ЗАКОНОДАТЕЛЬНОЕ ОБЕСПЕЧЕНИЕ ОХРАНЫ И ЗАЩИТЫ ПЕРСОНАЛЬНОЙ ИНФОРМАЦИИ В СЕТИ ИНТЕРНЕТ

Александр Радкевич

Национальная академия внутренних дел

Введение информационно – телекоммуникационных технологий в общественную жизнь вызвало распространение нарушений неимущественных прав лиц, которое проявляется в незаконном сборе, использовании и распространении информации персонального характера. К возникновению данной проблемы причастен правовой нигилизм населения нашего государства. Отсутствие должного законодательного обеспечения охраны и защиты персональной информации в сети Интернет приводит к увеличению количества правонарушений в этой сфере. Рассматривая дефиниции охраны и защиты, можно заметить что они представляют собой предусмотренную нормами права деятельность как государственных, так и общественных органов, направленную на принудительное восстановление нарушенных прав. Учитывая это, охрану и защиту персональной информации можно рассматривать как совокупность методов, средств и мер по обеспечению информационной безопасности человека, общества и государства во всех сферах жизнедеятельности. Кроме того, персональную информацию можно понимать как перечень конкретной информации о лице, с помощью которой можно конкретно идентифицировать личность.

С развитием высоких технологий появилась проблема обеспечения защиты личной информации граждан государства. Так, информационно – телекоммуникационные технологии по своему могут собирать, накапливать и передавать огромные массивы информации на значительное расстояние. Учитывая это, сеть Интернет служит информационной базой как об окружающей природе, так и о людях. Таким образом, сеть Интернет – это только инструмент для доступа к персональной информации. Поэтому под сетью Интернет можно понимать средство для реализации прав на свободный сбор, хранение, использование и распространение информации.

Основополагающим документом, который обеспечивает нормативно-правовое регулирование отношений в сети Интернет, является Конституция Украины. В частности, права на неприкосновенность частной жизни регулируются ч. 1 ст. 32, ст. 30 (неприкосновенность жилища), ст. 31 (тайна переписки, телефонных разговоров, телеграфной и другой корреспонденции), ч. 2 ст. 34 (право на свободу информации) Конституции Украины и т.п. Перечисленное свидетельствует о наличии положений, которые можно трактовать как такие, которые обеспечивают охрану и защиту лиц в сети Интернет, но при этом в ней отсутствуют положения, имеющие своей целью четкое регулирование отношений в сети Интернет и формирование законодательства о защите персональной информации. Кроме Конституции, важную роль играют законы, призванные устранить пробелы в законодательстве в сфере охраны и защиты персональной информации. Значительную роль в этом вопросе играет международный опыт охраны и защиты персональной информации. Так, отношения, связанные с информацией в сети Интернет, регулируются «Хартией глобального информационного общества», Конвенцией ООН «Об использовании электронных сообщений в международных договорах», Декларацией «О свободе обмена информацией в Интернете» и др. В контексте регулирования персональной информации научный интерес представляет опыт Японии, согласно которому к персональной информации, которая охраняется и защищается в соответствии с законом, отнесены: электронный «ник», Ір-адрес, электронный адрес, индификационный номер на сайте и другие сведения, которые находятся в электронном виде, то есть такую информацию, благодаря которой можно идентифицировать человека.

LEGISLATIVE ENSURE THE SAFETY AND PROTECTION OF PERSONAL INFORMATION IN THE INTERNET

Alexander Radkevich
National Academy of Internal Affairs

Introduction of information and communication technologies in public life been called to extend the practice of violations nonproperty rights individuals which is shown in the illegal collection, use and dissemination of personal character. The development of this problem leads to the presence of legal nihilism in the population of our country. Absence of proper legislation to ensure safety and security personal information on the Internet, leading to an increase in the number of offenses in this area. Considering the definition of protection and can be seen that they are provided by law the activities of both state and public agencies designed to force the restoration of violated rights. n view of this protection and defense personal information can be viewed as a set of methods, tools and measures to ensure the information security man, society and state in all spheres of life. Moreover personal information can be understood as: list specific information about the person and the object with which you can specifically identify the person. With the development of high technology caused the problem ensuring the security of personal information of citizens of the state. Information and telecommunication technologies in their property may collect, store and transmit vast amounts of information at a considerable distance. For this reason the Internet serves as an information base, as about the world and about people. So the Internet is only a tool for access to personal information. This way when the Internet may be understood by means for the rights to freedom of assembly, storage, use and dissemination of information. Should be noted that basic document that provides the legal regulation of relations on the Internet is the Constitution of Ukraine. In particular the right to privacy, including a regulated Art. 32, Art. 30 (inviolability of the home), Art 31 (privacy of correspondence, telephone conversations, telegraph and other correspondence), Art 34 (right to freedom of information) of the Constitution of Ukraine and others. Numbered indicates that the provisions under which can be interpreted as providing security and protection of individuals on the Internet, but there are no provisions that aim to clear the regulation of relations on the Internet and the formation of legislation on protection of personal information. Besides the constitutional role played by laws designed to close gaps in law enforcement for in the Protection and defense of personal information. Important part in this issue plays international experience and the protection of personal information. Thus, the the relations connected with information on the Internet be regulated "Charter of the global information society," UN Convention "On the Use of Electronic Communications in International Contracts," the Declaration "On freedom of communication on the Internet" and so on. In the context of regulation of personal information research interest is the experience of Japan under which your personal information is protected and defended by law consist of: an electronic "nickname», Ip-address, email address, id-number online and other information which are in electronic form, such information with which to identify the person.

УДК 534.873:88

ПРО ПРОБЛЕМУ РОЗРАХУНКУ ДАЛЬНОСТІ ПРИЙОМУ АКУСТИЧНОЇ ІНФОРМАЦІЇ З ВІДКРИТИХ МАЙДАНЧИКІВ

Михайло Дівізінюк, Юлія Гончаренко, Дмитро Гончаренко
Севастопольський національний університет ядерної енергії та промисловості

Стаття: ***6 стор., 4 джерел.***

Для побудови систем захисту акустичної інформації на відкритих майданчиках (тенісних кортах, гольфових полях, входах в будівлі, балконах, мансардах, верандах і т.д.) необхідно вирішити проблему розрахунку дальності прийому цієї інформації акустоелектронними засобами.

Показано, що енергетичною дальністю виявлення акустичного сигналу є відстань, при якій досягається рівність закономірності спаду інтенсивності акустичного поля в стандартній атмосфері та енергетичного потенціалу певного приймального пристрою з певною ціллю в заданій обстановці з перешкодами. Геометрична дальність виявлення акустичних хвиль визначається геометричною зоною акустичної освітленості, що отримується в результаті побудови променевої картини, яка залежить від стратифікації атмосфери, рельєфу підстильної поверхні та ін. Дальність виявлення акустичної мети, що визначається, враховує геометричну і визначається як добуток енергетичної дальності дії на коефіцієнт аномалії стратифікованої атмосфери. Для отримання значення цих коефіцієнтів необхідно проведення спеціалізованих досліджень.

О ПРОБЛЕМЕ РАСЧЕТА ДАЛЬНОСТИ ПРИЕМА АКУСТИЧЕСКОЙ ИНФОРМАЦИИ С ОТКРЫТЫХ ПЛОЩАДОК

Михаил Дивизинюк, Юлия Гончаренко, Дмитрий Гончаренко
Севастопольский национальный университет ядерной энергии и промышленности

Для построения систем защиты акустической информации на открытых площадках (теннисных кортов, гольфовых полях, входах в здания, балконах, мансардах, верандах и т.д.) необходимо решить проблему расчета дальности приема этой информации акустикоэлектронными средствами.

Показано, что энергетической дальностью обнаружения акустического сигнала является расстояние, при котором достигается равенство закономерности спада интенсивности акустического поля в стандартной атмосфере и энергетического потенциала определенного приемного устройства по определенной цели в заданной помеховой обстановке. Геометрическая дальность обнаружения акустических волн определяется геометрической зоной акустической освещенности, получаемой в результате построения лучевой картины, зависящей от стратификации атмосферы, рельефа подстилающей поверхности и др. Определяемая дальность обнаружения акустической цели учитывает геометрическую и определяется как произведение энергетической дальности действия на коэффициент аномалии стратифицированной атмосферы. Для получения значения этих коэффициентов необходимо проведение специализированных исследований.

THE PROBLEM OF CALCULATING DISTANCE RECEIVING INFORMATION FROM ACOUSTIC OPEN AREAS

Mykhailo Diviziniuk, Iulia Goncharenko, Dmytro Goncharenko
Sevastopol National University of Nuclear Energy and Industry

For the construction of acoustic systems for the protection of information in open areas (tennis courts, golf courses, building entrances, balconies, attics, porches, etc.) necessary to solve the problem of calculating the distance of the reception of this information with the help of acoustic and electronic means.

It is shown that the energy detection range of the acoustic signal is the distance at which the equality of the laws of the intensity decay of the acoustic field in a standard atmosphere and the energy potential of a specific receptor for a specific purpose in a given noise conditions. Geometric detection range of acoustic waves is determined by the geometrical area of acoustic illumination is obtained by constructing the ray pattern, which depends on the stratification of the atmosphere, land surface topography, and other-defined detection range of acoustic target takes into account the geometry and is defined as the product of the energy range of the anomaly by a factor of a stratified atmosphere. To obtain the values of these coefficients is necessary to conduct special investigations.

УДК 681.3

АНАЛІТИЧНІ МЕТОДИ ШИФРУВАННЯ НА ОСНОВІ ПЕРЕТВОРЕНЬ ІЗ ВИКОРИСТАННЯМ ЛИШКОВИХ КЛАСІВ

В'ячеслав Василенко
Національний авіаційний університет

Стаття: ***8 стор., 5 джерел.***

Однією із вкрай важливих для сучасних автоматизованих систем є проблема забезпечення конфіденційності інформації, для вирішення якої застосовуються ті чи інші методи, методики чи алгоритми. Для забезпечення конфіденційності інформації в багатьох випадках криптографічне перетворення є чи не єдиним шляхом забезпечення її конфіденційності (з певною стійкістю до спроб розкриття її змісту – криптографічною стійкістю). На цей час теорія криптографічних перетворень розвинута досить широко й для забезпечення конфіденційності інформаційних об'єктів можна застосувати ті чи інші алгоритми криптографічного перетворення. Для шифрування інформації серед інших можуть використовуватися і аналітичні перетворення. Із них найбільше поширення набули методи шифрування, засновані на використовуванні матричної алгебри.

В статті пропонується один із можливих варіантів таких аналітичних криптографічних перетворень на основі переводу із позиційної системи числення в систему лишкових класів, а також із системи лишкових класів у позиційну систему числення. При цьому в статті здійснено аналіз криптографічної стійкості таких перетворень та запроновано варіанти її підвищення до рівня сучасних вимог. Запропоновані варіанти для умов переводу з однієї системи числення в інші цифрових кодів, якими в автоматизованих (комп'ютерних) системах представлені інформаційні об'єкти.

Аналіз криптографічної стійкості запропонованих механізмів блокових матричних перетворень дає можливість стверджувати, що способи криптоаналізу шляхом "статистичного" аналізу з використанням фрагментів відкритого та зашифрованого тексту, спроби обрахування прямих чи зворотних матриць, при дотриманні рекомендацій, викладених у відповідних розділах статті, є не результативними, а кількість варіантів ключових наборів є не меншою ніж для інших відомих механізмів криптографічних перетворень.

АНАЛИТИЧЕСКИЕ МЕТОДЫ ШИФРОВАНИЯ НА ОСНОВЕ ПРЕОБРАЗОВАНИЙ С ИСПОЛЬЗОВАНИЕМ ОСТАТОЧНЫХ КЛАССОВ

Вячеслав Василенко

Национальный авиационный университет

Одной из крайне важных для современных автоматизированных систем является проблема обеспечения конфиденциальности информации, для решения которой применяются те или иные методы, методики или алгоритмы. Для обеспечения конфиденциальности информации во многих случаях криптографическое преобразование является едва ли не единственным путем обеспечения ее конфиденциальности (с определенной стойкостью к попыткам раскрытия ее содержания - криптографической стойкостью). В настоящее время теория криптографических преобразований развита достаточно широко и для обеспечения конфиденциальности информационных объектов можно применить те или иные алгоритмы криптографического преобразования. Для шифрования информации среди других могут использоваться и аналитические преобразования. Из них наибольшее распространение получили методы шифрования, основанные на использовании матричной алгебры.

В статье предлагается один из возможных вариантов таких аналитических криптографических преобразований на основе перевода из позиционной системы счисления в систему остаточних классов, а также из системы остаточной классов в позиционную систему счисления. При этом в статье осуществлен анализ криптографической стойкости таких преобразований и предложены варианты ее повышения до уровня современных требований. Предложенны варианты для условий перевода из одной системы счисления в другую цифровых кодов, которыми в автоматизированных (компьютерных) системах представлены информационные объекты.

Анализ криптографической стойкости предложенных механизмов блочных матричных преобразований дает возможность утверждать, что способы криптоанализа путем "статистического" анализа с использованием фрагментов открытого и зашифрованного текста, попытки расчета прямых или обратных матриц, при соблюдении рекомендаций, изложенных в соответствующих разделах статьи, являются не результативными, а количество вариантов ключевых наборов не менше, чем для других известных механизмов криптографических преобразований.

ANALYTICAL METHODS FOR ENCRYPTION BASED ON THE TRANSFORMATION OF THE USE OF RESIDUAL CLASS

Viacheslav Vasylenko

National Aviation University

One of the most important problem of today's automated systems is ensuring of the confidentiality of information, which is used to solve these or other methods, techniques, or algorithms. To ensure confidentiality of information in many cases the cryptographic transformation is perhaps the only way to ensure its confidentiality (with a certain resistance to attempts by the disclosure of its contents - the cryptographic resistance). The theory of cryptographic transformations developed widely and to ensure the confidentiality of information objects can use these or other algorithms for cryptographic transformations. To encrypt the information to others may be used and

the analytical transformation. Of these, the most widely used encryption methods,which are based on the use of matrix algebra.

The article suggests one possible analysis of cryptographic transformations on the basis of a translation of the positional number system to a system of residual classes, as well as from the system of residual classes in a positional number system. In the paper we made an analysis of cryptographic strength of such change and provide suggestions to improve it to the level of modern requirements. The proposed options for the conditions of transfer from one system to another digital codes, which in automated (computer) systems are information objects.

Analysis of the cryptographic strength of the proposed mechanisms of block matrix transformations allows us to assert that the methods of cryptanalysis by "statistical" analysis using a fragment of an open and encrypted text, attempts to calculate the direct and inverse matrices, subject to the recommendations contained in the relevant sections of the article are not effective, and number of options for the key sets of not less then than for other known mechanisms of cryptographic transformations.

УДК 004.516.1

УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ З ВИКОРИСТАННЯМ НЕЧІТКИХ КОГНІТИВНИХ КАРТ

Богдан Волобуєв, Владислав Черниш

Харківський національний університет радіоелектроніки

Стаття: ***5 стор, 3 джерела.***

В сучасному світі термін ризик широко використовується у різних сферах життєдіяльності. Управління ризиками інформаційної безпеки (ІБ) являє собою досить широке поняття, яке використовується в літературі як вид діяльності, що включає визначення загроз безпеки інформаційної системи (ІС), оцінку рівня небезпеки загроз (тобто розмір можливого збитку), а також ймовірностей реалізації цих загроз (проведення повного аналізу ризиків системи). На основі аналізу загроз приймається рішення про заходи щодо зниження загального рівня ризику для ІС. Причому конкретний зміст цього поняття залежить від розв'язуваної задачі.

Пропонується підхід управління ризиками ІБ на основі нечітких когнітивних карт і штучних нейронних мереж. Пропонується розділити поняття ризику на дві складові: системо залежний та системо незалежний ризики. Даний підхід дозволяє зменшити частку суб'єктивізму в оцінці ризику ІБ організації, врахувати усі елементи, що беруть участь та не беруть участь в обробці даних автоматизованої системи (АС), а також автоматизувати процес управління ризиками.

Проблема аналізу інформаційних ризиків значно спрощується і формалізується при використанні нечіткого когнітивного підходу у поєднанні з використанням штучних нейронних мереж. Перевагою запропонованого підходу до аналізу ризиків на базі НКК є можливість побудови адекватної моделі впливу загроз на захищаються ресурси та оцінки їх наслідків при наявності неповної чи навіть суперечливої вихідної інформації.

УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ НЕЧЁТКИХ КОГНИТИВНЫХ КАРТ

Богдан Волобуев, Владислав Черныш

Харьковский национальный университет радиоэлектроники

В современном мире понятие риска широко употребляется в разных сферах деятельности. Управление рисками информационной безопасности (ИБ) представляет собой достаточно широкое понятие, которое используется в литературе как вид деятельности, включающий определение угроз безопасности информационной системы (ИС), оценку уровня опасности угроз (т.е. размера возможного ущерба), а также вероятностей реализации этих угроз (т.е. проведение полного анализа рисков системы). На основе анализа угроз принимается решение о мерах по снижению общего уровня риска для ИС. Причем конкретное содержание этого понятия зависит от решаемой задачи.

Предлагается подход для управления рисками ИБ на основе нечётких когнитивных карт и искусственных нейронных сетей. В подходе предлагается разделить понятие риска на две составляющие:

системозависимый и системонезависимый риски. Данный подход позволяет уменьшить долю субъективизма при оценке риска ИБ организации, учесть все элементы, участвующие и не участвующие в обработке данных в автоматизированной системе (АС), и автоматизировать процесс управления рисками.

Проблема анализа информационных рисков значительно упрощается и формализуется при использовании нечеткого когнитивного подхода в сочетании с использованием искусственных нейронных сетей. Достоинством предложенного подхода к анализу рисков на базе НКК является возможность построения адекватной модели воздействия угроз на защищаемые ресурсы и оценки их последствий при наличии неполной или даже противоречивой исходной информации.

RISK MANAGEMENT OF INFORMATION SECURITY USING FUZZY COGNITIVE MAPS

Bogdan Volobuiev, Vladislav Chernish
Kharkiv national university of radioelectronics

In today's world the concept of risk is widely used in various fields. Risk management information security (IS) is a rather broad term that is used in the literature as an activity, including identification of threats to the security of information systems (IS), evaluation of severity of threats (the size of potential damage), as well as the probabilities of the realization of these threats (conduct a full risk analysis system). Based on analysis of threats to the decision on measures to reduce the overall risk for IS. Moreover, the specific content of this concept depends on the task at hand.

The paper proposes an approach to risk management of information security based on fuzzy cognitive maps and artificial neural networks. In the approach proposed to divide the notion of risk into two components: a system-dependent and system-independent risks. This approach allows to reduce the proportion of subjectivity in assessing the risk of information security organization, consider all the elements involved and not involved in the processing of data in the Automatic System and automate the process of risk management.

The problem of information risk analysis is greatly simplified and formalized using fuzzy cognitive approach, combined with the use of artificial neural networks. The advantage of this approach to risk analysis based on the NCC is the ability to build an adequate model of the impact of threats to protected resources and assess their implications in the presence of incomplete or even contradictory information source.

УДК 681.3.06

ЗАХИСТ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ В ЛОКАЛЬНИХ ОБЧИСЛЮВАЛЬНИХ МЕРЕЖАХ, ПОБУДОВАНИХ З ВИКОРИСТАННЯМ ОПЕРАЦІЙНИХ СИСТЕМ MS WINDOWS

Андрій Тимошенко
ТОВ "Інститут комп'ютерних технологій"

Стаття: ***9 стор., 10 джерел.***

На цей час широко використовуються автоматизовані (інформаційні) системи, що реалізують різні технології оброблення інформації та основу обчислювальної системи яких становлять локальні обчислювальні мережі - сукупність взаємодіючих у процесі свого функціонування комп'ютерів, що мають спільно використовувані (поділювані) ресурси (жорсткі диски, пристрої печатки й т.п.), які звичайно підрозділяють на однорангові - такі, у яких спільно використовуватися (розділятися) можуть ресурси будь-якого комп'ютера, який, таким чином, може виконувати роль як клієнтської робочої станції, так і роль невиділеного сервера, а також мережі із виділеними серверами - такі, у яких спільно використовуються ресурси тільки спеціально виділених комп'ютерів (серверів).

У статті розглядаються особливості забезпечення захисту інформації з обмеженим доступом, оброблюваної в інформаційних системах, що класифіковані як автоматизовані системи класу 2, або в окремих складових інформаційних систем, що класифіковані як автоматизовані системи класу 3, за умови, що основу їх обчислювальної системи становлять локальні обчислювальні мережі, побудовані з використанням комп'ютерів, що функціонують під керуванням операційних систем сімейства MS

Windows.

На підставі аналізу відомих архітектур прикладних програмних засобів сучасних інформаційних систем, а також вимог діючої нормативно-правової бази щодо захисту інформації з обмеженим доступом формулюється перелік завдань захисту, які повинні бути реалізовані стосовно інформаційних об'єктів, оброблюваних в інформаційних системах, у різному виді подання та у різному стані. Показується, що ці завдання захисту не можуть бути виконані ні штатними засобами захисту операційних систем сімейства MS Windows, ні засобами захисту, реалізованими в складі прикладних програмних засобів. Обґрунтовується необхідність створення інтегрованих комплексів засобів захисту, у складі яких, крім засобів захисту, реалізованих у складі прикладних програмних засобів, повинні використовуватися засоби захисту, що функціонують на рівні ядра операційної системи (засоби захисту, інтегровані до складу операційної системи).

Показується можливість використання при побудові інтегрованих комплексів засобів захисту засобів комплексу "Гриф" (Експертний висновок № 239 від 13 серпня 2010 р.) та комплексу "Гриф-Мережа" (Експертний висновок № 203 від 24 грудня 2009 р.) виробництва ТОВ "Інститут комп'ютерних технологій".

Наводиться приклад успішної практичної реалізації запропонованого підходу при створенні інтегрованого комплексу засобів захисту інформаційно-аналітичної системи "Кадри ЗІ" версії 7.2 (Експертний висновок № 344 від 29 лютого 2012 р.).

ЗАЩИТА ИНФОРМАЦИИ С ОГРАНИЧЕННЫМ ДОСТУПОМ В ЛОКАЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ, ПОСТРОЕННЫХ С ИСПОЛЬЗОВАНИЕМ ОПЕРАЦИОННЫХ СИСТЕМ MS WINDOWS

Андрей Тимошенко
ООО "Институт компьютерных технологий"

В настоящее время широко используются автоматизированные (информационные) системы, реализующие различные технологии обработки информации, в качестве основы вычислительной системы которых выступают локальные вычислительные сети – совокупность взаимодействующих в процессе своего функционирования компьютеров, имеющих совместно используемые (разделяемые) ресурсы (жесткие диски, устройства печати и т.п.), которые обычно подразделяют на одноранговые – такие, в которых совместно использоваться (разделяться) могут ресурсы любого компьютера, который, таким образом, может выполнять роль как клиентской рабочей станции, так и роль невыделенного сервера, а также сети с выделенными серверами – такие, в которых совместно используются ресурсы только специально выделенных компьютеров (серверов).

В статье рассматриваются особенности обеспечения защиты информации с ограниченным доступом, обрабатываемой в информационных системах, классифицируемых как автоматизированные системы класса 2, либо в отдельных составляющих информационных систем, классифицируемых как автоматизированные системы класса 3, при условии, что основу их вычислительной системы составляют локальные вычислительные сети, построенные с использованием компьютеров, функционирующих под управлением операционных систем семейства MS Windows.

На основании анализа известных архитектур прикладных программных средств современных информационных систем, а также требований действующей нормативно-правовой базы по защите информации с ограниченным доступом формулируется перечень задач защиты, которые должны быть реализованы по отношению к информационным объектам, обрабатываемым в информационной системе, в различном виде представления и в различном состоянии. Показывается, что эти задачи защиты не могут быть выполнены ни штатными средствами защиты операционных систем семейства MS Windows, ни средствами защиты, реализованными в составе прикладных программных средств. Обосновывается необходимость создания интегрированных комплексов средств защиты, в составе которых, кроме средств защиты, реализованных в составе прикладных программных средств, должны использоваться средства защиты, функционирующие на уровне ядра операционной системы (средства защиты, интегрированные в состав операционной системы).

Показывается возможность использования при построении интегрированных комплексов средств защиты средств комплекса "Гриф" (Экспертное заключение № 239 от 13 августа 2010 г.) и комплекса "Гриф-Мережа" (Экспертное заключение № 203 от 24 декабря 2009 г.) производства ООО "Институт

компьютерных технологий".

Приводится пример успешной практической реализации предложенного подхода при создании интегрированного комплекса средств защиты информационно-аналитической системы "Кадры ЗИ" версии 7.2 (Экспертное заключение № 344 от 29 февраля 2012 г.).

DEFENCE OF INFORMATION WITH A LIMIT ACCESS IN THE LOCAL AREA NETWORKS BUILT WITH THE USE OF OPERATING SYSTEMS MS WINDOWS

Andriy Tymoshenko

"Institute of computer technologies" Ltd.

Now it is widely used computerized (information) systems that implement various information technologies as the basis of a computer system which are the local area network - a set of interacting in the process of functioning of computers that have shared resources (hard drives, print devices etc.), which is usually divided into unirank-those in which the shared resources can be in any computer, which can thus act as a client workstation as well as an undedicated server, and networks with dedicated servers - those in which resources of specially dedicated computers (servers) are shared.

The article overviews features of protection of restricted information processed in information systems, which are classified as automated systems of class 2, or in individual components of information systems, classified as automated systems of class 3, as long as the basis of their computer systems is local computer networks, constructed with the use of computers, operating under MS Windows operating systems.

Based on the analysis of the known architecture of software applications of modern information systems, as well as the requirements of the existing legal framework for the protection of restricted information is formed the list of objectives of protection that should be implemented to the information objects that are processed in the information system, in a different form of presentation and in a different state. It is shown that these problems of protection can not be carried out neither by regular protection facilities of MS Windows operating systems, nor by the protection facilities that are implemented in the application software. The necessity of creating integrated security complex, as part of which, except for the protection facilities that are implemented in the application software should be used protective facilities, operating at the kernel level of operating system (protection facilities, integrated with the operating system).

The article shows the ability in usage in the construction of integrated systems of protection the facilities of complex "Grif " (Expert Conclusion № 239 from August 13, 2010), and complex "Grif-Merezha" (Expert Conclusion № 203 from December 24, 2009), produced by "Institute of computer technologies" Ltd. An example of a successful implementation of the proposed approach in creating an integrated security complex of information-analytical system “Kadry ZI” version 7.2 (Expert Conclusion № 344 of February 29, 2012) is provided.

УДК 004.051

ВИРІШЕННЯ ПРОБЛЕМИ ДОСТУПНОСТІ ДО МЕРЕЖІ ІНТЕРНЕТ ШЛЯХОМ ДИНАМІЧНОГО БАЛАНСУВАННЯ ПРОПУСКНОЇ ЗДАТНОСТІ КАНАЛУ WEB-ТРАФІКУ

Юрій Яремчук, Дмитро Кец, Тетяна Жевега, Кирило Безпалий

Вінницький національний технічний університет

Стаття: ***8 стор, 6 джерел.***

На сьогодні в багатьох підприємствах, установах та організаціях, що використовують локальні мережі актуальною є проблема обмеження пропускної здатності каналу доступу цих мереж до глобальної мережі Інтернет, що часто створює передумови до пікових навантажень. Існуючі методи аналізу мережевого трафіку та розроблені на його основі методи прогнозування не дають можливості виконувати динамічне балансування пропускної здатності каналу між користувачами мережі. Відомі методи прогнозування використовувані в мережі вимагають наявності інформації про фактичне використання мережевого трафіку за досить великі проміжки часу та не дають точності прогнозу хоча б до 10% за умови відсутності

самоподібності трафіку. Для вирішення проблеми доступності до мережі Інтернет було запропоновано метод прогнозування навантаження в мережі, що базується на попередньому аналізі фактичних даних про використання мережі користувачами і розрахунком лінійного тренду та показників сезонності. Такий підхід дозволяє з досить малим відсотком похибки спрогнозувати на короткий проміжок часу навантаження на мережу, за рахунок фільтрування та відкидання малоактивних проміжків часу, які можуть вплинути на прогноз. В свою чергу прогнозування навантаження дозволяє розподілити трафік між окремими підмережами локальної мережі та надати доступ до глобальної мережі Інтернет. Також було показано практичне застосування запропонованого методу прогнозування для локальної мережі досить великих розмірів, що підтверджує можливість його використання в мережах підприємств.

РЕШЕНИЕ ПРОБЛЕМЫ ДОСТУПНОСТИ К СЕТИ ИНТЕРНЕТ ПУТЕМ ДИНАМИЧЕСКОГО БАЛАНСИРОВКИ ПРОПУСКНОЙ СПОСОБНОСТИ КАНАЛА WEB-ТРАФИКА

Юрий Яремчук, Дмитрий Кец, Татьяна Жевега, Кирилл Беспалый
Винницкий национальный технический университет

На сегодня во многих предприятиях, учреждениях и организациях, которые используют локальные сети актуальной является проблема ограничения пропускной способности канала доступа этих сетей к глобальной сети Интернет, что часто создает предпосылки к пиковым нагрузкам. Существующие методы анализа сетевого трафика и разработанные на его основе методы прогнозирования не дают возможности выполнять динамическую балансировку пропускной способности канала между пользователями сети. Известные методы прогнозирования используемые в сети, требуют наличия информации о фактическом использовании сетевого трафика за достаточно большие промежутки времени и не дают точности прогноза хотя бы до 10% при условии отсутствия самоподобия трафика. Для решения проблемы доступности к сети Интернет был предложен метод прогнозирования нагрузки в сети, основанный на предварительном анализе фактических данных об использовании сети пользователями, расчетом линейного тренда и показателей сезонности. Такой подход позволяет с достаточно малым процентом погрешности спрогнозировать на короткий промежуток времени нагрузку на сеть, за счет фильтрации и отбрасывания малоактивных промежутков времени, которые могут повлиять на прогноз. В свою очередь, прогнозирование нагрузки позволяет распределить трафик между отдельными подсетями локальной сети и предоставить доступ к глобальной сети Интернет. Также было показано практическое применение предложенного метода прогнозирования для локальной сети достаточно больших размеров, что подтверждает возможность его использования в сетях предприятий.

SOLUTION OF PROBLEM OF AVAILABILITY TO NETWORK BY DYNAMIC BALANCING BANDWIDTH WEB-TRAFFIC

Yuri Yaremchuk, Dmitri rings, Tatiana Zhevega, Cyril Bespalyj
Vinnitsa National Technical University

Today, many enterprises, institutions and organizations use local network meet the actual problem of limiting the bandwidth of access networks to the Internet, which often creates the preconditions for peak loads. Existing methods for analyzing network traffic and developed on the basis of its forecasting methods do not allow performing dynamic balancing bandwidth between network users. Known methods of prediction used in the network, require information on the actual use of network traffic over a sufficiently long period of time and do not give accurate prediction of at least 10% in the absence of self-similarity of traffic. To solve the problem of accessibility to the Internet has been proposed a method of predicting the load on the network, based on preliminary analysis of the evidence on the use of network users, the calculation of the linear trend and seasonal indices. This approach allows a small enough percentage to forecast error for a short period of time the load on the network by filtering and discarding the low-activity periods, which may affect the prognosis. In turn, load forecasting allows you to distribute traffic between the individual subnets network and provide access to the Internet. It was also shown the practical application of the proposed prediction method for local area network is larger, which confirms the possibility of its use in enterprise networks.

УДК: 519.95

КОНТРОЛЬ ЯК МЕХАНІЗМ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНОГО ОБМІНУ В КОМП'ЮТЕРНИХ МЕРЕЖАХ І СИСТЕМАХ.

Юлій Савченко, Георгій Розоронів, Сергій Толюпа*

*Національний технічний університет України "КПІ", *Державний університет інформаційно-телекомунікаційних технологій*

Стаття: ***6 стор., 3 джерела.***

У зв'язку з використанням комп'ютерних мереж як засобу інформаційного обміну в системах управління реальними процесами в промисловості, банках та оборонних об'єктах особлива увага приділяється їх безпеці і надійності. Вже на інтуїтивному рівні поняття безпека й надійність – майже синоніми. Очевидно, що безпека пов'язана з надійністю не тільки апаратних засобів, але і програмного забезпечення, що реалізовує обробку і передачу інформації між робочими станціями (абонентами) комп'ютерної мережі.

У роботі розглядається завдання забезпечення достовірності і безпеки інформаційного обміну на основі використання інформаційної надмірності, яка присутня природно або введена штучно. Запропонована методика визначення реальної вірогідності невиявлення помилок в умовах застосування групових кодів. Отримані оцінки для деяких конкретних і широко вживаних в комп'ютерних мережах кодів. Запропонований підхід дозволяє точно розрахувати виявляючу здатність заданого коду відносно конкретних помилок. Це створює передумови для реалізації мереж з гарантованою безпекою інформаційного обміну шляхом вибору відповідного коду, де безпека, по суті, є вірогідністю відсутності помилок у повідомленні.

КОНТРОЛЬ КАК МЕХАНИЗМ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОГО ОБМЕНА В КОМПЬЮТЕРНЫХ СЕТЯХ И СИСТЕМАХ

Юлий Савченко, Георгий Розоринов, Сергей Толюпа*

*Национальный технический университет Украины "КПИ", *Государственный университет информационно-телекоммуникационных технологий*

В связи с использованием компьютерных сетей в качестве средства информационного обмена в системах управления реальными процессами в промышленности, банках и оборонных объектах особое внимание уделяется их безопасности и надежности. Уже на интуитивном уровне понятия безопасности и надежности – почти синонимы. Очевидно, что безопасность связана с надежностью не только аппаратных средств, но и программного обеспечения, реализующего обработку и передачу информации между рабочими станциями (абонентами) компьютерной сети.

В работе рассматривается задача обеспечения достоверности и безопасности информационного обмена на основе использования информационной избыточности, присутствующей естественно или введенной искусственно. Предложена методика определения реальной вероятности необнаружения ошибок в условиях применения групповых кодов. Получены оценки для некоторых конкретных и широко применяемых в компьютерных сетях кодов. Предлагаемый подход позволяет точно рассчитать обнаруживающую способность заданного кода по отношению к конкретным ошибкам. Это создает предпосылки для реализации сетей с гарантированной безопасностью информационного обмена путем выбора соответствующего кода, где безопасность, по сути, является вероятностью отсутствия ошибок в сообщении.

CONTROL AS A MECHANISM OF PROVIDING SAFETY OF INFORMATIVE EXCHANGE IS IN COMPUTER NETWORKS AND SYSTEMS

Yuliy Savchenko, Georgiy Rozorinov, Sergey Tolyupa*

*National Technical University of Ukraine "Kiev Polytechnic Institute", *State university of information and communication technologies*

In connection with the use of computer networks as a mean of informative exchange in control the system by the real processes in industry, jars and defensive objects the special attention is spared their safety and reliability. Already at intuitional level of concept of safety and reliability almost synonyms. Obviously, that safety is related to reliability of not only vehicle facilities but also software, realizing treatment and passing to information between the work stations (by subscribers) of computer network.

The task of providing of authenticity and safety of informative exchange is in-process examined on the basis of the use of informative surplus, present naturally or entered artificially. The method of determination of the real probability of undetection of errors is offered in the conditions of application of group kodas. Estimations are got for some concrete and widely applied in computer networks kodas. Offered approach allows exactly to expect discovering ability of the set koda in relation to concrete errors. It creates pre-conditions for realization of networks with the assured safety of informative exchange by the choice of the proper koda, where safety, in fact, is probability of absence of errors in a report.

УДК.621.791

МЕТОДИКА КОНТРОЛЮ ПРАЦЕЗДАТНОСТІ ВІБРОВИПРОМІНЮВАЧІВ ДЛЯ СИСТЕМ АКТИВНОГО ЗАХИСТУ МОВНОЇ ІНФОРМАЦІЇ

Михайло Кузнєцов, Ігор Порошин, Михайло Прокофьєв
НДЦ "ТЕЗИС" НТУУ "КПІ"

Стаття: ***7 стор., 3 джерела.***

Нормативні вимоги, згідно з якими характеристики вібровипромінювачів (ВІ) перевіряються на стандартній сталевій масі, не враховують всю різноманітність будівельних конструкцій, на які ВІ встановлюються. Різні конструкції ("важкі" - стіни, стелі, підлоги і т.п.; «легкі» конструкції - вікна, сантехнічно системи, воздуховоди і тому подібне) вимагають для ефективного зашумлення різні рівні шумового віброприскорення. Враховуючи виробничий розкид параметрів ВІ доцільно при входном/виходном контролі показників призначення ВІ розподіляти по групах залежно від рівня віброприскорення, що розвивається ними на стандартній масі.

Подібний диференційований підхід до перевірки ВІ дозволяє у ряді випадків істотно підвищити такий важливий виробничий показник, як «відсоток виходу придатних», а при створенні комплексу ТЗІ істотно зменшити тимчасові і стоїмотсниє витрати на його створення.

Представляється актуальним завдання розробки такої методики перевірки ВІ, яка могла б бути реалізована за допомогою досяжних засобів (персонального комп'ютера (ПК) і відповідного безкоштовного програмного забезпечення) і при цьому по ефективності відбору придатних ВІ не поступалася б традиційній методиці, заснованій на вживанні стандартного устаткування, до складу якого входить шумомір (ВШВ).

Пропонована методика може бути реалізована за допомогою стенду, в якому ВІ, що перевіряється, підключений до виходу віброакустичного генератора, передає вібрацію безпосередньо ВД, який використовується в режимі прямого п'єзоефекту. При цьому конструкція стенду забезпечує надійний прямий механічний контакт між робочими поверхнями ВД і ВІ, що перевіряється.

Сигнал, що поступає з виходу ВД безпосередньо на вхід звукової карти ПК, дозволяє спостерігати у вікні програми аналізатора спектру що огинає спектру вихідного сигналу ВД. По розташуванню що цією огинає спектру відносно межі поля допуску («кордони знизу») робиться висновок про стан працездатності ВІ, що перевіряється.

Межа поля допуску заздалегідь наноситься на робоче поле вікна програми аналізатора спектру і там фіксується. Запропонована методика була апробована при перевірці партії ВІ, прошедшей випробування з використанням стандартних вимірювальних засобів (комплекту ВШВ і стандартної сталевої маси).

Порівняння результатів, отриманих в обох випадках, показало, що дані випробувань ВІ за допомогою запропонованої методики і дані випробувань ВІ за допомогою традиційної методики повністю збігаються. Тому є підстави вважати, що запропонована методика перевірки працездатності ВІ (з врахуванням відносної простоти і дешевизни її реалізації) може бути використана у ряді випадків для оперативної діагностики ВІ як в умовах виробництва (наприклад, при вихідному контролі виробника), так і у споживача (як вхідний контроль).

МЕТОДИКА КОНТРОЛЯ РАБОТОСПОСОБНОСТИ ВИБРОИЗЛУЧАТЕЛЕЙ ДЛЯ СИСТЕМ АКТИВНОЙ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ

Михаил Кузнецов, Игорь Порошин, Михаил Прокофьев
НИЦ "ТЕЗИС" НТУУ "КПИ"

Нормативные требования, согласно которым характеристики виброизлучателей (ВИ) проверяются на стандартной стальной массе, не учитывают всё разнообразие строительных конструкций, на которые ВИ устанавливаются. Различные конструкции ("тяжелые" - стены, потолки, полы и т.п.; «лёгкие» конструкции - окна, сантехнически системы, воздуховоды и т.п.) требуют для эффективного зашумления различные уровни шумового виброускорения. Учитывая производственный разброс параметров ВИ целесообразно при входном/выходном контроле показателей назначения ВИ распределять по группам в зависимости от уровня виброускорения, развиваемого ими на стандартной массе. Подобный дифференцированный подход к проверке ВИ позволяет в ряде случаев существенно повысить такой важный производственный показатель, как «процент выхода годных», а при создании комплекса ТЗИ существенно уменьшить временные и стоимотсные затраты на его создание. Представляется актуальной задача разработки такой методики проверки ВИ, которая могла бы быть реализована с помощью легкодоступных средств (персонального компьютера (ПК) и соответствующего бесплатного программного обеспечения) и при этом по эффективности отбора годных ВИ не уступала бы традиционной методике, основанной на применении стандартного оборудования, в состав которого входит шумомер (ВШВ).

Предлагаемая методика может быть реализована с помощью стенда, в котором проверяемый ВИ, подключённый к выходу виброакустического генератора, передаёт вибрацию непосредственно ВД, который используется в режиме прямого пьезоэффекта. При этом конструкция стенда обеспечивает надёжный прямой механический контакт между рабочими поверхностями ВД и проверяемого ВИ. Сигнал, поступающий с выхода ВД непосредственно на вход звуковой карты ПК, позволяет наблюдать в окне программы анализатора спектра огибающую спектра выходного сигнала ВД. По расположению этой огибающей спектра относительно границы поля допуска («границы снизу») делается заключение о состоянии работоспособности проверяемого ВИ. Граница поля допуска заранее наносится на рабочее поле окна программы анализатора спектра и там фиксируется.

Предложенная методика была апробирована при проверке партии ВИ, прошедшей испытания с использованием стандартных измерительных средств (комплекта ВШВ и стандартной стальной массы). Сравнение результатов, полученных в обоих случаях, показало, что данные испытаний ВИ с помощью предложенной методики и данные испытаний ВИ с помощью традиционной методики полностью совпадают. Поэтому есть основания полагать, что предложенная методика проверки работоспособности ВИ (с учётом относительной простоты и дешевизны её реализации) может быть использована в ряде случаев для оперативной диагностики ВИ как в условиях производства (например, при выходном контроле производителя), так и у потребителя (в качестве входного контроля).

METHODOLOGY OF CONTROL THE CAPACITY OF VIBROEMITTERS FOR THE SYSTEMS OF ACTIVE DEFENCE OF VOCAL INFORMATION

Michael Kuznecov, Igor Poroshin, Michael Prokof'ev
WITH one's the face touching the ground "THESIS" of NTUU "KPI"

Normative requirements according to that descriptions of vibroemitters(VE) are checked for standard steel mass do not take into account all variety of building constructions, on that VE set. Different constructions("heavy" are walls, ceiling, полы etc.; "easy" constructions are windows, sanitary engineering systems, air-ducts etc.) are required for effective noise masking by the different levels of noise vibroacceleration. Taking into account productive variation of parameters of VE expediently at an entrance/weekend control of indexes of setting of VE to distribute on groups depending on the level of the vibroacceleration developed by them on standard mass. The similar differentiated going near verification of VE allows in a number of cases substantially to promote such important productive index, as "percent of exit suitable", and at creation of complex TZI substantially to decrease temporal and стоимотсные expenses on his creation. A task of development of such methodology of verification of ВИ, that would be realized by means of accessible facilities of personal computer(PC) and corresponding public domain

software) and here on efficiency of selection of suitable VE would not yield to the traditional methodology, based on application of standard equipment of audio-noise meter (ANM) enters in the complement of that.

The offered methodology can be realized by means of stand, in that checked up VE connected to the exit of vibroacoustic generator passes a vibration directly VD, that is used in the mode of direct piezo-effect. Thus the construction of stand provides a reliable direct mechanical contact between the working surfaces of VD and checked up VE. A signal acting from the exit of VD directly to the entrance of sound card PC allows to look after in the window of the program of spectrum analyzer circumflex spectrum of output signal of VD. On a location this circumflex spectrum in relation to the border of the field of admittance("borders from" below) concluded about the state of capacity of checked up VE. The border of the field of admittance is beforehand inflicted on the working field of window of the program of spectrum analyzer and fixed there.

An offer methodology was approved at verification of party of VE, passing tests with the use of standard measuring facilities(complete set of ANM and standard steel mass). Comparison of the results got in both cases showed that data of tests of VE by means of an offer methodology and data of tests of VE by means of traditional methodology coincided fully. Therefore there are grounds to suppose that an offer methodology of verification of capacity of VE (taking into account relative simplicity and cheapness of her realization) can be used in a number of cases for operative diagnostics of VE both in the conditions of production(for example, at output control of producer) and for a consumer(as entrance control).

УДК: 004.052.2+004.056

ОРГАНІЗАЦІЙНО-ТЕХНІЧНЕ ЗАБЕЗПЕЧЕННЯ ПРОЦЕСУ ВІДНОВЛЕННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ ПІСЛЯ АВАРІЇ

Любомир Пархуць, Тетяна Хома, Олена Хмиз
Національний університет «Львівська політехніка»

Стаття: ***7 стор, 9 джерел.***

За своїми наслідками особливо катастрофічними є аварії інформаційних систем, які можуть призвести не лише до тривалих простоїв, але і до втрати критичних даних. Створення абсолютно безпечної інформаційно-телекомунікаційної системи (ІКС) є неможливим через повну втрату її функціональності. Тому навіть у захищених системах завжди існує залишковий ризик. Заздалегідь створений та відповідно організаційно і технічно забезпечений план аварійного відновлення ІКС здатний пом'якшити наслідки аварії і у підсумку зменшити фінансові та інші ризики організації.

Метою роботи є характеристика аварії у контексті функціонування інформаційної системи, формулювання завдань плану відновлення після аварії, опис існуючих рішень із ефективного обслуговування аварійних ситуацій, а також обґрунтування доцільності розроблення та використання при управлінні аваріями в ІКС системи підтримки прийняття рішень. Якщо проаналізувати статистику загроз інформаційної безпеки, які найчастіше реалізуються приводячи ІКС до нештатного режиму, то це насамперед є інциденти з причин помилок персоналу і тільки за ними йдуть атаки зловмисників.

План аварійного відновлення має містити докладний перелік заходів і дій, які необхідно виконати «до», «під час» і «після» виникнення надзвичайної ситуації. Тут визначається порядок повідомлення відповідальних співробітників та викладаються детальні інструкції для виконавців. Все це дозволяє максимально швидко відновити працездатність ІКС. *Запобігання аварії у майбутньому* передбачає реалізацію низки заходів щодо ліквідації причин аварії, зменшення виявлених вразливостей компонентів ІКС. За рахунок аналізу аварій в ІТ-системі підвищується ймовірність запобігання майбутніх аварій, поліпшуються механізми і процеси забезпечення інформаційної безпеки. Надійне збереження дуже важливих даних у випадку виникнення надзвичайної ситуації забезпечується за допомогою розподілених мереж зберігання даних (англ. Storage Area Network - SAN), для роботи яких необхідні надійні й високопродуктивні канали передачі даних. Технологія SAN забезпечує відмовостійкий доступ серверів до ресурсів зберігання і дозволяє знизити сукупну вартість утримання ІТ-інфраструктури за рахунок оптимального онлайнового управління доступу серверів до ресурсів зберігання, використання зовнішнього ресурсу, тобто передача організацією на основі довгострокових контрактів деяких виробничих функцій на обслуговування іншій компанії, що спеціалізується у відповідній області - аутсорсинг інформаційних систем. Хоча аутсортсинг центрів обробки даних є привабливим і перспективним напрямком у забезпеченні аварійностійкості інформаційної інфраструктури, на цей час в Україні його поширення наштовхується на певні труднощі,

пов'язані насамперед із недостатньою кількістю ЦОД, недоступністю високоякісних і швидкісних каналів передачі даних для багатьох організацій.

Видається доцільним варіант запровадження в організаціях системи підтримки прийняття рішень у аварійних ситуаціях, яка дасть можливість не тільки обробляти значно більший об'єм інформації, а й значно зменшити вплив психологічних факторів на прийняття необхідних рішень на кожному з етапів відновлення ІКС.

ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПРОЦЕССА ВОССТАНОВЛЕНИЯ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СИСТЕМ ПОСЛЕ АВАРИИ

Любомир Пархуць, Татьяна Хома, Елена Хмыз
Национальный университет «Львовская политехника»

По своим последствиям особенно катастрофическими являются аварии информационных систем, которые могут привести не только к длительным простоям, но и к потере критических данных. Создание абсолютно безопасной информационно телекоммуникационной системы (ИКС) являются невозможными через полную потерю ее функциональности. Поэтому даже в защищенных системах всегда существует остаточный риск. Предварительно созданный и соответственно организационно и технически обеспеченный план аварийного возобновления ИКС способен смягчить последствия аварии и в результате уменьшить финансовые и другие риски организации.

Целью работы является характеристика аварии в контексте функционирования информационной системы, формулировки заданий плану возобновления, после аварии, описание существующих решений из эффективного обслуживания аварийных ситуаций, а также обоснования целесообразности разрабатывания и использования, при управлении авариями в ИКС системы поддержки принятия решений. Если проанализировать статистику угроз информационной безопасности, которые чаще всего реализуются приводя ИКС к нештатному режиму, то это в первую очередь является инцидентами из причин ошибок персонала и только за ними идут атаки злоумышленников.

План аварийного возобновления должен содержать подробный перечень мероприятий и действий, которые необходимо выполнить «к», «под время» и «после» возникновения чрезвычайной ситуации. Здесь определяется порядок сообщения ответственных сотрудников и выкладываются детальные инструкции для исполнителей. Все это позволяет максимально быстро возобновить работоспособность ИКС. Предотвращение аварии в будущем предусматривает реализацию ряда мероприятий по ликвидации причин аварии, уменьшения обнаруженных уязвимых компонентов, ИКС. За счет анализа аварий в ИТ-системе повышается вероятность предотвращения будущих аварий, улучшаются механизмы и процессы обеспечения информационной безопасности. Надежное сохранение очень важных данных в случае возникновения чрезвычайной ситуации обеспечивается с помощью распределенных сетей хранения данных (англ. Storage Area Network SAN), для работы которых необходимы надежные и высокопродуктивные каналы передачи данных. Технология SAN обеспечивает отказоустойчивый доступ серверов к ресурсам хранения и позволяет снизить совокупную стоимость содержания ИТ-инфраструктуры за счет оптимального онлайнового управления доступа серверов к ресурсам хранения, использования внешнего ресурса, то есть передача организацией на основе долгосрочных контрактов некоторых производственных функций на обслуживание другой компании, которая специализируется в соответствующей области - аутсорсинг информационных систем. Хотя аутсортсинг центров обработки данных является привлекательным и перспективным направлением в обеспечении аварийностойкости информационной инфраструктуры, на это время в Украине его распространения наталкивается на определенные трудности, связанные в первую очередь с недостаточным количеством ЦОД, недоступностью высококачественных и скоростных каналов передачи данных для многих организаций.

Кажется целесообразным вариант внедрения в организациях системы поддержки принятия решений в аварийных ситуациях, которая даст возможность не только обрабатывать значительно больше объема информации, но и значительно уменьшить влияние психологических факторов на принятие необходимых решений на каждом из этапов возобновления ИКС.

ORGANIZATIONAL-TECHNICAL PROVIDING OF RENEWAL PROCESS OF INFORMATIVELY-COMMUNICATION SYSTEMS AFTER ACCIDENT

Lubomyr Parhyz, Tatyana Homa, Elena Hmuz
Lviv Polytechnic National University

On the consequences especially catastrophic are accidents of the informative systems, that can result not only in the protracted outages but also to the loss of critical data. Creation absolutely safe informatively telecommunication system(ITS) are impossible through the complete loss of her functionality. Therefore there always is a remaining risk even in the protected systems. Preliminary created and accordingly organizationally and the technically provided plan of emergency renewal ITS is able to soften the consequences of accident and as a result to decrease financial and other risks of organization.

The aim of work is description of accident in the context of functioning of the informative system, formulation of tasks to the plan of renewal, after an accident, description of existent decisions from effective maintenance of emergency situations, and also ground of expediency of development and use, at a management by accidents in ITS of the system of support of making decision. If to analyse statistics of threats of informative safety, that mostly will be realized bringing ITS over to the nonpermanent mode, then it first of all is incidents from reasons of errors of personnel and only the attacks of malefactors follow after them.

The plan of emergency renewal must contain the detailed list of events and actions that must be executed "to", "under time" and "after" the origin of emergency. The order of report of responsible employees is here determined and the detailed instructions are laid out for performers. All of it allows maximally quickly to renew a capacity ITS. Prevention of accident in the future envisages realization of row of events for liquidations of reasons of accident, reduction of found out exposures components, ITS. Due to the analysis of accidents probability of prevention of future accidents rises in the IT-system, mechanisms and processes of providing of informative safety get better. Reliable maintenance of very important data in case of origin of emergency is provided by means of the up-diffused networks of storage of data(eng of Storage Area Network SAN), for work of that the reliable and highly productive channels of data are needed.

Technology of SAN provides fault-tolerant access of servers to the resources of storage and allows to bring down the combined upkeep of IT-infrastructure costs due to the optimal on-line management of access of servers to the resources of storage, uses of external resource, id est transmission by organization on the basis of long-term contracts of some productive functions on maintenance of other company that is specialized in a corresponding area - аутсорсинг of the informative systems. Although outsourcing DPCS is attractive and perspective direction in providing of emergency capability of informative infrastructure, on this time in Ukraine of his distribution comes across the certain difficulties, related first of all to the insufficient amount of DPC, inaccessibility of high-quality and speed channels of data for many organizations.

The variant of introduction in organizations of the system of support of making decision seems expedient in emergency situations, that will give an opportunity not only to process the considerably anymore volume of information but also considerably to decrease influence of psychological factors on the acceptance of necessary decisions on each of the stages of renewal ITS.